Table of Contents

Abbreviations and Acronyms

ACLU	American Civil Liberties Union (US)
ADMA	Australian Direct Marketing Association (AU)
ADR	Alternative Dispute Resolution
ADVISE	Analysis, Dissemination, Visualization, Insight, and Semantic Enhancement
ALRC	Australian Law Reform Commission (ALRC)
ALWD	Association of Legal Writing Directors Citation Manual (3rd ed.).
APEC	Asia-Pacific Economic Cooperation
ARPA	Advanced Research Projects Agency (US)
AU	Australia - Commonwealth of Australia
B2B	Business to Business
B2C	Business to Consumer
BCR	Binding Corporate Rules
BT	British Telecom (UK)
CA	Canada - Government of Canada
CA-ASA	The CA Anti-Spam Act (CA)
CAD	Canadian Dollars
CEAA	Canadian Environmental Assessment Act (CA)
CEPA	Canadian Environmental Protection Act (CA)
CIA	Central Intelligence Agency (US)
CM	Comparative Model of Legal Support of DPSIP Models
COPPA	Children's Online Privacy Protection Act (US)
CORBA	Common Object Request Broker Architecture
CPO	Chief Privacy Officer
CSA	Canadian Standard Association (CA)
DARPA	Defense Advanced Research Projects Administration (US)
DEA	Drug Enforcement Agency (US)
DHS	Department of Homeland Security (US)
DNC	Do Not Call Registry (US)
DOC	Department of Commerce (US)

DOT	Department of Transportation (US)
DPA	Data Protection Act (UK)
DPA-EU	Data Protection Authority (EU)
DPSIP	Data Protection, Security, and Information Privacy
ECHR	European Court of Human Rights.
EEA	European Economic Area
ECPA	Electronic Communications Privacy Act (US)
EDPS	European Data Protection Supervisor (EU)
EHR	Electronic Health Records
EMR	Electronic Medial Records
EPC	Electronic Product Code
EPIC	Electronic Privacy Information Center
EU	European Union
FACA	Federal Advisory Committee Act (US)
FBI	Federal Bureau of Investigation (US)
FCC	Federal Communications Commission (US)
FDIC	Federal Deposit Insurance Corporation (US)
FERPA	Family Educational Rights and Privacy Act (US)
FISA	Foreign Intelligence Surveillance Act (US)
FTC	Federal Trade Commission (US)
FTP	File Transfer Protocol
GB	Great Britain - England, Scotland, and Wales
GAO	Government Accountability Office (US)
GLBA	Gramm-Leach-Bililey Act (US)
GPS	Global Positioning Systems
HIPAA	Health Insurance Portability and Accountability Act (US)
HITECH	Health Information Technology for Economic and Clinical Health
HP	Hewlett Packard
HPPs	Health Privacy Principles (AU, NSW)
HRA	Human Rights Act (UK)
HUAC	House Un-American Activities Committee (US)
ICO	Information Commissioner’s Office (UK)
IDL	Interface Definition Language

IETF	Internet Engineering Task Force
IIOP	Inter-ORB Protocol
IP	Intellectual Property
InP	Internet Protocol
IPPs	Information Privacy Principles (AU)
IRS	Internal Revenue Service (US)
ISP	Internet Service Providers
IT	Information Technology
KDD	Knowledge Discovery in Databases
MPAA	Motion Picture Association of America (US)
NAACP	National Association for the Advancement of Colored People (US)
NAI	National Advertising Network (US)
NCLB	National Civil Liberties Bureau (CA)
NEPA	National Environmental Policy Act (US)
NFC	Near Field Communications
NGO	Non-Governmental Organizations
NPP	National Privacy Principles (AU)
NSA	National Security Agency (US)
NSF	National Science Foundation (US)
NSW	New South Wales (AU)
NT	Northern Territory (AU)
OAS	Organization of American States (Western Hemisphere)
OECD	Organization for Economic Co-operation and Development
OMB	Office of Management and Budget (US)
OMG	Object Management Group
OTA	Office of Technology Assessment (US)
PbD	Privacy by Design
PCPA	Pest Control Products Act (CA)
PCC	Privacy Commissioner of Canada (CA)
PDE	Personal Data Ecosystem
PDV	Personal Data Vault
PET	Privacy Enhancing Technologies

PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIPEDA	Personal Information Protection and Electronic Document Act (CA)
PM	Personalized Medicine
POIP	Protection of Personal Information (SA)
Qld	Queensland (AU)
RCMP	Royal Canadian Mounted Police (CA)
RFID	Radio Frequency Identification
RIPA	Regulation of Investigatory Powers Act (UK)
SA	Republic of South Africa
SA-AU	South Australia (AU)
SALRC	South African Law Reform Commission (SA)
SEC	Securities and Exchange Commission (US)
SLAPPS	Strategic Lawsuits Against Public Participation (CA)
SOAP	Simple Object Access Protocol
SPSS	Statistical Package for the Social Sciences
SQL	Structured Query Language
SSL	Secure Socket Layer Encryption
SSN	Social Security Number (US)
SWIFT	Society for Worldwide Interbank Financial Telecommunications
TAPAC	Technology and Privacy Advisory Committee (US)
Tas	Tasmania (AU)
TIDE	Terrorist Identities' Datamart Environment (US)
TSR	Telemarketing Sales Rule (US)
UK	United Kingdom of Great Britain (England, Scotland, and Wales) and Northern Ireland.
UN	United Nations
UPPs	Uniform Privacy Principles (AU)
US	United States of America
USA-Patriot Act	Uniting and Strengthening America by Providing Appropriate Tools Required to Obstruct Terrorism Act (US)

USD	United States Dollar
VA	Veterans Administration (US)
Vic	Victoria (AU)
W3C	World Wide Web Consortium
WA	Western Australia (AU)
WIPO	World Intellectual Property Organization

List of Figures

List of Tables

Table of Authorities

Table of Cases

Australia (AU)

Lenah Game Meats (2001) 208 CLR 199. (AU)

Minister for Immigration and Ethnic Affairs v Teoh, 183 CLR 273 at 286-6, (1995) (AU).

MT v Director General, NSW Department of Education & Training, NSWADT 194, (3 September 2004) (NSW-AU).

NRMA v John Fairfax, NSWSC 563, (2002) (NSW AU).

OD v Department of Education and Training, NSWADT 161, (2005) (NSW-AU).

ON v Marrickville Council, NSWADT 274, (2 December 2005) (NSW-AU).

OQ v Commissioner of Police, NSWADT 240, (2005) (NSW-AU).

PN v Department of Education and Training, NSWADT 122, (2006) (NSW-AU).

SW v Forests NSW, NSWADT 74, (2006) (NSW-AU).

Vice-Chancellor Macquarie University v FM, NSWCA 192, (2005) (NSW-AU).

Victoria Park Racing & Recreation Grounds Co Ltd v Taylor, HCA 45; (1937) 58 CLR 479, (26 August 1937) (AU).

Canada (CA)

A-G Canada v A-G Quebec, 2 D.L.R. 81 (JCPC), (1932) (CA).

Aubry v. Editions Vice-Versa Inc, 1 S.C.R. 591, (1998) (CA).

B.C.G.E.U. v. British Columbia (Minister of Health Services), 2005 CarswellBC 672, 2005 BCSC 446, 27 Admin. L.R. (4th) 125, 129 C.R.R. (2d) 301, (25 March 2005) (CA-BCSC).

Canada (Information Commissioner) v. Canada (Minister of Citizenship & Immigration), 2002 CarswellNat 1476, 2002 FCA 270, 291 N.R. 236, 228 F.T.R. 319 (note), [2003] 1 F.C. 219, 21 C.P.R. (4th) 30, 1 Admin. L.R. (4th) 270, (21 June 2002) (CA).

Canada (Privacy Commissioner) v. Canada (Attorney General) (2003), [2003] B.C.J. No. 1344, 14 B.C.L.R. (4th) 359, [2003] 9 W.W.R. 242, 2003 BCSC 862, 2003 CarswellBC 1394 (B.C. S.C.), (5 June 2003) (CA).

Canada Post Corp. v. Canada (Minister of Public Works) (1995), [1995] F.C.J. No. 241, 60 C.P.R. (3d) 441, 91 F.T.R. 320 (note), (sub nom. Societe canadienne des postes v. Canada) [1995] 2 F.C. 110, 179 N.R. 350, 30 Admin. L.R. (2d) 242, 1995 CarswellNat 688, 1995 CarswellNat 652

(CA).

R. v. Dyment, 2 S.C.R. 417 at 427-428, 55 D.L.R. (4th) 503, 66 C.R. (3d) 348, (1988) (CA).

R. v. Drybones, S.C.R. 282, 9 D.L.R. (3d) 473, 3 C.C.C. 355, 10 C.R.N.S. 334, 71 W.W.R. 161, (1970) (CA).

R. v. E. (M.) (2006), 2006 CarswellOnt 2482, 2006 ONCJ 146, [2006] O.J. No. 1657 (Ont. C.J.), (8 March 2006) (CA).

R. v. Edwards Books and Art Ltd., (1986) 2 S.C.R. 713 at 779, (1986) (CA).

R. v. Plant, 3 S.C.R. 281 (S.C.C.), (1993) (CA).

R. v. Stewart, (1988). Stewart v. The Queen. (1988) 1 S.C.R. 963 (1988) (CA).

R. v. Wise, 1992 CarswellOnt 71, 11 C.R. (4th) 253, [1992] 1 S.C.R. 527, 70 C.C.C. (3d) 193, 133 N.R. 161, 8 C.R.R. (2d) 53, 51 O.A.C. 351, (27 February 1992) (CA).

Rodriguez v. British Columbia (Attorney-General) 107 D.L.R. (4th) 342 (SC.C.), (1993) (CA).

Rousseau v. Wyndowe A-551-06, 2008 FCA 39, (2008) 2 F.C.R. D-12, (1 February 2008) (CA).

Ruby v Canada (Solicitor General) 2000 CarswellNat 1106, 256 N.R. 278, 184 F.T.R. 159 (note), 6 C.P.R. (4th) 289, [2000] 3 F.C. 589, 2000 CarswellNat 3423, 187 D.L.R. (4th) 675, 3 F.C. 589, 2000 F.C.J. No. 779, 42 Admin. L.R. (3d) 214) (CA).

Slaight Communications Inc. v. Davidson, 1 S.C.R. 1038 (1989) (CA).

Somwar v. McDonald's Restaurants of Canada Ltd., (2006), 79 O.R. (3d) 172 (2006), 263 D.L.R. (4th) 752, (2006) (CA).

Stubicar v Alberta (Information & Privacy Commissioner, 2008 CarswellAlta 1625, 2008 ABCA 357 (Alta. C.A.) (CA - Alberta).

Thorson v. Attorney General of Canada, 1 S. C.R. 138, (1975) (CA).

X. v. Accusearch Inc., dba Abika.com et al., Federal Court File No. T–2228–05, (2007) (CA).

X. v. Telus Communications Inc., Federal Court of Appeal File No. A–639–05, (2007) (CA).

European Union (EU)

Amann v. Switzerland, ECHR 27798/95, (2000) (EU).

Case of Copland v. The United Kingdom, Application no. 62617/00 (3 April 2007) (ECHR 2007) (EU).

Chavenee Jullien v. France, Appl 14461/88, 71 DR 141, (1991) (EU).

European Court of Human Rights, *Case of I v. Finland (Application no. 20511/03)*. (2008, July 17,), at http://cmiskp.echr.coe.int/tkp197/view.asp?item=3&portal=hbkm&action=html&highlight=Finland%20%7C%20data%20%7C%20security%20%7C%20privacy&sessionid=12271808&skin=hudoc-en (accessed 30 July 2011). (EU)

Gaskin v. United Kingdom 10454/83 [1989] European Court of Human Rights 13 (7 July 1989) (EU).

Hatton v. United Kingdom, E.C.H.R. 565, (2002) 34 EHRR 1, (2001) (EU).

Leander v. Sweden, 26 March 1987, 9 EHRR 433, (1987) (EU).

Niemietz v. Germany, E.C.H.R. 12/16/1992, (1992) (EU).

P.G. & J.H. v. United Kingdom, E.C.H.R., 9/25/2001, (2001) (EU).

Productores de Música de España (Promusicae) v. Telefónica de España SAU, Case C-275/06, (2008) (EU).

Rotaru v. Romania ECHR 28341/95; 8 BHRC 449, (2000) (EU).

The Rachel Affaire. Trib. pr. inst. de la Seine, 1858 D.P. III 62, (1858) (Sweden).

Republic of South Africa (SA)

Bernstein v Bester, 1996 (2) SA 751 (CC); 1996 (4) BCLR 449 (SA).

C v Minister of Correctional Services, 1996 (4) SA 292 (T) (SA).

Carmichele v Minister of Safety and Security (Centre for Applied Legal Studies Intervening), 2001 (4) SA 938 (CC) (SA).

Case v Minister of Safety and Security 1996 (3) SA 617 (CC)) (SA).

Castell v De Greef 1994 (4) SA 408 (T) (SA).

Financial Mail (Pty) Ltd v Sage Holdings Ltd, 1993 (2) SA 451 (A) (SA).

Gosschalk v Rossouw, 1966 (2) SA 476, 492 (C) (SA).

Grutter v Lombard, 2007 (4) SA 89 (SCA) (SA).

Hendy v. Oomkens abd Shallies, 1924 T.P.D. 165, (1924) (SA).

Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Ply) Ltd 2001 1 SA 545 (CC) (SA).

Janit v Motor Industry Fund Administrators (Pty) Ltd, 1995 (4) SA 293 (A) (SA).

Jansen van Vuuren v Kruger 1993 (4) *SA 842 (A*) (SA).

Jeffreys v Boosey, (4) HLC 815 862, (1854) (SA).

Kidson v SA Associated Newspapers LTD 1957 (3) SA 461 (W) (SA).

La Grange v Schoeman, 1980 (1) SA 885 (E) (SA).

Madallie & Schieff v. Roux, 1920 20 S.C. 438 (SA).

Mhlongo v Bailey, 1958 (1) SA 370 (C) (SA).

Mistry v Interim Medical and Dental Council of South Africa, 1998 (4) SA 1127 (CC) (SA).

Motor Industry Fund Administrators (Pty) Ltd v Janit, 1994 (3) SA 56 (W)(SA).

National Media v Jooste 1996 (3) *SA 262 (A*) (SA).

O'Keefe v. Argus Printing & Publishing Co. Ltd 1954 (3) SA 244 (CPD) (SA).

Protea Technology v Wainer, [1997] 3 All SA 594 (W) 608; 1997 9 BCLR 1225 (W) 1241) (SA).

Rhodesian Printing and Publishing v Duggan 1975 (1) SA 590 (R) (SA).

S v A, 1971 (2) SA 293 (T) (SA).

S v Bailey, 1981 (4) SA 187 (N) (SA).

S v. Jordan (6) SA 642 (CC), [2002] (11) B.C.L.R. 1117; 2002 (6) SA 642) (SA).

Van Tonder v. Alexander, 1906 E.D.L.D. 186 (SA).

Waring & Gillow Ltd v Sherborne, 1904 TS 340 (SA).

United Kingdom (UK)

Alan Lord v. The Secretary of State for the Home Department, EWHC 2073, (1 September 2003) (UK).

Ash & Anor v. McKennitt & Ors, [2006] EWCA Civ 1714 (14 December 2006) [2007] 3 WLR 194, [2007] EMLR 4, [2006] EWCA Civ 1714, [2008] QB 73, [2006] EMLR 178, (2006) (UK).

Campbell v. MGN Ltd., [2004] UKHL 22 (6 May 2004) [2004] UKHRR 648, [2004] 2 AC 457, [2004] EMLR 15, [2004] UKHL 22, 16 BHRC 500, [2004] 2 WLR 1232, [2004] HRLR 24, [2004] 2 All ER 995, (2004)

(UK).

Community Charge Registration Officer of Runnymede Borough Council v Data Protection Registrar (Case Da/90 24/49/3) (UK).

Community Charge Registration Officer of South Northamptonshire District Council v Data Protection Registrar (Case Da/90 24/49/4) (UK).

Community Charge Registration Officer of Harrow Borough Council v Data Protection Registrar (Case Da/90 24/49/5)) (UK).

Derbyshire County Council v Times Newspapers Ltd and Others, [1993] AC 534, [1993] 1 All ER 1011, [1993] 2 WLR 449, 91 LGR 179 House of Lords, (1993) (UK).

Douglas & Ors v. Hello! Ltd & Ors, [2003] EWHC 786 (Ch) (11 April 2003) [2003] 3 All ER 996, [2003] EMLR 31, [2003] EWHC 786 (Ch), (2003) (UK).

Durant v. Financial Services Authority, EWCA Civ 1746, (2003) (UK).

Entick v. Carrington, 1558-1774. All E.R. Rep. 45, (1765) (UK).

Equifax Europe Limited v The Data Protection Registrar, Data Protection Tribunal (DA/90 25/49/7) (UK).

Gaskin v. United Kingdom, July 7,1989, Series A, No 160, (1998) (UK).

Grant v. Allen (1987 S.C.C.R): Grant v. Procurator Fiscal, High Court of Justiciary, Hearing-Dates: 5 June, (1987) (UK).

Heydon's Case 76 Eng. Rep. 637, (1584) (UK).

Hm Advocate v. Wilson High Court of Justiciary, SCCR 420, (1983) (UK).

Infolink Limited v The Data Protection Registrar, Data Protection Tribunal (DA/90 25/49/6) (UK).

Infolink Limited v. The Data Protection Registrar, (DA/90 25/49/6)) (UK).

Innovations (mail order) Limited v Data Protection Registrar, case da/92 31/49/1) UKIT DA92_31491 (29 September, (1992) (UK).

Johnson v. Medical Defense Union, EWCA Civ 262, (28 March 2007) (UK).

Kaye v. Robertson, FSR 62, (1991) (UK).

Linguaphone Institute Limited v Data Protection Registrar, Data Protection Tribunal (Case DA/94 31/49/1)) (UK).

London Street Tramways v London County Council, [1898] AC 375, (1898) (UK).

Marcel v Metropolitan Police Commissioner, Ch. 225 at 240, (1992) (UK).

Midlands Electricity PLC v. The Data Protection Registrar, Data Protection Registrar (DA/ 99) (UK).

Miller v. Taylor, 4 Burr. 2303, 2379, (1769) (UK).

Morison v. Moat, 68 Eng. Rep. 492, 9 HARE 241, (1851) (UK).

Murray v. Big Pictures (UK) Ltd [2008] EWCA Civ 446, (7 May 2008) (UK).

Norman Baker v. Secretary of State for the Home Department, UKHRR 1275, (2001) (UK).

Oxford v. Moss Queen's Bench Divisional Court, 68 Cr App Rep 183., (1978) (UK).

Peter Hitchens v. Secretary of State for the Home Department, UKHRR 1275, (10 December 2001) (UK).

Pitman Training Ltd. v. Nominet UK Ch. 1997-F-No, 1984 (High Court. of Justice May 22, 1997) (UK).

Pope v. Curl, 2 Atk. 324, 26 Eng. Rep. 608 (1741) (UK).

Prince Albert v. Strange, 1 H & Tw 1; 2 De G & SM 293; (1849) 1 Mac & G 25; [1849] EWHC Ch J20, (1849) (UK).

R v Secretary of State for Employment ex parte Equal Opportunities Commission, 2 WLR 409, (1994) (UK).

R. v. Gold, 2 ALL ER 186 (Court of Appeal), (1988) (UK).

Regina v Secretary of State for Transport, ex parte Factortame (No 2) [1991] 1 AC 603, (1991) (UK).

Regina v. Brown, 1 ALL ER 545 at 555-556, (24 July 1997) (UK).

Regina v. Jacqueline Mary Rooney, EWCA Criminal 1841 (12 July 2006) (UK).

Saltman Engineering Co. Ltd. v. Campbell Engineering Co. Ltd., 65 R.P.C. 203, (1948) (UK).

Slater v. Baker & Stapelton, 95 English Reporter 860 (K. B.), (1767) (UK).

Sykes v. Sykes, 107 Eng. Rep. 834 (1824) (UK).

The Community Charge Registration Officer of Rhondda Borough Council v Data Protection Registrar, Data Protection Tribunal (Case DA/90 25/49/2)) (UK).

Tony Gosling v. Secretary of State for the Home Department, UKHRR 1275, (10 December 2001) (UK).

X v. British Broadcasting Corporation & Anor, [2005] ScotCS CSOH_80 (22

June 2005) (UK).

United States (US)

Abrams v. United States, 250 U.S. 616, 1180, 40 S. Ct. 17, 63 L. Ed. 1173 616, 30 (Holmes, J., dissenting), (1919) (US).

ACLU v. Gonzales, No. 04-2614 (S.D.N.Y. Sept. 6. (2007),(US) at http://www.aclu.org/pdfs/safefree/nsldecision.pdf (accessed 15 June 2011). (US)

ACLU v. Reno, 117 S.Ct. 2329, 138 L117, (2000) (US).

American Communications Association v. Douds, 339 U.S. 382, (1950) (US).

American Friends Service Committee, et al. v City and County of Denver, United States District Court, District of Colorado, Civil Action No. 02-N-0740 (CBS), (2002) (US).

Arizona Retail Systems v. The Software Link, Inc, F. Supp.831 759 (D. Ariz.) (1993) (US).

Arizona v. Evans, 115 S.Ct. 1185, (1995) (US).

Asbury Park Press, Inc. v. Department of Health, 558 A.2d 1363 (N.J. 1989).) (US).

Associated Film Distribution Corp. v. Thornburg, 520 F. Supp. 971 (E.D. Pa. 1981); rev'd and remanded on other grounds, 683 F.2d 808 (3d Cir. 1982), cert. denied, 480 U.S. 933 (1982) (US).

Beacon Journal Publishing v. Akron, 70 Ohio St. 3d 605, (1994) (US).

Bigelow v. Virginia, 421 U.S. 809, 95 S.Ct. 222, 44 L.Ed.2d 600, (1975) (US).

Bond v. Floyd, 385 U.S. 116 (1966) (US).

Boyd v. United States, 116 U.S. 616, (1886) (US).

Brandenburg v. Ohio, 395 U.S. 444, (1969) (US).

Breard v. Alexandria, 341 U.S. 622, 625-26, (1951) (US).

Brown v. Board of Education, 347 U.S. 483 (1954) (US).

Brown v. FBI, 658 F.2d 71, 75 (2d Cir. 1981) (US).

Buckley v. Valeo, (No. 75-436) No. 75-36, 171 U.S.App.D.C. 172, 519 F.2d 821, affirmed in part and reversed in part; No. 75-437, 401 F.Supp. 1235, affirmed, (1976) (US).

Burton v. Wilmington Parking Authority, 365 U.S. 715, (1961) (US).

Cahlin v. General Motors Acceptance Corporation, 936 F2d 1151 (11th Cir.

1991) (US).

California v. Ciraolo, 476 U.S. 207, (1986) (US).

California v. Greenwood, 486 U.S. 35, 108 S.Ct. 1625, 100 L.Ed.2d 30, (1988) (US).

Canterbury v. Spence, 464 F.2d 772 (D.C. Cir. 1972) (US).

Chaplinsky v. New Hampshire, 315 U.S. 568 (1942) (US).

Chevron v. NRDC, 467 US 837, (1984) (US).

Coates v. Cincinnati, 402 U.S. 611, (1971) (US).

Cohen v. California, 403 U.S. 15, (1971) (US).

Communist Party v. Subversive Activities Control Board, 367 U.S. 1, (1961) (US).

Comp Examiner Agency, Inc., dba 25th Century Internet Publishers, v. JURIS, INC., a Tennessee corporation, Defendant, No. 96-0213-WMB (CTx), (1996) (US).

Cox v. Riley, 83 Cr. App. R. 54 d, Queen's Bench Divisional Court, Hearing-Dates: 12 March, (1986) (US).

Dallas v. Staglin, 109 S.Ct. 1591, 1595, (1989) (US).

Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579, (1993) (US).

Davidson v. Dill, 503 P.2d 157, (1972) (US).

Deal v. Spears, 980 F.2d 1153, 1157-58 (8th Cir. 1992) (US).

Department of Air Force v. Rose, 425 U.S. 352, (1976) (US).

Dickerson v. Raphael, 222 Mich. App. 185 (Mich. Ct. App. 1997) (US).

Dietemann v. Time, 449 F. 2d 245, 248 (9th Cir. 1971) (US).

Doe v. Gonzales, 449 F.3d 415 (2d Cir. 2006) (US).

Dow Chemical v. United States, 476 U.S. 227, 106 S.Ct. 1819, 90 L.Ed.2d 226, (1986) (US).

Eastman Photographic Materials Co. v. Kodak Cycle Company, 15 R.P.C. 105, (1898) (US).

ECPA, Andersen Consulting LLP v. OUP and Bickel & Brewer, No. 97 C 5501, 1998 WL 30703 (N.D. Ill. Jan. 23, 1998) (US).

Edgar v. Mite Corporation, 457 U.S. 624, 631, (1982) (US).

Eisenstadt v. Baird, 405 U.S. 438, 92 S.Ct. 1029, 31 L.Ed.2d 349, (1972) (US).

Erickson v. Erickson, 246 Conn. 359, 716 A.2D 92 (Conn. 1998) (US).

Erven Warnink v. Townend, FSR 397, Lord Diplock, (1979) (US).

Federal Trade Commission v. Audiotex Communication, Inc. (2003), at http://www.Loundy.com/E-LAW_Links.html (accessed 20 May 2011).

Federal Trade Commission v. Zuccarini, No. CIV.A.01-CV4854, 2002 WL 1378421 at *2 (E.D. Pa Apr 9, 2002) (slip op.) (US).

Felsher v. University of Evansville, 755 N.E. 2d 589 (Ind. 2001) (US).

Florida Star v. B.J.F, 491 U.S. 524, (1989) (US).

Folsom v. Marsh, 2 Story 100, 111 (1841) (US).

Frohwert v. United States, , 249 U.S. 204 (1919) (US).

Frye v. United States, 293 F. 1013 (D.C. Cir, (1923) (US).

Gibson v Florida Legislative Investigation Committee, 372 U.S. 539, 548, (1963) (US).

Goldman v. United States, 316 U.S. 129, 138, (1942) (US).

Griswold v. Connecticut, 38 1 U.S. 479, 85 S.Ct. 1678, 14 L.Ed.2d 510, (1965) (US).

Handschu v. Special Services Division (NYPD), S.D.N.Y., Index No. 71 Civ. 2203 (CSH) (direct). 605 F.Supp. 1384 (D.C.N.Y. 1985). affirmd, 787 F.2d 828 (2d Cir. 1986) (US).

Hasbro, Inc., Plaintiff, v. Internet Entertainment Group, Ltd., et al., Defendants, 1996 U.S. Dist. LEXIS 11626, (1996) (US).

Henke v. United States Department of Commerce, 83 F.3d 1453, 1461 (D.C. Cir. 1996) (quoting Bartel v. FAA, 725 F.2d 1403, 1408 n.10 (D.C. Cir. 1984). (1996) (US).

Herrera v. Collins, 506 US 390, (1993) (US).

Hines v. Davidowitz, 312 U.S. 52, 67 (1941) (US).

Houston v. Hill, 482 U.S. 451, (1987) (US).

Humphrey's Executor v. United States, 295 U. S. 602 (1935) (US).

Hunt v. Bradshaw, 88 S.E. 2d 762 (N.C. 1955) (US).

Hunter v. Burroughs, 123 Va. 113, 96 S.E. 360, 366-368, (1918) (US).

In re Northwest Airlines Privacy Litigation, 2004 U.S. Dist. LEXIS 10580 (D. Minn., (2004) (US).

In re Pharmatrak, Inc. Privacy Litigation, 329 F.3d 9 (1st Cir. 2003) (US).

In re: Sealed Case, 310 F.3d 7817, 746 (Foreign Intelligence Surveillance Court of Review, (2002) (US).

Intercon v. Bell Atlantic Internet Solutions, 10 US Number 98-6428, (2000) (US).

Interstellar Starship Services Limited v. Epix, Inc., Civil No. 97-107-FR. Nov. 20, (1997) (US).

J. E. M. AG. Supply v Pioneer Hi-Bred International, 534 U.S. 124, 141-142. (1974) (US).

Jacobellis v. Ohio, 378 U. S. 184, 197 (Stewart J., concurring), (1964) (US).

Junger v. Daley, 2000 FED App. (6th Cir. 2000) (US).

Juno On-Line Services, L.P. v. Juno Lighting, Inc., 979 F. Supp 684 (N.D. Illl. 1997) (US).

Kasky v. Nike, Inc., 27 Cal. 4th 939 (2002) (US).

Katz v. United States, 389 U.S. 347, 88 S.Ct. 507, 19 L.Ed.2d 576, (1967) (US).

Kestenbaum v. Michigan State University, 327 N.W.2d 783, (1982) (US).

Kingsley Books, Inc. v. Brown, 354 U.S. 436, 447 (1957) (US).

Kolender v. Lawson, 461 U.S. 352, 358, (1983) (US).

Kyllo v. United States, 533 U.S. 27, 121 S.Ct. 2038, 150 L.Ed.2d 94, (2001) (US).

Lawrence v. Texas, 539 U.S. 558, 564, 123 S.Ct 2472, 156 L.Ed.2d 508, (2003) (US).

Liebling, Jeff, dba The "Lectric Law Library" v. Interlaw Limited, et. al. , U. S. District Court of Nevada [Case # N-96-107 DWH] (February 15, 1996) (US).

Lloyd & Henninger v. Marshall, 526 F.Supp. 485, 487 (M.D. Fla. 1981) (US).

Lopez v. United States 373 U.S. 471, (1963) (US).

Lorillard Tobacco Co. v. Reilly, 2000 U.S. Dist. LEXIS 862 (D. Mass., January 24, 2000) (US).

Loving v. Virginia, 388 U.S. 1, (1967) (US).

Mapp v. Ohio, 367 U.S. 644, (1961) (US).

Marbury v. Madison, 1 Cranch (5 U.S.) 137, (1803) (US).

Mc Donald v. Mabee, 243 U.S. 90, 91, (1917) (US).

McIntyre v. Ohio Election Commission, 115 S. Ct. 1511, 514 U.S. 334, (1995) (US).

McVeigh v. Cohen, 983 F. Supp 215 (D.D.C., (1998) (US).

Mead Data Central, Inc. v. Toyota Motor Sales, U.S.A., Inc., 875 F.2d 1026 (2d Cir. 1989) (US).

Melvin v. Reid, 112 Cal. App. 285, (1931) (US).

Miller v. California, 413 U.S. 15, 93 S.Ct. 2607, 37 L.Ed.2d 419 (1973), rehearing denied 414 U.S. 881, 94 S.Ct. 26, 38, L.Ed.2d 128 (1973) (US).

Minnis v. Department of Agriculture, 737 F.2d 784 (9th Cir. 1984) cert. denied 471 U.S. 1053, (1985) (US).

Miranda v. Arizona, 384 U.S. 436, (1966) (US).

Morton v. Mancari, 417 U.S. 535, 550 (2001) (US).

MTV Networks v. Curry, (867 F.Supp. 202 S.D.N.Y.) (US).

Multnomah County Medical Society v. Scott, 825 F.2d 1410 (9th Cir., (1987) (US).

Murray v. GMAC Mortgage Corporation, 434 F. 3d 948 (7th Cir. 2006) (US).

NAACP v. Alabama, 357 U.S. 449, 462, 78 S. Ct. 1163, 2 L. Ed. 2d 1488, (1958) (US).

NAACP v. Button, 371 U.S. 415, 432-433 (1963) (US).

Natanson v. Kline, 354 P.2d 671 (Kan. 1960) (US).

National Archives and Records Administration v. Allan J. Favish, et al., 124 S. Ct. 1570, (2004) (US).

National Association of Retired Federal Employees v. Horner, 879 F.2d 873 (D.C. Cir. 1989) (US).

National Cable & Telecommunications Association v. Federal Communications Commission, United States of America, Qwest Communications International Inc. and Verizon. (2009, February 13), at http://pacer.cadc.uscourts.gov/common/opinions/200902/07-1312-1164901.pdf (accessed 2 April 2011). (US)

National Cable & Telecommunications Association v. Federal Communications Commission, United States of America, Qwest Communications International Inc. and Verizon. (2009, February 13), at http://pacer.cadc.uscourts.gov/common/opinions/200902/07-1312-1164901.pdf (accessed 13 February 2011). (US)

New York Times v. Sullivan, 376 U.S. 254, 84 S.Ct. 710, 11 L.Ed.2d 83 (1964) (US).

Nixon v. Administrator of General Services, 433 U.S. 425, (1977) (US).

Norwood v Harrison 413 U.S. 455, (1973) (US).

Nutrition Physiology Corp. v. Enviros Ltd., N.D. Texas, No. 5:99-CV-0107-C, 3/9/00.) (US).

Oklahoma Press Publishing Company v. Walling, 327 U.S. 186, 66 S.Ct. 494, 90 L.Ed. 614, (1946) (US).

Olmstead v. U.S., 277 U.S. 438, 478 S. Ct. 564. 66 ALR 376, 72 L.Ed. 944, (1928) (US).

Osborn v. United States, 385 U.S. 323, 341, (1966) (US).

Panavision v. Network Solutions, 41 U.S.P.Q. 2d [BNA] 1310 [C.D. Cal. Entered Dec. 2, 1996]) (US).

Paramount Motor Works, Inc v. Gateway Marine, Inc., No. C 06-2703 1997 U.S. Dist. (N.D. Cal. Dec. 17,) (US).

Paul v. Davis, 424 U.S. 693, (1976) (US).

Paulsen v. Gundersen, 260 N.W. 448 (Wis. 1935) (US).

Pavesich v. New England Life Insurance Company, 122 Ga. 190; 50 S.E. 68; 1905 Ga. LEXIS 156, (1905) (US).

Peck v. the United Kingdom, (application no. 44647/98), (2003) (EU).

Pennoyer v. Neff, 95 U.S. 714, 722 (1878) (US).

Perry Education Association v. Perry Local Educators' Association, 460 U.S. 37, 45, (1983) (US).

Pittsburgh Press Company v, Pittsburgh Commission on Human Rights, 413 U.S. 376, 93 S.Ct. 2553, 37 L.Ed.2d 669 (1973), rehearing denied 414 U.S. 881, 94 S.Ct. 30, 38 L.Ed.2d 128 (1973) (US).

Planned Parenthood Federation of America, Inc. v. Bucci, 142 L. Ed. 2d 71: 67 U.S.L.W., 3231 (1998) (US).

Planned Parenthood v. ACLA, 41 F.Supp 2d 1130, D. Or. 1999) (US).

Playboy Enterprises, Inc. v. Calvin Designer Label, 985 F. Supp. 1220 [N.D. Cal.] (1997) (US).

Police Department of Chicago v. Mosley, 408 U.S. 92, 95-96, (1972) (US).

Pratt v. Davis 118 Ill. App. 161, (1905) (US).

ProCD Inc. v Zeidenberg. 86 F. 2d 1447 (7th Cir. 1996). (US), at http://floridalawfirm.com/procdinc.html (accessed 11 November 2011).

Procunier v. Martinez, 416 U.S. 396, 427 (Marshall, J., concurring), (1974)

(US).

Public Utilities Commission v. Pollak, 343 U.S. 451, 467, (1952) (US).

R.A.V. v. City of St. Paul, 505 U.S. 377, 382, (1992) (US).

Railroad Commission Cases, 116 U. S. 307, 331 (1886) (US).

Richmond Newspapers v. Virginia, 448 U.S. 555, (1980) (US).

Roe v. Wade, 410 U.S. 113, 93 S.Ct. 705, 35 L.Ed.2d 147, (1973) (US).

Roth v. United States, 354 U.S. 476 (1957) (US).

Safeco Insurance Company of America v. Burr, 551 U.S. 1, 127 S. Ct. 2201, 2213 (June 4, 2007) (US).

Salgo v. Leland Stanford Jr. University Board of Trustees, 317 P.2d 170, (1957) (US).

Santa Clara County v. Southern Pacific Railroad Company, 118 U.S. 394 - 417, (1886) (US).

Savage v. Jones, 225 U.S. 501, 533 (1912) (US).

Save the Yaak Committee v. Block, 840 F.2d 714 (9th Cir.), (1988) (US).

Schenck v. United States, 249 U.S. 47, 52, 63 L.Ed. 470, 473, 39 S. Ct. 247 (1919) (US).

Schloendorff v The Society of New York Hospital, 105 N.E. 92, (1914) (US).

Schuyler v. Curtis et al., 15 N.Y.S. 787, (1891) (US).

Scott v. Bradford, 606 P.2d 554, (1979) (US).

Shelton v. Tucker, 364 U.S. 479, (1960) (US).

Shirley v. Time, Inc., 45 Ohio App. 2d 69, 341 NE2d 337 (Ohio App. 1975) (US).

Sierra Club v. United State Forest Service, 843 F.2d 1190 (9th Cir. 1988) (US).

Silverman v. United States, 365 U.S. 505, 81 S.Ct. 679, 5 L.Ed.2d 734, (1961) (US).

Smith v. Goguen, 415 U.S. 566, 569, (1974) (US).

Smith v. Maryland, 442 U.S. 735, 99 S.Ct. 2577, 61 L.Ed2d 220, (1979) (US).

Smyth v. Pillsbury Company, 914 F. Supp. 97 (E.D. Pa. 1996) (US).

South Carolina v. Katzenbach, 383 U.S. 301, (1966) (US).

Spitzer vs. Network Associates D/B/A Mcafee 758 N.Y.S.2d 466 (2003) (US).

Stanley v. Georgia, 394 U.S. 557, 89 S.Ct. 1243, 22 L.Ed.2d 542, (1969) (US).

Step-Saver Data Systems, Inc. v. Wyse Technology and The Software Link, Inc., 939 F.2d 91, 3d Circuit, (1991) (US).

Steve Jackson Games, Inc. v. United States Secret Service, 816 F. Supp. 432 (W.D. Tex. 1993), *aff'd*, 36 F.3d 457 (5th Cir. 1994) (US).

Talley v. California, 362 U.S. 60, (1960) (US).

Tarasoff v. Regents of the University of California, 17 Cal. 3d 425, 551 P.2d 334, 131 Cal. Rptr. 14, (1976) (US).

Tavoulareas v. Washington Post, 724 F2d 1010, (1984) (US).

Tbornburgh v. American College of Obstetricians & Gynecologists, 476 U.S. 747 (1986) (US).

TCE, 1996 – The Comp Examiner Agency, Inc. d/b/a 25th Century Internet Publishers v. Juris, Inc., U.S. District Court, Central District of California, 96 CV 0213-WMB [CTx] April 23, 1966) (US).

Tehan v. Shott, 382 U.S. 406, 86, S.Ct. 459, 15 L.Ed.2d 453, (1966) (US).

Terry v. Ohio, 392 U.S. 1, (1968) (US).

The Federal Trade Commission v. James J. Rapp, Regana L. Rapp, d/b/a/ Touch Tone Information, Inc., (Civil Action No. 99-WM-783) (2000) (US).

Theodore v. Ellis, 141 La. 709, 75 So. 655, 660, (1917) (US).

TicketMaster Corp. v. Microsoft Corp. , *Computer & Online Industry Litigation Report,* 24,144 (April. 28, 1997) (US).

Time Inc v. Hill, 385 U.S. 374, 383, (1967) (US).

Truck Equipment Serv. Co. v. Fruehauf Corporation, 536 F.2d 1210 (8th Cir.), cert. denied, 429 U.S. 861, (1976) (US).

Turner Broadcasting System v. Federal Communications Commission, 114 S. Ct. 2445-2459 (1994) (US).

U. S. Department of Defense v. Federal Labor Relations Authority, 114 S.Ct. 1006, (1994) (US).

U.S. Department of Justice v. Reporters Committee for Freedom of the Press, 489 U.S. 749, (1989) (US).

U.S. v. Czubinski, 106 F3d 1069 (1st Cir.), (1997) (US).

U.S. v. Oakland Cannabis Buyers Corporation, 532 U.S. 483, 494, (2001) (US).

U.S. v. Playboy Entertainment Group, Inc., 30 F. Supp. 2d 702, affirmed. May

22) (US).

United States Department of Justice v. Reporter's Committee for Freedom of the Press, 489 US 749, 109 S. Ct. 1468, (1989) (US).

United States v. Aluminum Company of America, 148 F.2d 416, 443 (2d Cir. 1945)) (US).

United States v. Auler, 539 F.2d 642 (7th Cir. 1976) (US).

United States v. Brown, 381 U.S. 437 (1965) (US).

United States v. Carolene Products, 304 U.S. 144 (1938) (US).

United States v. Karo, 468 U.S. 705, 104 S.Ct. 3296, 82 L.Ed.2d 530, (1984) (US).

United States v. Kennedy, 81 F. Supp. 2nd 1103 (D. Kan., (2000) (US).

United States v. Miami University, 91 F.Supp.2d 1132, 1147 (S.D. Ohio 2000) (US).

United States v. Miller, 425 U.S. 435, 96 S.Ct. 1619, 48 L.Ed.2d 71, (1976) (US).

United States v. New York Telephone Company, 434 U.S. 159, 98 S.Ct. 364, 54 L.Ed.2d 376, (1977) (US).

United States v. O'Brien, 391 U.S. 367, (1968) (US).

United States v. Scarfo, 180 F. Supp. 2d 572 (D.N.J. 2001) (US).

United States v. Steel Company, 334 U.S. 495, 536 (1948) (US).

United States v. United States District Court, 407 U.S. 297, 92 S.Ct. 2125, 32 L.Ed.2d 752, (1972) (US).

US West v. FCC, 182 F.3d 1224 (10 Cir. 1999) (US).

Valentine v. Chrestensen, 316 U.S. 52, 54, 62 S. Ct. 920, 921, 86 L.Ed. 1262, (1942) (US).

Vault Corp. v. Quaid Software Ltd., 847 F.2d 255 (5th Cir.), (1988) (US).

Vega-Rodriguez v. Puerto Rico Tel. Co., 110 F.3d 174 (1st Cir. 1997) (US).

Vega-Rodriguez v. Puerto Rico Telephone. Company 110 F.3d 174 (1st Cir. 1997) (US).

Virginia State Board of Pharmacy v. Virginia Citizens Council, Incorporated, 425 U.S. 748, 96 S.Ct. 1817, 48 L.Ed.2d 346, (1976) (US).

Walker v. Carnival Cruise Lines, 63 F. Supp. 2d 1083, 1089 (N.D. Cal. 1999) (US).

Wall v Brim, 138 F.2d 478 (5th Cir. 1943) (US).

Waynick v. Reardon, 72 S.E.2d 4 (N.C. 1952) (US).

West Virginia Board of Education v. Barnette, 319 U.S. 624 (1943) (US).

Whalen v. Roe, 429 U.S. 589, (1977) (US).

Wheaton v. Peters, 33 U.S. 591, 8 L.Ed. 1055, (1834) (US).

Wheeling Steel Corporation v. Glander, 337 U.S. 562, (1949) (US).

Whitney v. California, 274 U.S. 357, 375-77, (1927) (US).

Wickard v. Filburn 317 U.S. 111, 129 (1942) (US).

Wine Hobby USA, Inc. v. IRS, 502 F.2d 133 (3d Cir. 1983).) (US).

Wisconsin v. Mitchell, 508 U.S. 476 (1993) (US).

Wojciechowski v. Coryell, 217 S.W. 638, 644 (Mo.App, (1920) (US).

Wooley v. Maynard, 430 U.S. 705, 714, (1977) (US).

Zurcher v. Stanford Daily. 436 U.S. 457, 98 S. Ct. 1970, 56 L. Ed. 2d 525, (1978) (US).

Table of Authorities

Table of Regulations and Statutes

***Australia* (AU)**

Australia Act 1986 Chapter 2 (1986) (AU, UK).

Charter of Human Rights and Responsibilities Act 2006 (Vic) amend. No. 43 of 2006 (2006) (AU).

Commonwealth of Australia Constitution Act 1900 (Imp), 63 & 64 Victoria, c 12 (Imp.) (1900) (AU).

Commonwealth of Australia Constitution Act as amended. (2003), at http://www.aph.gov.au/senate/general/constitution/par5cha1.htm (accessed 7 January 2011).

Constitution Act 1902, Act 32 of 1902. (NSW) (1902), at http://www.austlii.edu.au/au/legis/nsw/consol_act/ca1902188/ (accessed 16 February 2011).

Constitution of Queensland 2001, Act No. 80 of 2001. (2001), at http://www.legislation.qld.gov.au/LEGISLTN/ACTS/2001/01AC080.pdf (accessed 16 February 2011).

Criminal Law (Rehabilitation of Offenders) Act 1986 (Qld) (1986) (AU).

Criminal Records Act of 1991 (NSW). (1991), at http://www.austlii.edu.au/au/legis/nsw/consol_act/cra1991167/ (accessed 7 January 2011).

Criminal Records spent Convictions) Act 1992 (NT). (1992), at http://www.austlii.edu.au/au/legis/nt/consol_act/crca368/ (accessed 8 January 2011).

Health Records Act (HRA) 2001 (Vic) amend. No. 2 of 2001 (2001) (AU).

Health Records and Information Privacy Act of 2002 (NSW). (2002), at http://www.informationcommissioner.nsw.gov.au/lawlink/privacynsw/ll_pnsw.nsf/pages/PNSW_03_hripact (accessed 1 January 2011).

Human Rights Act 2004. (Act) (2004, amended 2010), at http://www.legislation.act.gov.au/a/2004-5/current/pdf/2004-5.pdf (accessed 27 July 2011).

Information Act 2002 amend 2009 (NT). (2002), at

http://www.austlii.edu.au/au/legis/nt/consol_act/ia144.txt (accessed 8 January 2011).

Information Privacy Act of 2000 (Vic-AU) amend. No. 98 of 2000 (2000) (AU).

Information Privacy Act of 2009 (Qld). (2009), at http://www.austlii.edu.au/au/legis/qld/consol_act/ipa2009231.txt/cgi-bin/download.cgi/download/au/legis/qld/consol_act/ipa2009231.txt (accessed 9 January 2011).

Listening and Surveillance Devices Act (SA AU). (1972), at http://www.austlii.edu.au/au/legis/sa/consol_act/lasda1972326/index.html (accessed 12 February 2011).

Listening Devices Act of 1991 (Tas AU). (1997), at http://www.austlii.edu.au/au/legis/tas/consol_act/lda1991181/ (accessed 11 February 2011).

National Consumer Credit Protection Act. (2009), at http://www.treasury.gov.au/consumercredit/content/legislation.asp The actual code is at http://www.comlaw.gov.au/ComLaw/Legislation/Act1.nsf/0/151D9CCDD6F2FAC1CA25768E001B64CC?OpenDocument (accessed 26 July 2011).

Privacy Act of 1988 (Cwlth) amend. Act No. 119 of 1988, Act No. 102 of 2009 (1988) (AU).

Privacy and Personal Data Protection Act 1998 (NSW). (1998), at http://www.austlii.edu.au/au/legis/nsw/consol_act/papipa1998464/ (accessed 7 January 2011).

Privacy Committee Act of 1975 (NSW). (1975), at http://www.worldlii.org/int/other/PrivLRes/1995/3/51_2_1.html (accessed 7 January 2011).

Queensland, *Invasion of Privacy Act 1971 (Qld)*. (2002), at http://www.legislation.qld.gov.au/LEGISLTN/CURRENT/I/InvasOfPrivA71.pdf (accessed 9 January 2011).

South Australia, *Constitution Act 1934*. (1934), at http://www.legislation.sa.gov.au/LZ/C/A/CONSTITUTION%20ACT%201934/CURRENT/1934.2151.UN.PDF (accessed 16 February 2011).

Spent Convictions Act 1988 (WA) (1988) (AU).

Surveillance Devices Act 1999 (Vic) amend. Act No. 21/1999 (1999) (AU).

Surveillance Devices Act of 1998 (WA AU). (1998), at http://www.austlii.edu.au/au/legis/wa/consol_act/sda1998210/ (accessed 12 February 2011).

Surveillance Devices Act of 2007 (NT AU). (2007), at http://www.austlii.edu.au/au/legis/nt/consol_act/sda2007210/ (accessed 12 February 2011).

***Canada* (CA)**

Canadian Environmental Protection Act (CEPA) amend. c. 15.31 (1999) (CA).

Certain Personality Rights amend. Civil Code of Quebec, Chapter III: Respect of Reputation and Privacy, 35-41, (S.Q. 1991, c.64) (1991) (CA).

Civil Code of Quebec amend. 1991, c. 64, a. 35; 2002, c. 19, s. 2. (1991) (CA).

Environmental Assessment Act (CEAA) amend. S.C. 1992, c. 37 (1992) (CA).

Ontario Health Care Consent Act amend. c. 10, Sched. R, s. 14 (1996) (CA).

Personal Health Information Act. SNL2008. c. P-7.01. (2010), at http://www.assembly.nl.ca/legislation/sr/statutes/p07-01.htm (accessed 17 July 2011). (SJNL CA).

Personal Health Information Protection Act, 2004. S.O. 2004, c. 3. (2010), at http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_04p03_e.htm (accessed 17 July 2011).

Pest Control Products Act (PCPA) amend. S.C. 2002, c. 28 (2002) (CA).

Privacy Act (R.S., 1985, c. P-21). (1985), at http://laws.justice.gc.ca/en/P-21/ (accessed 6 July 2011).

Right to Information Act Chapter R-10.3. (1978), (NB CA) at http://www.gnb.ca/0062/PDF-acts/r-10-3.pdf (accessed 8 July 2011).

Statutes of Canada 2010; Chapter 23: Anti-Spam amend. Third Session, Fortieth Parliament, 59 Elizabeth II, 2010 (2010) (CA).

***Republic of South Africa* (SA)**

Constitution of the Republic of South Africa 1996. (SA).
Consumer Protection Act 68 of 2008 (SA).
Copyright Act 98 of 1978 (SA).
Electronic Communications and Transactions Act 25 of 2002 (SA).
National Credit Act 34 of 2005 (SA).
Open Democracy Bill B 67-98 of 1999 (SA).
Promotion of Access to Information Act 2 of 2000 (SA).
Protection of Information Bill 6 of 2010 (SA).
Protection of Personal Information Bill 9 of 2009 (SA).
Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002 (SA).

***United Kingdom* (UK)**

British Race Relations Act of 1965 amend. ch. 73 § 6(1), as amended in 1976 and 1986 (1986) (UK).
Data Protection Act of 1998 amend. Chapter 29 (1998) (UK).
European Communities Act 1972 (c. 68) (1972) (UK).
Fox's Libel Act, 32 Geo. 3, c. 60 (1792) (UK).
Government of Wales Act 2006 Chapter 32 (2006) (UK).
Justices of the Peace Act amend. (Eng.). 34 Edw. 3, c. 1. (1361) (UK).
Regulation of Investigatory Powers (Scotland) Act 2000 asp 11 (2000) (UK).
Scotland Act 1998 Chapter 46 (1998) (UK).
The Consumer Protection Act 1987 (Commencement No. 1) Order 1987 (1987) (UK).

***United States* (US)**

Atomic Energy Act of 1946 amend. 68 Stat. 919; 42 U.S.C. § 2011-296 (1946) (US).
Cable Communication Policy Act amend. 47 U.S.C. § 551 (1984) (US).
Cable Television Consumer Protection and Competition Act amend. 18 U.S.C. § 2710-2711 (1992, 1994) (US).
California Financial Information Privacy Act amend. California Finance Code

§§ 4050-4060 (2003) (US).

California Health and Safety Code § 130200-130203 (US).

California Invasion of Privacy to Capture Physical Impression Act amend. California Penal Code,§ 632, subd. (a) (1989) (US).

California Penal Code. § 633 (2006) (US).

Children's Online Privacy Protection Act of 1998 (COPPA) amend. 15 U.S.C. §§ 6501-6506 (1998) (US).

Communications Act of 1934 amend. ch. 652, § 605, 48 Stat. 1064 (codified as amended at 47 U.S.C. § 605) (1934) (US).

Computer Fraud and Abuse Act (CFAA) amend. 18 U.S.C. § 1030 (1994) (US).

Computer Matching and Privacy Protection Act amend. 5 USC 552a (1988) (US).

Computer Matching and Privacy Protection Act of 1988 amend. 5 U.S.C sec. 552a (1988) (US).

Copyright Act amend. 17 U.S.C. §§ 101 - 810 (1976) (US).

Digital Telephony Act aka, Communications Assistance for Law Enforcement Act 1994 amend. 18 USC 2510-2522 (1994) (US).

E-government Act amend. (Pub.L. 107-347, 116 Stat. 2899, 44 U.S.C. § 101, H.R. 2458/S. 803) (2002) (US).

Electronic Communications Privacy Act amend. (ECPA Title I) 18 U.S.C.A. §§ 2510-2521 (1986) (US).

Fair and Accurate Credit Transaction Act, amend. 15 U.S.C.A. § 1681 (2003) (US).

Fair Credit Reporting Act (FCRA) amend. Public Law No. 91-508 (1970) (US).

Family Educational Rights and Privacy Act (FERPA) amend. 20 U.S.C. § 1232g; 34 CFR Part 99 (1974) (US).

Federal Power Act amend. 16 U.S.C. §§ 791a-797, 798-824a, and 824b-825r, June 10, 1920, as amended 1930, 1935, 1936, 1948, 1949, 1951, 1953, 1956, 1958, 1960, 1962, 1968, 1970, 1978, 1980, 1982, 1986, 1988, 1990-1992 and 1996. (1920) (US).

Federal Telecommunications Act amend. (18 USC 2511(2)(a) (1996) (US).

Federal Trade Commission (FTC) amend. See 16 C.F.R. 701 ("the Disclosure Rule") and 16 C.F.R. 702 ("the Pre-Sale Availability Rule") (2000) (US).

Federal Trade Commission Act, 15 U.S.C. § 41 (1914) (US).

Foreign Intelligence Surveillance Act (FISA) amend. Public Law 95-511, 92 Stat. 1783 (1978) (codified at 50 U.S.C. § 1801-1811) (1978) (US).

Freedom of Information Act amend. 5 U.S.C. sec. 552(b)(6)(7) (1974) (US).

Freedom of Information Act amend. 5 USC, 552 (2005) (US).

Gramm-Leach-Bliley Act aka Financial Services Modernization Act amend. Pub. L. No. 106-102, 113 Stat. 1338 (1999) (US).

Health Insurance Portability and Accountability Act (HIPAA) amend. 42 U.S.C. § 1320 (1996) (US).

Higher Education Amendments amend. Public Law No. 102-325, § 1555(a), 106 Stat. 448, 840 (1992) (US).

Information Practices Act amend. California Civil Code, § 1798 (1977) (US).

Inventions Secrecy Act of 1951 amend. 35 U.S.C. §§ 181-88 (1951) (US).

Lanham Act amend. 15 U.S.C.1127 (1994) (US).

Mail Fraud Act amend. 39 U.S.C. § 3623 (1994), 39 C.F.R. § 233.3 (1996) (US).

National Research Act amend. 45 CFR 46 (1974) (US).

Omnibus Crime Control and Safe Streets Act amend. Pub. L. No. 90-350, 82 Stat. 197 18 U.S.C. § 2511-2520) (1968) (US).

Pen Register and Trap and Trace Device Use amend. 18 U.S.C. II, 206, § 3121 (1984) (US).

Presidential Recordings and Materials Preservation Act (PRMPA) amend. 44 U.S.C. § 2111 (1974) (US).

Presidential Recordings and Materials Preservation Act amend. 44 U.S.C. § 2107 (1970 ed., Supp. V). (1974) (US).

Privacy Act of 1974 amend. 5 U.S.C. § 552(a)(4) (1974) (US).

Privacy Protection Act amend. 42 U.S.C. § 2000(a)(a) *et seq* (1980) (US).

Public Records Act, *California Government Code, 6250.* (1996), at http://caselaw.lp.findlaw.com/cacodes/gov/6250-6270.html (accessed 10 September 2011).(US).

Restatement (Second) of Conflict of Laws § 187 Author. (2003), at http://www.nccusl.org/pressrel/UCITAQA.HTM#_edn26 (accessed 5 September 2011).

Restatement of American Common Law. (2002), at http://www.ali.org/ali/newprds.htm (accessed 20 November 2011).

Restatement of Contracts 2d. . (1979), at http://www.law.onu.edu/review/contracts/warner/rsk/71.html § 71 http://www.law.onu.edu/review/contracts/warner/rsk/90.html § 90 http://www.law.onu.edu/review/contracts/warner/rsk/344.html § 344 (accessed 10 November 2011).

Right to Financial Privacy Act amend. 18 U.S.C. §§ 3401 3422 (1978) (US).

Sarbanes-Oxley Act . Corporate Responsibility amend. 15 USC 7201 (2002) (US).

Stored Communications Act amend. 18 U.S.C. 121, 2702 (1986) (US).

Telecommunications Act of 1996 amend. Pub. LA. No. 104-104, 110 Stat. 56 (1996) (US).

The Freedom of Information Act amend. 5 U.S.C. § 552 (1966) (US).

Trademark (Lanham) Act amend. ch. 540, 60 Stat. 427. (codified as amended at 15 U.S.C. 1051-1127 (1994) (1946) (US).

Trademark Law Revision Act amend. Pub. L. No. 100-667, 102 Stat. 3935. 15 U.S.C.1051-1127 (1994) (US).

United States Code Congressional and Administrative News (USCCAN) amend. 102 Stat. 3935, 5603 (1988) (US).

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act) amend. Public Law No. 107-56, 115 Stat. 272 (codified at 50 U.S.C. § 1804(a)(7)(B)) (2001) (US).

US Federal Information Policy amend. 44 U.S.C § 3542 (b)(1) (2006) (US).

Video Privacy Protection Act. Pub L. No, 104-104 § 222, 110 Stat. 56 (US). (1966), at http://www.law.cornell.edu/uscode/18/2710.shtml (accessed 21 September 2011).

Table of Authorities

Table of International Conventions, Declarations, and Treaties – Alphabetical

African Commission on Human and Peoples' Rights, *Declaration of Principles on Freedom of Expression in Africa*. (2002), at http://www.achpr.org/english/declarations/declaration_freedom_exp_en.html (accessed 21 January 2012).

Article 29 Data Protection Working Party, *Opinion 3/2009 on the Draft Commission Decision on Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries, under Directive 95/46/EC*. (2009), at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp161_en.pdf (accessed 26 December 2011).

Article 29 Data Protection Working Party, *Working Document on Data Protection Issues Related to RFID Technology (10107/05/EN-WP 105)*. (2005), at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp105_en.pdf (accessed 29 August 2011).

Article 29 Data Protection Working Party, *Working Document Setting Up a Table with the Elements and Principles to be Found in Binding Corporate Rules (1271-00-00/08/EN-WP 153)*. (2008), at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp153_en.pdf (accessed 26 December 2011).

Asia-Pacific Economic Cooperation, *APEC Privacy Framework*. (2004, November 17-18), at http://www.nacpec.org/docs/APEC_Privacy_Framework.pdf (accessed 21 December 2011).

Asia-Pacific Economic Cooperation, *What is Asia-Pacific Economic Cooperation?* (2009), at http://www.apec.org/apec/about_apec.html (accessed 10 October 2011).

Council of Europe, *Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data,*

regarding supervisory authorities and transborder data flows. (2001), at http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=181&CM=1&DF=11/5/2008&CL=ENG (accessed 4 March 2011).

Council of Europe, *Convention for the Protection of Human Rights and Fundamental Freedoms*. (1950), at http://conventions.coe.int/treaty/en/Treaties/Html/005.htm (accessed 20 August 2011).

Council of Europe, *Convention for the Protection of Human Rights and Fundamental Freedoms*. (2009), at http://conventions.coe.int/treaty/en/Treaties/Html/005.htm (accessed 5 August 2011).

Council of Europe, *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data: Strasbourg, 28.I.1981*. (1981), at http://conventions.coe.int/Treaty/EN/Treaties/Html/108.htm (accessed 15 January 2011).

Council of Europe, *Council of Europe's Convention on the Automated Processing of Personal Data* (2004), at http://www2.echo.lu/legal/en/dataprot/counceur/conv.html (accessed 29 May 2011).

Council of Europe, *Model Contract*. (2006), at http://www.coe.fr/DataProtection/ectype.htm (accessed 23 August 2011).

Council of Europe, *Resolution (73) 22 on the Protection of the Privacy of Individuals vis-àvis Electronic Data Banks in the Private Sector*. (1973), at http://www.coe.int/t/e/legal_affairs/legal_co%2Doperation/data_protection/documents/international_legal_instruments/Resolution(73)22_EN.pdf (accessed 20 January 2011).

Council of Europe, *Resolution (74) 29 on the Protection of the Privacy of Individuals vis-à-vis Electronic Data Banks in the Public Sector*. (1974), at http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Data_protection/Documents/International_legal_instruments/Resolution %2874%29 29.asp - TopOfPagehttp://www.coe.int/T/E/Legal_affairs/Legal_co-

operation/Data_protection/Documents/International_legal_instruments/Resolution %2874%29 29.asp - TopOfPage (accessed 22 January 2011).

Council of the European Union, *Agreement between the European Community and the Government of Canada on the processing of API/PNR data (2006/230/EC)*. (2005), at http://ec.europa.eu/justice_home/fsj/privacy/docs/adequacy/pnr/canada_ec_230_2006_en.pdf (accessed 26 December 2011).

Council of the European Union, *Council Decision 2007/551/CFSP/JHA of 23 July 2007 on the signing, on behalf of the European Union, of an Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS) (2007 PNR Agreement) (*(2007, August 4), at http://eur-lex.europa.eu/LexUriServ/site/en/oj/2007/l_204/l_20420070804en00160017.pdf (accessed 28 September 2011).

Council of the European Union, *Council Regulation (EC) No 2252/2004 of 13 December 2004 on Standards for Security Features and Biometrics in Passports and Travel Documents Issued by Member sSates*. (2004, December 29), at http://dematerialisedid.com/PDFs/l_38520041229en00010006.pdf (accessed 28 September 2011).

Court of Justice of the European Communities (Including Court of First Instance Decisions), *Lindquist (Approximation of laws) [2003] EUECJ C-101/01 (06 November 2003) [2004] QB 1014, C-101/01, [2003] EUECJ C-101/01, [2004] All ER (EC) 561 (*(2004), at http://www.bailii.org/eu/cases/EUECJ/2003/C10101.html (accessed 28 September 2011).

Court of Justice, *European Parliament v Council of the European Union. (Joined Cases C-317/04 and C-318/04). (2006/C 178/02)*. (2006), at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2006:178:0001:0002:EN:PDF (accessed 29 May 2011).

Court of Justice, *Rechnungshof v. Österreichischer Rundfunk and Others and Christa Neukomm and Joseph Lauermann v. Österreichischer RundfunkJoined Cases C-465/00, C-138/01 and C-139/01*. (2003), at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62000J0465:EN:HTML (accessed 29 May 2011).

European Commission, *General Data Protection Regulation*. (2012), at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf (accessed 25 January 2012).

European Commission, *General Data Protection Regulation: Impact Assessment*. (2012), at http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_en.pdf (accessed 25 January 2012).

European Commission, *How Will the "Safe Harbor" Arrangement for Personal Data Transfers to the US Work?* (2009), at http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/adequacy-faq1_en.htm (accessed 26 December 2011).

European Commission, *Regulation of the European Parliament and of the Counsel on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data (General Data Protection Regulation)*. (2012), at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf (accessed 11/3).

European Commission, *Submission to the House of Representatives Committee on Legal and Constitutional Affairs Concerning its Inquiry into the Privacy Amendment (Private Sector) Bill 2000. MARKT/E1//FB/fb D(2000)*. (2000), at http://www.aph.gov.au/house/committee/laca/Privacybill/sub113.pdf (accessed 30 December 2011).

European Commission, *US-EU Safe Harbor Frameworks*. (2011), at http://export.gov/safeharbor/index.asp (accessed 4 August 2011).

European Convention of Human Rights and Fundamental Freedoms, *European Convention of Human Rights and Fundamental Freedoms*.

(1950), at http://conventions.coe.int/treaty/en/Treaties/Html/005.htm (accessed 24 September 2011).

European Council, *The Hague Programme: Strengthening Freedom, Security and Justice in the European Union*, *Official Journal of the European Union*, C 53(1), pp 1-14. (2005), at http://eurocrim.jura.uni-tuebingen.de/cms/en/doc/557.pdf (accessed 10 September 2011).

European Data Protection Supervisor, *Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council on the Follow-Up of the Work Programme for Better Implementation of the Data Protection Directive*, Official Journal of the European Union, 27.10.2007, C 255/1 - 14. (2007, July 25), at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2007:255:0001:0012:EN:PDF (accessed 22 September 2011).

European Parliament Council - Commission on Risk Assessment and Risk Management, *Charter of Fundamental Rights of the European Union (2007/C 303/01)*. (2007), at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2007:303:0001:0016:EN:PDF (accessed 21 December 2011).

European Parliament, *Charter of Fundamental Rights of the European Union (2000/C 364/01)*. (2000), at http://www.europarl.europa.eu/charter/pdf/text_en.pdf (accessed 5 August 2011).

European Patent Office, *Persistent Client State in a Hypertext Transfer Protocol Based Client-Server System. European G06F17/30W9; H04L29/08N1; USA US19950540342 19951006* (1998, June 30), at http://v3.espacenet.com/publicationDetails/biblio?CC=US&NR=5774670&KC=&FT=E (accessed 5 January 2011).

European Union Directives, *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications)*. (2002), at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:

HTML (accessed 4 January 2011).

European Union Directives, *Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC*. (2006), at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF (accessed 4 September 2011).

European Union Directives, *European Union Protection Directive*. (2004), at http://www2.echo.lu/legal/en/dataprot/directiv/directiv.html (accessed 27 May 2011).

European Union Directives, *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data* (1995), at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML (accessed 4 January 2011).

OECD, *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*. (1980), at http://www.olis.oecd.org/horizontal/oecdacts.nsf/linkto/C(80)58 (accessed 22 January 2011).

OECD, *Implementing the OECD "Privacy Guidelines" in the Electronic Environment: Focus on the Internet. DSTI/ICCP/REG(97) 6/FINAL.* (1997), at http://www.oecd.org/dataoecd/33/43/2096272.pdf (accessed 20 July 2011).

Organization for Economic Co-Operation and Development, *Guidelines for Consumer Protection in the Context of Electronic Commerce*. (2002), at http://www.oecd.org/dataoecd/18/13/34023235.pdf (accessed 6 January 2011).

Organization of American States, *American Convention on Human Rights*. (1969), at http://www.hrcr.org/docs/American_Convention/oashr.html (accessed 10 June 2011).

Organization of American States, *American Declaration of the Rights and*

Duties of Man. (1948), at http://www.oas.org/juridico/english/ga-Res98/Eres1591.htm (accessed 10 June 2011).

United Nations, *Convention on the Recognition and Enforcement of Foreign Arbitral Awards*. (1958), at http://www.uncitral.org/pdf/english/texts/arbitration/NY-conv/XXII_1_e.pdf (accessed 20 August 2011).

United Nations, *Convention on the Rights of the Child. UN General Assembly Document A/RES/44/25*. (1989), at http://www.cirp.org/library/ethics/UN-convention/ (accessed 20 August 2011).

United Nations, *Guidelines Concerning Computerized Personal Data Files. Adopted by the General Assembly on 14 December 1990.* (1990), at http://ec.europa.eu/justice_home/fsj/privacy/instruments/un_en.htm (accessed 3 January 2011).

United Nations, *International Convention on the Protection of the Rights of All Migrant Workers and Members of their Families*. (1990), at http://www.un.org/documents/ga/res/45/a45r158.htm (accessed 20 August 2011).

United Nations, *International Covenant on Civil and Political Rights, (ICCPR). Article 17*. (1966), at http://www2.ohchr.org/english/law/ccpr.htm (accessed 20 August 2011).

United Nations, *Universal Declaration of Human Rights* (1948), at http://www.hrweb.org/legal/udhr.html (accessed 20 August 2011).

World Intellectual Property Organization, *WIPO Copyright Treaty*. (1996), at http://www.wipo.int/treaties/en/ip/wct/trtdocs_wo033.html (accessed 15 June 2011).

Table of Governmental Documents

Australia (AU)

Australian Government Department of the Prime Minister and Cabinet, *Administrative Arrangements*, Australian Government (2011 October), at http://www.dpmc.gov.au/privacy/causeofaction/ (accessed 20 October 2011).

Australian Government Office of the Privacy Commissioner, *Credit Reporting Fact Sheet 7: Credit Reporting Databases (May 1996)*. (2009), at http://www.privacy.gov.au/materials/types/factsheets/view/6494 (accessed 16 February 2011).

Australian Government Office of the Privacy Commissioner, *Issues Paper: A Commonwealth Statutory Cause of Action for Serious Invasion of Privacy; Submission to the Attorney-General's Department*, Author. (2011), at http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/%289A5D88DBA63D32A661E6369859739356%29%7E14B+-+Office+of+the+Australian+Information+Commissioner+-+Word.pdf/$file/14B+-+Office+of+the+Australian+Information+Commissioner+-+Word.pdf (accessed 12 December 2011).

Australian Government, *Australian Government*. (2010), at http://australia.gov.au/ (accessed 5 August 2011).

Australian Government, *Australian Privacy Principles: Companion Guide*, Author. (2010 June), at http://www.aph.gov.au/senate/committee/fapa_ctte/priv_exp_drafts/Guide/companion_guide.pdf (accessed 26 June 2011).

Australian Government, *Australian Privacy Principles: Exposure Draft*. (2010), at http://www.aph.gov.au/senate/committee/fapa_ctte/priv_exp_drafts/Guide/exposure_draft.pdf (accessed 26 June 2011).

Australian Human Rights Commission, *About the Commission*. (2010), at http://www.hreoc.gov.au/about/index.html (accessed 27 July 2011).

Australian Office of the Federal Privacy Commission, *Information Privacy*

Principles. (2009), at http://www.privacy.gov.au/materials/types/law/view/6892 (accessed 27 December 2011).

Australian Office of the Federal Privacy Commission, *Privacy and Business*. (2001, July), at http://www.privacy.gov.au/publications/rbusiness.html (accessed 5 January 2011).

Australian Privacy Foundation, *Recommendations for Improvements to APEC Privacy Principles (Version 9)*. (2004), at http://www.privacy.org.au/Papers/APEC0403.html (accessed 29 July 2011).

Commonwealth of Australia Law, *Market and Social Research Privacy Code*. (2003), at http://www.comlaw.gov.au/comlaw/legislation/legislativeinstrument1.nsf/framelodgmentattachments/0671CDE24C557D58CA257309000A399E (accessed 29 December 2011).

Commonwealth of Australia, *Privacy Amendment (Private Sector) Act 2000. Act - C2004A00748*. (2000), at http://www.comlaw.gov.au/ComLaw/Legislation/Act1.nsf/0/3E8F716C0779E822CA256F72000B40F8?OpenDocument (accessed 29 December 2011).

Commonwealth of Australia, *Privacy Amendment Act of 2004*. (2004), at http://www.austlii.edu.au/au/legis/cth/consol_act/paa2004188/sch1.html (accessed 29 December 2011).

Government of Australia, *High Court of Australia*. (2010), at http://www.hcourt.gov.au/ (accessed 5 August 2011).

Government of Australia, *Parliament of Australia*. (2010), at http://www.aph.gov.au/ (accessed 5 August 2011).

Government of Australia, *Prime Minister of Australia*. (2010), at http://www.pm.gov.au/ (accessed 5 August 2011).

Government of South Australia, *Information Privacy Principles (IPPs) Instruction, and Premier and Cabinet Circular 12, as amended by Cabinet 18 May 2009 (SA-AU)*. (1989), at http://www.premcab.sa.gov.au/pdf/circulars/pc12_privacy.pdf (accessed 9 January 2011).

High Court of Australia, *About the Court*. (2010), at http://www.hcourt.gov.au/about.html (accessed 5 July 2011).

Office of the Australian Information Commissioner, *Privacy Impact Assessment Guide (Revised May 2010)*. (2010), at http://www.oaic.gov.au/publications/guidelines/Privacy_Impact_Assessment_Guide.html (accessed 20 June 2011).

Parliament of New South Wales, *Legislation Review Committee: Strict and Absolute Liability*. (2006), at http://www.parliament.nsw.gov.au/Prod/parlment/committee.nsf/0/88212f7a0a84b436ca2571870022bc55/$FILE/Strict%20and%20Absolute%20Liability%20Discussion%20Paper.pdf (accessed 6 December 2011).

Tasmania Ombudsman, *Personal Information Protection*. (2009), at http://www.ombudsman.tas.gov.au/personal_information_protection (accessed 9 January 2011).

Tasmania, *Constitution Act 1934, Act 94 of 1934; Royal Assent 14 January 1935*. (1934), at http://www.austlii.edu.au/au/legis/tas/consol_act/ca1934188/ (accessed 16 February 2011).

Tasmanian Legislation, *Personal Information Protection Act 2004 (Tas)*. (2004), at http://www.thelaw.tas.gov.au/tocview/index.w3p;cond=;doc_id=46%2B%2B2004%2BAT%40EN%2B20100110130000;histon=;prompt=;rec=;term= (accessed 9 January 2011).

Victoria Government, *Charter of Human Rights and Responsibilities Act 2006*. (2006, amended 2010), at http://www.austlii.edu.au/au/legis/vic/consol_act/cohrara2006433/ (accessed 27 July 2011). (Vic AU)

Victoria Government, *Constitution Act 1975, No. 8750 of 1975. Version incorporating amendments as at 1 January 2010*. (1975), at http://www.legislation.vic.gov.au/Domino/Web_Notes/LDMS/PubLawToday.nsf/a12f6f60fbd56800ca256de500201e54/4C214C9ECF03BDFFCA257695000AFCAC/$FILE/75-8750a194.pdf (accessed 16 February 2011). (Vic AU)

Victoria Government, *Privacy Regulation Across Australia*. (2003), at

http://www.privacy.vic.gov.au/privacy/web.nsf/download/11344F7F3050AF9ECA256D58000597A7/$FILE/03.03_Interstate.pdf (accessed 27 March 2011).

Western Australia, *Constitution Act 1889* (1889), at http://www.austlii.edu.au/au/legis/wa/consol_act/ca1889188/ (accessed 16 February 2011).

Western Australia, *Freedom of Information Act 1992 (WA)*. (1992), at http://www.slp.wa.gov.au/legislation/agency.nsf/foi_main_mrtitle_353_homepage.html (accessed 9 January 2011).

Canada (CA)

Canadian Bar Association, *Comprehensive Revision of Privacy Act: Resolution 08-06a*. (2008, September 26), at http://www.cba.org/cba/resolutions/pdf/08-06-a-pdf.pdf (accessed 26 September 2011).

Canadian Constitution Act, *Constitution Act, 1982, being Schedule B to the Canada Act 1982 (U.K.), 1982, c. 11 (CA)*. at http://www.canlii.org/en/ca/const/const1982.html (accessed 3 August 2011).

Canadian Constitution Act, *Constitution Acts from 1867 to 1982*. (1867), at http://laws.justice.gc.ca/en/const/c1867_e.html (accessed 2 August 2011).

Canadian Constitution Act, *The Canadian Charter of Rights and Freedoms*. (1982), at http://laws.justice.gc.ca/en/charter/ (accessed 25 July 2011).

Canadian Constitutional Documents, *A Legal History*. (2004), at http://www.solon.org/Constitutions/Canada/English/ (accessed 6 July 2011).

Canadian Criminal Code, *R.S.C. 1985, c. C-46*. (1985), at http://www.canlii.org/ca/sta/c-46/sec184.html (accessed 15 August 2011).

Canadian Federal Government, *Canadian Privacy Act - R.S.C. 1985, c. P-21*. (1982), at http://laws.justice.gc.ca/en/P-21/index.html (accessed 7 November 2011).

Canadian Federal Government, *Personal Information Protection and Electronic Document Act*. (2000), at http://laws.justice.gc.ca/en/showtdm/cs/P-8.6 (accessed 1 November 2011).

Canadian Laws, *Canadian Consumer Protection Laws*. (2010), at http://www.canadianlawsite.ca/consumer-protection.htm#g (accessed 3 January 2011).

Canadian Privacy Commissioner, *Privacy by the Numbers in 2007*. (2007), at http://www.privcom.gc.ca/information/ar/200708/2007_pipeda_e.asp (accessed 4 September 2011).

Canadian Standards Association, *Model Code for the Protection of Personal Information*. (1996), at http://www.csa.ca/standards/privacy/code/Default.asp?language=English (accessed 15 June 2011).

Constitution Act, *Canadian Charter of Rights and Freedoms*. (1982), at http://www.solon.org/Constitutions/Canada/English/ca_1982.html (accessed 29 February 2011).

Government of Alberta, *Personal Information Protection Amendment Act, 2009*. (2009), at http://www.qp.alberta.ca/546.cfm?page=CH50_09.CFM&leg_type=fall (accessed 8 July 2011).

Government of Canada, *Government of Canada*. (2010), at http://www.canada.gc.ca/home.html (accessed 5 August 2011).

Government of Canada, *Parliament of Canada*. (2010), at http://www.parl.gc.ca/common/index.asp?Language=E (accessed 5 August 2011).

Government of Canada, *Prime Minister of Canada*. (2010), at http://pm.gc.ca/eng/index.asp (accessed 5 August 2011).

Government of Canada, *Privacy and Your business* (2010), at http://www.canadabusiness.ca/eng/guide/2338/ (accessed 19 July 2011).

Government of Canada, *Supreme Court of Canada*. (2010), at http://www.scc-csc.gc.ca/home-accueil/index-eng.asp (accessed 5 August 2011).

Government of the Northwest Territories, *Access to Information Protection of*

Privacy Act. (1996), at http://www.justice.gov.nt.ca/pdf/ACTS/Access_to_Information.pdf (accessed 24 September 2011).

Government of Yukon, *Access to Information and Protection of Privacy Act*. (2002), at http://www.gov.yk.ca/legislation/acts/atipp.pdf (accessed 19 September 2011).

Information and Privacy Commissioner/Ontario, *Commissioner Cavoukian to Unveil Best Practices for Smart Grid Privacy Protection at Toronto Summit, June 16*. (2010), at http://www.ipc.on.ca/images/Resources/2010-06-14-Smart-Grid-Paper-Media-Advisory.pdf (accessed 14 June 2011).

Information and Privacy Commissioner/Ontario, *The New Federated Privacy Impact Assessment (F-PIA): Building Privacy and Trust-enabled Federation*, Author. (2009), at http://www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=836 (accessed 2 March 2011).

Office of the Privacy Commissioner of Canada, *Annual Report to Parliament 2009: Report on the Personal Information Protection and Electronic Documents Act*. (2010), at http://www.priv.gc.ca/information/ar/200910/2009_pipeda_e.pdf (accessed 8 July 2011).

Office of the Privacy Commissioner of Canada, *Canadians Concerned Corporate Cost Cutting Could Affect their Privacy: Poll.* . (2009, April 27), at http://www.priv.gc.ca/information/survey/2009/ekos_2009_01_e.cfm (accessed 28 April 2011).

Office of the Privacy Commissioner of Canada, *PIPEDA Self-Assessment Tool: Personal Information Protection and Electronic Documents Act*. (2008. August 8), at http://www.privcom.gc.ca/information/pub/ar-vr/pipeda_sa_tool_200807_e.asp (accessed 10 August 2011).

Office of the Privacy Commissioner of Canada, *PIPEDA: Processing Personal Data Across Borders Guidelines*, Author. (2009), at http://www.priv.gc.ca/information/guide/2009/gl_dab_090127_e.pdf (accessed 2 July 2011).

Office of the Privacy Commissioner of Canada, *Poll: Canadian Businesses Unconcerned About Privacy Breach Risk*. (2010), at http://www.priv.gc.ca/media/nr-c/2010/nr-c_100527_e.cfm (accessed 27 May 2011).

Supreme Court of Canada, *About the Court*. (2010), at http://www.scc-csc.gc.ca/court-cour/index-eng.asp (accessed 5 July 2011).

South Africa

Constitutional Court of South Africa, *Constitutional Court of South Africa*. (2011), at http://www.constitutionalcourt.org.za/site/home.htm (accessed 29 May 2011).

Republic of South Africa, *Constitution of the Republic of South Africa, Act 108*. (1996), at http://www.info.gov.za/documents/constitution/1996/index.htm (accessed 24 January 2011).

South Africa Government, *Executive Authority*. (2010), at http://www.info.gov.za/aboutgovt/exec.htm (accessed 5 August 2011).

South Africa Government, *Justice System*. (2010), at http://www.info.gov.za/aboutgovt/justice/courts.htm (accessed 5 August 2011).

South Africa Government, *National Legislature - Parliament*. (2010), at http://www.info.gov.za/aboutgovt/parliament/index.htm (accessed 5 August 2011).

South Africa Government, *South Africa Government Online*. (2010), at http://www.gov.za/ (accessed 5 August 2011).

South African Law Reform Commission, *Issue Paper on Privacy and Data Protection*. (2003), at http://www.doj.gov.za/salrc/ipapers.htm (accessed 6 March 2011).

South African Law Reform Commission, *Media Statement by the South African Law Reform Commission: Project 124: Privacy and Data Protection*. (2005), at http://www.nqf.org.za/download_files/nqf-support/Privacy%20and%20Data%20protection%20Paper%2024%20Project%20124.pdf (accessed 2 May 2011).

United Kingdom (UK)

Information Commissioner Office, *Information Commissioner's Guidance About the Issue of Monetary Penalties Prepared and Issued Under Section 55C (1) of the Data Protection Act 1998*, Author. (2010), at http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/ico_guidance_monetary_penalties.pdf (accessed 12 September 2011).

Information Commissioner Office, *Privacy Impact Assessment Handbook*. (2009), at http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/html/0-advice.html (accessed 6 October 2011).

Information Commissioner Office, *Privacy Notices Code of Practice*. (2009), at http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/privacy_notices_cop_final.pdf (accessed 6 July 2011).

Information Commissioner Office, *The Information Commissioner's Response to the Ministry of Justice's Call for Evidence on the Current Data Protection Legislative Framework.* (2010), at http://www.ico.gov.uk/upload/documents/library/data_protection/notices/response_to_moj_dpframework.pdf (accessed 6 October 2011).

Information Commissioner's Office, *Banks in Unacceptable Data Protection Breach*. (2007, March 13), at http://www.ico.gov.uk/upload/documents/pressreleases/2007/banks_in_unacceptable_data_protection_breach.pdf (accessed 17 June 2011).

Information Commissioner's Office, *Enforcement Notices*. (2008), at http://www.ico.gov.uk/what_we_cover/data_protection/enforcement.aspx (accessed 29 September 2011).

Information Commissioner's Office, *Mark & Spencer v. ICO*. (2008, January 23), at http://www.ico.gov.uk/upload/documents/library/data_protection/notices/m_and_s_sanitiseden.pdf (accessed 29 September 2011).

Information Commissioner's Office, *Ministers breach Data Protection Act*, Contractor UK. (2008), at

http://www.contractoruk.com/news/004075.html (accessed 18 November 2011).

Information Commissioner's Office, *The Information Commissioner's Inspection Powers and Funding Arrangements under the Data Protection Act 1998: Response of the Information Commissioner to the Ministry of Justice's Consultation Paper of 16 July 2008*. (2008, August 22), at http://www.ico.gov.uk/upload/documents/library/corporate/notices/response_of_ic_to_moj_consultation_paper.pdf (accessed 12 September 2011).

Information Commissioner's Office, *Orange Personal Communication Services v. ICO* UK. (2007, March 21), at http://www.ico.gov.uk/upload/documents/library/data_protection/notices/orange_undertaking.pdf (accessed 30 September 2011).

Magna Carta, *Magna Carta*. (1215), at http://www.yale.edu/lawweb/avalon/medieval/magframe.htm (accessed 24 September 2011).

Scottish Executive, *Data Protection Act 1998 Explanatory Guidance*. (1998), at http://www.scotland.gov.uk/Resource/Doc/1066/0006064.pdf (accessed 19 August 2011).

Statutes of Great Britain, *The British North America Act*. (1867), at http://home.cc.umanitoba.ca/~sprague/bna.htm (accessed 29 February 2011).

The Supreme Court of the United Kingdom, *The Supreme Court*. (2010), at http://www.supremecourt.gov.uk/ (accessed 30 December 2011).

United Kingdom Government, *Data Protection Tracking Research*. (1995-1996-1997), at http://www.open.gov.uk/dpr/report97/%21app8.pdf (accessed 1 September 2011).

United Kingdom Government, *Government, Citizens and Rights*. (2010), at http://www.direct.gov.uk/en/Governmentcitizensandrights/index.htm (accessed 5 August 2011).

United Kingdom Government, *Parliament*. (2010), at http://www.parliament.uk/ (accessed 5 August 2011).

United Kingdom Government, *The Official Site of the Prime Minister's Office*.

(2010), at http://www.number10.gov.uk/ (accessed 5 August 2011).

United Kingdom Government, *The Supreme Court*. (2010), at http://www.supremecourt.gov.uk/index.html (accessed 5 August 2011).

United Kingdom Government, *The U.K. Data Protection Act of 1998*. (1998), at http://www.hmso.gov.uk/acts/acts1984/1984035.htm (accessed 17 May 2011).

United Kingdom Home Office, *Retention of Communications Data under part 11: Anti-terrorism Crime and Security Act of 2001, Voluntary Code of Practice*. (2001), at http://www.opsi.gov.uk/si/si2003/draft/5b.pdf (accessed 10 October 2011).

United Kingdom, *Data Protection Act 1998: 1998 Chapter 29*. (1998), at http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1 (accessed 5 June 2011).

United Kingdom, *Human Rights Act 1998: 1998 Chapter 42*. (1998), at http://www.opsi.gov.uk/acts/acts1998/ukpga_19980042_en_1 (accessed 5 June 2011).

United Kingdom, *Regulation of Investigatory Powers Act 2000: 2000 Chapter 23*. (2000), at http://www.opsi.gov.uk/acts/acts2000/ukpga_20000023_en_1.htm (accessed 5 June 2011).

United Kingdom, *United Kingdom Anti-terrorism, Crime and Security Act 2001 Chapter 24* (2001), at http://www.opsi.gov.uk/acts/acts2001/ukpga_20010024_en_1 (accessed 2 July 2011).

United States (US)

California Constitution, *Privacy*. (2003), at http://www.csc.calpoly.edu/~aeaston/california-sp.html (accessed 10 June 2011).

California Senate, *Senate Bill No. 541*. (2008), at http://info.sen.ca.gov/pub/07-08/bill/sen/sb_0501-0550/sb_541_bill_20080930_chaptered.pdf (accessed 1 October 2011).

Department of Health and Human Services, *Resolution Agreement*. (2008), at

http://www.dhhs.gov/ocr/privacy/enforcement/agreement.pdf (accessed 29 July 2011).

Federal Communication Commission, *Commission Orders Comcast to End Discriminatory Network Management Practices*. (2008), at http://www.fcc.gov/Daily_Releases/Daily_Business/2008/db0801/DOC-284286A1.txt (accessed 2 August 2011).

Federal Deposit Insurance Corporation, *FDIC*. (2007), at http://www.fdic.gov/ (accessed 30 August 2011).

Federal Trade Commission, *BJ's Wholesale Club, Inc. (DOCKET NO. C-4148)*. (2005, September 23), at http://www.ftc.gov/os/caselist/0423160/092305comp0423160.pdf (accessed 24 July 2011).

Federal Trade Commission, *Bonzi Software, Inc., A Corporation, and Joe Bonzi and Jay Bonzi, Individually and as Officers of Said Corporation (DOCKET NO. C-4126)*. (2004, October 13), at http://www.ftc.gov/os/caselist/0423016/041013cmp0423016.pdf (accessed 25 July 2011).

Federal Trade Commission, *CardSystems Solutions, Inc., & Solidus Networks, Inc., d/b/a/ Pay By Touch Solutions. (DOCKET NO. C-4168)*. (2006, September 8), at http://www.ftc.gov/os/caselist/0323040/041008comp0323040.pdf (accessed 23 July 2011).

Federal Trade Commission, *ChoicePoint Inc.* (2006 December 6), at http://www.ftc.gov/os/caselist/choicepoint/0523069complaint.pdf (accessed 1 August 2011).

Federal Trade Commission, *DirecTV, a California Corporation; D.R.D., Inc., also d/b/a Power Direct, an Ohio Corporation; Daniel R. Delfino, individually & as an officer of D.R.D., Inc.; & Nomrah Records, also d/b/a Direct Activation, a Florida Corporation (File No. 042 3039)*. (2006, December 14), at http://www.ftc.gov/os/caselist/0423039/0423039.shtm (accessed 12 August 2011).

Federal Trade Commission, *Dot Com Disclosure*. (2003), at http://www.ftc.gov/bcp/conline/pubs/buspubs/dotcom/index.html

(accessed 22 May 2011).

Federal Trade Commission, *DSW, Inc. (DOCKET NO. C-4157)*. (2006, March 7), at http://www.ftc.gov/os/caselist/0523096/0523096c4157DSWComplaint.pdf (accessed 23 July 2011).

Federal Trade Commission, *Education Research Center of American, Inc., Student Marketing Group, Inc., Marian Sanjana, & Jan Stumacher (DOCKET NO. C-4079)*. (2003, May 9), at http://www.ftc.gov/os/2003/05/ERCAcomplaint.pdf (accessed 1 August 2011).

Federal Trade Commission, *Eli Lilly Company. (DOCKET NO. C-4047)*. (2002, May 10), at http://www.ftc.gov/os/2002/05/elililllycmp.htm (accessed 23 July 2011).

Federal Trade Commission, *Executive Financial Home Loan Corp., d/b/a Executive Home Loan, a California Corporation, Michael Nikravesh, Individually & as an Officer of Executive Financial Home Loan Corp., & Ron Fattal, Individually & as an Officer of Executive Financial Home Loan Corp.* (2006, June 21), at http://www.ftc.gov/os/caselist/0423143/0423143ExechomeLoanCmplt.pdf (accessed 21 July 2011).

Federal Trade Commission, *Facebook, Inc. (DOCKET NO. C-4365)*. (2012), at http://ftc.gov/os/caselist/0923184/120810facebookcmpt.pdf (accessed 10 August 2012).

Federal Trade Commission, *FTC Consumer Alert*. (2005, June), at http://www.ftc.gov/bcp/conline/pubs/alerts/disposalalrt.shtm (accessed 2 September 2011).

Federal Trade Commission, *FTC Recommends Congressional Action to Protect Consumer Privacy Online* (2002), at http://www.ftc.gov/opa/2000/05/privacy2k.htm (accessed 22 May 2011).

Federal Trade Commission, *Gateway Learning Corporation (DOCKET NO. C-4120)*. (2004, September 14), at http://www.ftc.gov/os/caselist/0423047/040917comp0423047.pdf (accessed 24 July 2011).

Federal Trade Commission, *GeoCities*. (1998), at http://www.ftc.gov/os/1999/02/9823015cmp.htm (accessed 2 June 2011).

Federal Trade Commission, *Google, Inc. (Docket C-4335)*. (2012), at http://www.ftc.gov/os/caselist/c4336/120809googlecmptexhibits.pdf (accessed 20 November 2012).

Federal Trade Commission, *Guess?, Inc., and Guess.com, Inc. (DOCKET NO. C-4091)*. (2003, August 5), at http://www.ftc.gov/os/caselist/0223260.shtm (accessed 19 July 2011).

Federal Trade Commission, *Hersey Food Corporation*. (2003, February 27a), at http://www.ftc.gov/os/2003/02/hersheycmp.htm (accessed 26 July 2011).

Federal Trade Commission, *Kids*. (1997), at www.ftc.gov/opa/1997/9712/kids.htm (accessed 20 February 2011).

Federal Trade Commission, *Letter.* (1999), at http://www.ftc.gov/be/v990010.htm (accessed 15 November 2011).

Federal Trade Commission, *Microsoft Corporation. (DOCKET NO. C-4069)*. (2002, December 24), at http://www.ftc.gov/os/caselist/0123240/microsoftcmp.pdf (accessed 22 July 2011).

Federal Trade Commission, *Mrs. Fields Famous Brands, Inc., Mrs. Fields' Holding Company, Inc., and Mrs. Fields' Original Cookies, Inc*. (2003 February 27b), at http://www.ftc.gov/os/2003/02/mrsfieldscmp.htm (accessed 9 August 2011).

Federal Trade Commission, *MTS, Inc., d/b/a Tower Records/Books/Video, a corporation, and Tower Direct, LLC, d/b/a TowerRecords.com, a corporation. (DOCKET NO. C-4110)*. (2004, June 2), at http://www.ftc.gov/os/caselist/0323209/040602comp0323209.pdf (accessed 21 July 2011).

Federal Trade Commission, *Petco Animal Supplies, Inc. (DOCKET NO. C-4133)*. (2005, March 8), at http://www.ftc.gov/os/caselist/0323221/050308comp0323221.pdf (accessed 20 July 2011).

Federal Trade Commission, *Pretexting: Enforcement Cases*. (2007), at

http://www.ftc.gov/privacy/privacyinitiatives/pretexting_enf.html (accessed 2 September 2011).

Federal Trade Commission, *Privacy Online: A Report to Congress*. (1998), at http://www.ftc.gov/reports/privacy3/toc.shtm (accessed 10 May 2011).

Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace: A Report to Congress*. (2000), at http://www.ftc.gov/reports/privacy2000/privacy2000.pdf (accessed 26 July 2011).

Federal Trade Commission, *Privacy Workshop '97 Hearings Transcripts for Session 2, panel 2, part 3*. (1997), at http://consumer-info.org/FTCpriv97/FTCprivacyw.asp (accessed 2 March 2011).

Federal Trade Commission, *Privacy*. (1998), at www.ftc.gov/opa/1998/9806/privacy2.htm (accessed 20 February 2011).

Federal Trade Commission, *Protecting Privacy in an Era of Rapid Change: Recommendations for Business and Policymakers*. (2012), at http://www.ftc.gov/os/2012/03/120326privacyreport.pdf (accessed 26 March 2012).

Federal Trade Commission, *Superior Mortgage Corporation (Docket C-4153)*. (2005, December 16), at http://www.ftc.gov/os/caselist/0523136/051216comp0523136.pdf (accessed 2 August 2011).

Federal Trade Commission, *The Fair Credit Reporting Act*. (2004), at http://www.ftc.gov/os/statutes/031224fcra.pdf (accessed 11 June 2011).

Federal Trade Commission, *The Ohio Art Company (FTC File Nos. 022-3028)*. (2005, April 22), at http://www.ftc.gov/os/2002/04/ohioartconsent.htm (accessed 24 July 2011).

Federal Trade Commission, *Vision I Properties, LLC d/b/a CartManager International, Inc.* (2005, April 26), at http://www.ftc.gov/os/caselist/0423068/050426comp0423068.pdf (accessed 21 July 2011).

Office of Management and Budget, *Fiscal Year 2009 Report to Congress on*

Implementation of the Federal Information Security Management Act of 2002. (2009), at http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/FY09_FISMA.pdf (accessed 12 March 2012).

State of Alaska, *Constitution*. (1956), at http://old-www.legis.state.ak.us/cgi-bin/folioisa.dll/acontxt/query=*/doc/%7Bt25%7D (accessed 10 July 2011).

State of Arizona, *Constitution*. (1881), at http://www.azleg.state.az.us/const/2/8.htm (accessed 10 July 2011).

State of California, *California Office of Information Security and Privacy Protection*. (2009), at http://www.oispp.ca.gov/ (accessed 4 September 2011).

State of California, *Constitution*. (1879), at http://www.leginfo.ca.gov/cgi-bin/waisgate?waisdocid=8071921924+0+0+0&waisaction=retrieve (accessed 10 July 2011).

State of California, *The California Security Breach Information Act (SB-1386), Civil Code §1798.29,, §1798.82, & 1798.84* (2002), at http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html (accessed 3 July 2011).

State of Florida, *Constitution*. (1968), at http://www.flsenate.gov/Statutes/index.cfm?Mode=Constitution&Submenu=3&Tab=statutes#A01S23 (accessed 10 July 2011).

State of Hawaii, *Constitution*. (1978), at http://www.state.hi.us/lrb/con/conart1.html (accessed 10 July 2011).

State of Illinois, *Constitution*. (1970), at http://www.ilga.gov/commission/lrb/con1.htm (accessed 10 July 2011).

State of Louisiana, *Constitution*. (1974), at http://www.senate.legis.state.la.us/Documents/Constitution/Article1.htm#%EF%BF%BD5.%20Right%20to%20Privacy (accessed 10 July 2011).

State of Montana, *Constitution*. (1972), at http://data.opi.mt.gov/bills/mca/const/II/10.htm (accessed 10 July 2011).

State of New Jersey, *Constitution*. (1947), at

http://www.njleg.state.nj.us/lawsconstitution/constitution.asp (accessed 10 July 2011).

State of South Carolina, *Constitution*. (2006), at http://www.scstatehouse.net/scconstitution/a01.htm (accessed 10 July 2011).

State of Utah, *Constitution*. (1895), at http://le.utah.gov/~code/const/htm/CO_02015.htm (accessed 10 July 2011).

State of Washington, *Constitution*. (1889), at http://www.courts.wa.gov/education/constitution/index.cfm?fa=education_constitution.display&displayid=Article-01 (accessed 10 July 2011).

Supreme Court of the United States, *About the Supreme Court*. (2010), at http://www.supremecourt.gov/ (accessed 5 July 2011).

The Alien Act, *An Act Respecting Alien Enemies*. (1798), at http://www.yale.edu/lawweb/avalon/statutes/alien.htm (accessed 15 June 2011).

The Sedition Act, *An Act for the Punishment of Certain Crimes Against the United States*. (1798), at http://www.yale.edu/lawweb/avalon/statutes/sedact.htm (accessed 15 June 2011).

The Sedition Act, *An Amendment to Section 3 of the Espionage Act of June 15, 1917*. (1918), at http://www.wfu.edu/~zulick/341/sedition1918.html (accessed 15 June 2011).

U.S. Congress Joint Committee on Governmental Operations, *Legislative History of the Privacy Act of 1974: Source Book on Privacy*. (1976), at http://www.loc.gov/rr/frd/Military_Law/pdf/LH_privacy_act-1974.pdf (accessed 2 January 2011).

U.S. Department of Health and Human Services, *Health Information Policy*, Author. (2011), at http://www.hhs.gov/ocr/privacy/ (accessed 14 July 2011).

U.S. Department of Justice, *Overview of the Privacy Act of 1974*. (2010), at http://www.justice.gov/opcl/1974intro.htm (accessed 4 January 2011).

United State GAO, *Information Security: Agencies Continue to Report Progress, but Need to Mitigate Persistent Weaknesses*. (2009), at

http://www.gao.gov/new.items/d09546.pdf (accessed 23 July 2011).

United States Codes, *United States Codes. 17 U.S.C. Section 102(b)* (2003), at http://www4.law.cornell.edu/uscode/17/102.html; **Computer Programs** http://www4.law.cornell.edu/uscode/17/117.html; **Exceptions** http://www4.law.cornell.edu/uscode/17/110.html; **Fair Use** http://www4.law.cornell.edu/uscode/17/107.html; **Library** http://www4.law.cornell.edu/uscode/17/108.html; **Recordings** http://www4.law.cornell.edu/uscode/17/112.html; **Secondary Transfer** http://www4.law.cornell.edu/uscode/17/111.html; **Transfer** http://www4.law.cornell.edu/uscode/17/109.htm (accessed 25 November 2011).

United States Congress, *The National Environmental Policy Act of 1969, as amended (Pub. L. 91-190, 42 U.S.C. 4321-4347, January 1, 1970, as amended by Pub. L. 94-52, July 3, 1975, Pub. L. 94-83, August 9, 1975, and Pub. L. 97-258, § 4(b), Sept. 13, 1982)*. (1969), at http://ceq.eh.doe.gov/nepa/regs/nepa/nepaeqia.htm (accessed 5 March 2011).

United States Constitution, *United States Constitution.* (1788), at http://www.kearney.net/~tclayton/The%20Constitution%20of%20the%20United%20States.htm (accessed 4 July 2011).

United States Declaration of Independence, *Declaration of Independence* (1776), at http://usinfo.state.gov/usa/infousa/facts/democrac/1.htm (accessed 26 September 2011).

United States Department of Defense Technology and Privacy Advisory Committee, *Safeguarding Privacy in the Fight Against Terrorism*. (2004, March), at http://www.cdt.org/security/usapatriot/20040300tapac.pdf (accessed 5 December 2011).

United States Department of Homeland Security, *Privacy Office - DHS Data Privacy and Integrity Advisory Committee*. (2008), at http://www.dhs.gov/xinfoshare/committees/editorial_0512.shtm (accessed 10 December 2011).

United States Department of Justice, *Microsoft Agrees to End Unfair*

Monopolistic Practices. (1994), at http://www.usdoj.gov/opa/pr/Pre_96/July94/94387.txt.html (accessed 8 April 2011).

United States Department of Justice, *The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet*. (2003), at http://www.usdoj.gov/criminal/cybercrime/unlawful.htm (accessed 19 May 2011).

United States Government Accountability Office, *Agencies Should Ensure that Designated Senior Officials Have Oversight of Key Functions*. (2008, May 30), at http://www.gao.gov/new.items/d08603.pdf (accessed 18 June 2011).

United States Government Accountability Office, *Alternatives Exist for Enhancing Protection of Personally Identifiable Information*. (2008, April 19), at http://www.gao.gov/new.items/d08536.pdf (accessed 19 June 2011).

United States Government Accountability Office, *Congress Should Consider Alternatives for Strengthening Protection of Personally Identifiable Information*. (2008, June 18), at http://www.gao.gov/new.items/d08795t.pdf (accessed 18 June 2011).

United States Government Accountability Office, *Data Mining: Federal Efforts Cover a Wide Range of Uses*. (2004), at http://epic.org/privacy/profiling/gao_dm_rpt.pdf (accessed 23 June 2011).

United States Government Accountability Office, *Information Secuirty: FBI Needs to Address Weaknesses in Critical Network*. (2007), at http://www.gao.gov/new.items/d07368.pdf (accessed 31 December 2011).

United States of America, *Find Government Agencies*. (2010), at http://www.usa.gov/ (accessed 5 August 2011).

United States of America, *Supreme Court of the United States*. (2010), at http://www.supremecourt.gov/ (accessed 5 August 2011).

United States of America, *The Executive Branch*. (2010), at http://www.whitehouse.gov/our-government/executive-branch (accessed 5 August 2011).

United States of America, *United States House of Representatives*. (2010), at http://www.house.gov/ (accessed 5 August 2011).

United States of America, *United States Senate*. (2010), at http://www.senate.gov/ (accessed 5 August 2011).

US Department of Health & Human Services, *The Belmont Report: Ethical Principles and Guidelines for the Protection of Human Subjects of Research; The National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research*. (1979), at http://www.hhs.gov/ohrp/humansubjects/guidance/belmont.html (accessed 21 July 2011).

US Rules of Civil Procedure, *Rules of Civil Procedure*. (2006), at http://www.law.cornell.edu/rules/frcp/index.html (accessed 25 September 2011).

US Rules of Evidence, *Rules of Evidence*. (2006), at http://www.law.cornell.edu/rules/fre/index.html (accessed 22 September 2011).

Detailed Outline

Chapter One: Data Protection and Security Law: The Problem

Chapter Two: Data Protection And Security Law: Sociolegal Issues

Chapter Four: Data Protection and Security Law: Australian Legal Standards

Chapter Five: Data Protection and Security Law: Canadian Legal Standards

Chapter Six: Data Protection and Security Law: South African Legal Standards

Chapter Seven: Data Protection and Security Law: United Kingdom Legal Standards

Chapter Ten: Data Protection and Security Law: Gold Standard Proposal

CHAPTER ONE: DATA PROTECTION AND SECURITY LAW: THE PROBLEM

> *The law is not a series of calculating machines where definitions and answers come tumbling out when the right levers are pushed.* Justice William O. Douglas[1]

> *There is … unanimity that opportunists, for private gain, cannot be permitted to arm themselves with an acceptable principle, (to) proceed to use it as an iron standard to smooth their path by crushing the living rights of others to privacy and repose.* Stanley F. Reed[2]

At the time of this writing, the Republic of South Africa (SA) has engineered the largest Internet connectivity of any country on the African continent, and has been investigating and developing data protection legal standards. This thesis examines the legal strategies of developed countries relevant to data collection, security, storage, use, and transfer, along with the integrity of these legal approaches.

Material reviewed for comparison included both international legal standards and governmental and nongovernmental protection and security guidelines from five countries that had a contradictory history of dealing with the issues: the Commonwealth of Australia (AU), the Government of Canada (CA), SA, the United Kingdom of Great Britain and Northern Ireland (UK), and the United States of America (US).[3]

---

[1] William Orville Douglas, The Dissent, A Safeguard of Democracy, 32 *Journal of the American Judicial Society* 104, 105 (1948).

[2] *Breard v. Alexandria*, 341 U.S. 622, 625–26, (1951). (US)

[3] The purpose and function of a cite and reference system is to help readers and researchers find relevant information. Given that the contradictory and inconsistent national and international systems related to the use of abbreviations and citations, the author selected a consistent approach, with the permission of the promoter. Abbreviations follow the UK system of eliminating full stops or periods and two letter country codes.

1.0 Overview of Chapter One

This chapter presents a statement of the problem and relevant background information; an overview of the research strategy used in this study; the purpose, legal rationale, and importance of the study; and the approach to be used. The theoretical framework, questions, and objectives to be investigated in this study will also be examined in chapter one.

Every study is based on conceptual and substantive assumptions. This chapter presents the assumptions made; provides key definitions; describes the research methodology and approach used in the study; presents a justification for using a comparative law analysis model; and explains the data collection procedures and data processing and analysis used. The chapter ends with a summary of the problem, a summary of the literature and issues reviewed, and an outline of the entire thesis.

1.1 Statement of the Problem

As access to and use of the World Wide Web expanded, the market for personal information became global. Various countries and regions have established, or were in the process of establishing, data protection, data

---

The footnote format system followed the Association of Legal Writing Directors (ALWD) (4th ed.) Citation Manual as it is the closest to the unique South African legal citation system yet it was internationally recognized and consistent with the comparative focus of this work. One exception was the citation of international sources for which ALWD was silent and somewhat ethnocentric (due to yet unpublished but projected manuals based on proprietary gain). In such situations, the author applied rules 20.3 and 20.5 of the BlueBook (18th ed.) system, which added country identification at the end of cases and statutes. Publication names are spelled out due to the international nature of the sources used. This standard is based on the APA (6th ed.) which is the behavior, policy, and social science standard in the US and the majority of the English speaking word. Journal titles are in italics as directed by my professor, the SA approach, and the APA standard. Copies of all electronically collected files are on file with the author. The vast majority of in-print journals and books are also on file with the author. When the intellectual property (IP) laws apply, the IP law will be applied. Generally, a copy of the cited books, book chapters, journals, journal articles, and electronic sources are on file with the Author. Internet and intranet resources have been verified on a yearly basis. The UNISA School of Law has some unique standards which have been followed – like access or visit data.

security, and information privacy (DPSIP) laws. The international debate on privacy concerns was prominent. Business abuses were evident. Consumers wanted clearer protections.[4]

Existing data protection and information privacy laws were generally out-of-date, ignored, inadequate, or nonexistent. In 2008, David Weisbrot, the president of the Australian Law Reform Commission, documented the need for a reevaluation. He declared:

> Recent advances in information, communication and surveillance technologies have created and intensified a range of privacy issues. The internet, biometrics, digital phones and cameras, powerful computers and radio-frequency identification have all contributed to making it easier, cheaper and faster for government agencies and business organizations to collect, store and aggregate large amounts of personal and sensitive information.[5]

Integrated DPSIP laws administered by independent regulatory agencies are essential but lacking. The following ten findings substantiate the need for such laws:[6]

1. Behavioral science research showed DPSIP was essential to psychological, psychosocial, community, and cultural survival.
2. Independent surveys showed the majority of people in the selected countries wanted information privacy protection but were not receiving it. Behavioral science research showed that information privacy was vital to human and societal functioning.

---

[4] William Mitting, *Data Privacy Debate to Come to the Fore, Experts Say*. (2009), at http://www.printweek.com/digital/news/915730/Data-privacy-debate-to-fore-experts-say/ (last visited on 25 June 2012).

[5] David Weisbrot, *Technology-Neutral Privacy Principles Should Govern Rapidly Developing ICT.* (2008, August 11), at http://www.alrc.gov.au/media/2008/mbn2.pdf (last visited on 11 August 2012).

[6] The data supporting the first seven principles are documented in Chapter Two. The data for the rest of the points are found in the comparative legal standards chapters.

3. Personal information had become a valuable commodity that was easily acquired, accessed, stored, traded, transferred, and sold without permission or quality controls.
4. Governments and business organizations often failed to adequately address civil liberties, human rights, consumer protection, and personal property standards related to DPSIP. Because of the desire for control and their greed, governments and business also often failed in their duty to adequately protect and secure the data they held.
5. DPSIP practices violated analogous principles including informed consent, confidentiality, impact assessments, and audits.
6. Technological innovations received governmental approval and protection without there being any examination of information privacy, data protection, and data security assessments.
7. DPSIP violations threatened related legal principles and the security of individuals, businesses, and governments. The issues include asset protection, contract law, information control, intellectual property law, property laws, tort law, and privacy law conflicts.
8. Different national laws and regulatory approaches were inconsistent and often contradictory, making predictability often impractical.
9. Different national laws and regulatory approaches made DPSIP vulnerable to unauthorized use and abuse.
10. Different national laws and regulatory approaches made DPSIP violations and violators unaccountable.

The need for integrated DPSIP laws that these findings validate are well documented. David Holtzman[7] studied issues of technology and privacy, finding seven technological *sins* against privacy, including the following: (1) the *Sin of Intrusion*, which is a violation of one's physical and virtual spaces; (2) the *Sin of Latency*, which includes the "excessive hoarding" of personal data; (3) the *Sin of Deception*, which includes the use of private data for

[7] David H. Holtzman, *Privacy Lost: How Technology is Endangering your Privacy*, (Jossey-Bass ed. 2006).

purposes other than those approved or consented to; (4) the *Sin of Profiling*, which is the mishandling of personal data (including data mining); (5) the *Sin of Identity Theft*, includes criminal theft, and also the sale of data without consent or adequate data security; (6) the *Sin of Outing*, which includes misuse of personal data and sharing data without permission; and (7) the *Sin of Lost Dignity*, which includes using personal data for social control and abuses by powerful sources, including businesses and governments.[8] Holtzman concluded that as these sins harm individuals and society, privacy and data protection laws are required.

1.2 Background of the Problem

For centuries, informational privacy and data were protected by the technology of the age. Collected data was handwritten and later typed and placed in location-secure specific files. Such information was limited, not openly shared, and difficult to find, but it was also economically unimportant. The historic pattern was suddenly changed with the advent of the computer, information economy and the Internet, as information became economically valuable. Data could be mined (i.e., automatically scanned and collected) and easily shared, so information became instantly available and collectable.

The impact of data mining was established as early as 1997 when the *Minneapolis Star Tribune* received permission from a randomly selected individual to determine the depth and breadth of available information sources. The searchers determined where the person was born, lived, went to school, and worked. Data on the individual's preferences in beer, entertainment, food, politics, and vacations were also easily found.[9]

In the late nineteenth century, most modern governments also started a system of collecting and analyzing personal data for legitimate service purposes. In the mid-twentieth century, businesses followed this pattern,

---

[8] *Id.* at 5–34. The UNISA School of Law standard uses *Ibid*. In the US, *Id.* is used in legal citations and *Ibid.* is used in non-legal systems.

especially in credit reporting. However, data storage was via file cabinets, and access was limited.[10] The processes changed when the US government gave TRW Incorporated governmental computer programs to computerize credit reporting. Subsequently, the collection methods, uses, and value of information expanded.

As the Internet became commercial and companies demanded access and control over more data and databases, an economically powerful global system emerged. Large global corporations (including Acxiom, ChoicePoint, Experian, and LexisNexis) began purchasing databases from thousands of businesses and organizations to build extensive databases of their own on millions of people in the US alone. The data aggregators built electronic dossiers on millions of individuals that could then be filtered for specific data and sold on demand.[11]

More data was more easily available than ever before, and that data could be shared at unprecedented speeds. Whitfield Diffie and Susan Landau[12] documented that at the start of the nineteenth century, it took the UK government eighteen weeks to send a message to the New Delhi ambassador. By the end of the next century, the same message took only a couple of days, and then decreased to an hour. Currently the message could be sent in seconds. However, each increase in speed due to technological advances, resulted in a decrease in privacy protections.

There was a general realization that these privacy infringements required legal remedies, but information technology evolved faster than traditional legal bases could respond. The law largely ignored evolving privacy concerns. For example, intellectual property protections were awarded with no attention to privacy enhancing technology design. In effect, the law followed a traditional

---

[9] Jeffrey Rothfeder, *No Privacy on the Net*, PC World, 223 (1997, February).
[10] James B. Rule, *Privacy in Peril: How We Are Sacrificing a Fundamental Right in Exchange for Security and Convenience*, (Oxford University Press ed. 2007).
[11] Robert O'Harrow, *No Place to Hide*, (Free Press ed. 2006).
[12] Whitfield Diffie & Susan Landau, *Privacy on the Line: The Politics of Wiretapping and Encryption*, (The MIT Press. ed. 1998).

reactive pattern when the significance of these changes required a proactive legal response. The Internet and increased computer access, and the nature, speed, and implications of this technology presented a number of legal and policy challenges to traditional legal models and methods. The central legal issue was what hypotheses, deductions, objectives, and questions ought to be addressed. These developments challenged traditional common law views of asset protection, civil rights, consumer protection, data protection, data security, human rights, information privacy, and personal property rights.[13]

Powerful interests worked to make those challenges greater and to delay any emerging legal protections. Large corporations used the battle cry of marketing services and free speech, while governments used the need for national security. Both claimed ownership of data mining methods and data. The US Government Accountability Office (GAO) defined data mining as "the application of database technology and techniques—such as statistical analysis and modeling—to uncover hidden patterns and subtle relationships in data and to infer rules that allow for the prediction of future results."[14] Individual intellectual property rights, knowledge control, confidentiality rules, tort principles, and the legal principle of informed consent were ignored along with existing legal constraints. The US government violated its own laws and pulled data from private sources for its own purposes. For example, JetBlue Airlines released personal data on five million passengers when the government asked—no warrant, only a request for information.[15] Similar data were released under the same circumstances by several major telecommunication companies. There were no legal constraints in the United States to stop governments and private businesses from collecting, using, or sharing personal information. Corporations were found to share such information as they wanted to be seen as being nice or to avoid the problems

---

[13] *See* Lawrence Lessig, *Code: Version 2.0*, (Basic Books ed. 2006). *See also* Virginia Postrel, *The Future and its Enemies: The Growing Conflict Over Creativity, Enterprise, and Progress*, (The Free Press ed. 1998).

[14] United States Government Accountability Office, *Data Mining: Federal Efforts Cover a Wide Range of Uses.* (2004), at http://epic.org/privacy/profiling/gao_dm_rpt.pdf (last visited on 23 June 2012).

related to saying no. Neil Richards[16] analyzed the government business connection, and concluded the system allowed the government to circumvent statutory and constitutional constraints protecting individual privacy.

Personal data was now a unit of exchange that was usually secretly collected and monitored, then used to increase wealth and power. Modern data regarding an individual's existence included name, home address, pictures, social security number, medical treatment, and insurance records. Data on livelihood included the individual's airline and other travel information, certified and registered mail sent or received, computer uses by the individual, credit information on cards, credit history, delivery services used, listings in directories, driver's license, and information held by Federal Express. The data also included licensing information, Internet research records, office phone and fax numbers, online testing services, passport data, membership in professional organizations, publications, research used, security systems data, records of telephone calls, testifying records, websites used, and work address. Data that individuals gave voluntarily (such as for goods, services, causes, or vanity) included data on airport VIP cards, data in cable TV records, directories, frequent flyer/staying cards, merchant loyalty cards, and data related to political registrations. A staggering volume of private information was readily available on any given person.

This information was obtained from individuals via a number of methods ranging from fraudulently, involuntarily, and under duress to unknowingly and voluntarily. The sources included public records; quasi-public records; marketing data; business, financial, and personal records; and Internet use. The data would often be accessed online (either for free or via subscription), independent of location or authority. The individual's level of control was poor-to-moderate. With the aid of laws and judicial decisions, some businesses and governments had taken the information and declared it their

---

[15] Markle Foundation, *Creating a Trusted Information Network for Homeland Security*. (2003), at http://www.markletaskforce.org/ (last visited on 11 January 2012).

own to use, abuse, and share. An example was the Work Number Company, for which Carrie Teegardin[17] published data. The company collected detailed employment records of employees from a number of sources. The data included generally private data such as social security number, employer, job title, and wages. The Work Number then collected and sold the data to others without the employees' consent. The data included private information on a third of all American employees and constituted over 165 million records. There were no legal constraints on the collection or sale of this data—in fact, the US government was a customer.

By now it is clear that such individual employment data and other personal information should be secure, but are not. A recent study by Deloitte & Touche[18] found that data protection breaches and information privacy violations were increasing. In a study of over 827 privacy professionals, thirty-five percent reported six to ten privacy breach incidents, with forty-three percent reporting more than ten incidents in the last several months. Eighty-five percent reported at least one, and sixty-three percent reported multiple significant breaches. Of the breaches, thirty-four percent involved over 1,000 records and ten percent over 25,000 files. The Irish Privacy Commission reported that the office received 300 complaints in 2005, 658 in 2006, and in 2007 over 1,000 complaints.[19]

A similar pattern was found in the United States with privacy thefts. In 2006 there were 49.7 million reports, while in 2007 over 162 million records were lost or stolen. Disclosures came from "98 companies, 85 schools, 80

---

[16] Neil M. Richards, Reconciling Data Privacy and the First Amendment, 52 *UCLA Law Review*, 4, 1149 (2005).

[17] Carrie Teegardin, *Guess Who Knows How Much You Earn Each Week?,* The Atlanta Journal-Constitution. (2008), at http://www.ajc.com/search/content/business/stories/2008/01/20/worknumber_0120.html (last visited on 23 May 2012).

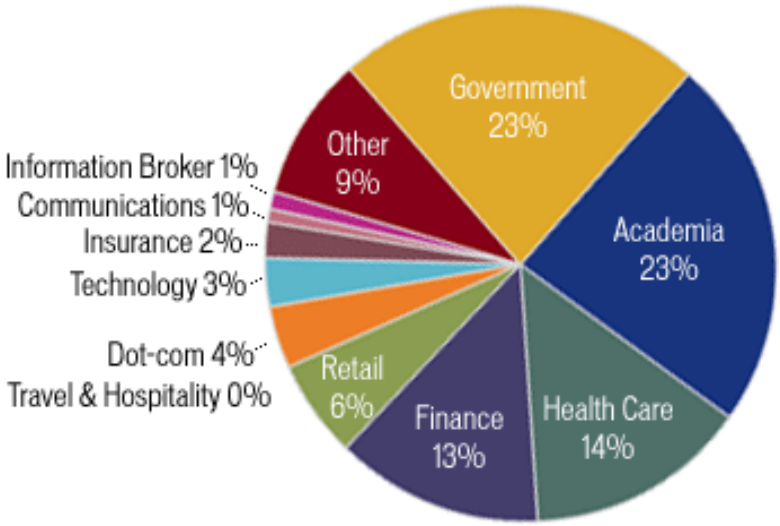
[18] Deloitte & Touche, LLP, *Enterprise@Risk: Insights Into the Emerging Privacy and Data Protection Function* (2007), http://www.deloitte.com/dtt/cda/doc/content/us_risk_s%26P_2007%20Privacy10Dec2007final.pdf (last visited Dec. 26, 2008).

[19] Ciara O'Brien, *Data Protection Complaints Soar*. (2007 December 12), at http://www.electricnews.net/article/10123588.html (last visited on 26 December 2012).

government agencies and 39 hospitals and clinics."[20] For example, records of 6,313 medical patients at the University of California-San Francisco were mistakenly made available on the Internet. The university took six months to make any notification to the individuals involved. The released data included names, addresses, medical identification numbers, treating physician and department records, financial information, donation history, and neighborhood maps.[21]

DPSIP data loss and breach violations alone were massive. Cline[22] determined that from 2000 to 2008, publically reported breaches alone involved more than 530 billion records (see Figure 1.1). The number was greater than the entire population of the European Union (EU) or of CA, the Caribbean, Central America, Mexico, and the US combined. The reported DPSIP violations accounted for more that the entire population of Africa.

Figure 1.1 Source of Breaches



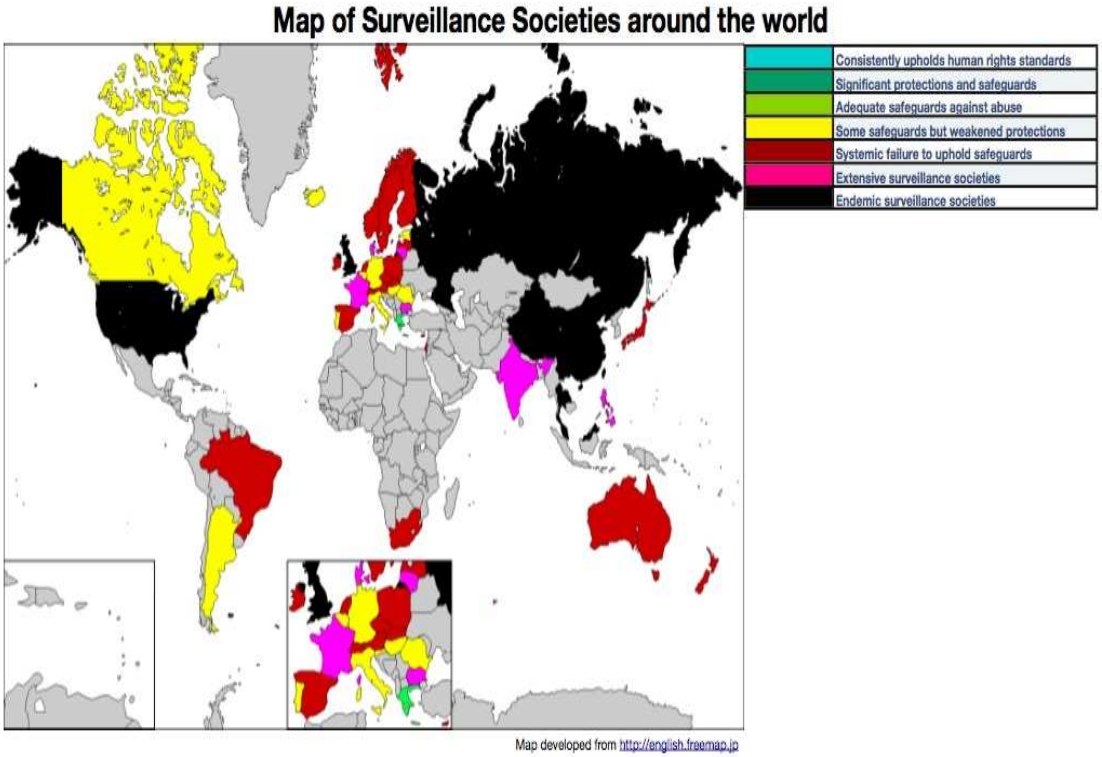
[20] Byron Acohido, *Theft of Personal Data More Than Triples This Year*. (2007, December 9), at http://www.usatoday.com/money/industries/technology/2007-12-09-data-theft_N.htm?POE=click-refer (last visited on 2 January 2012).

[21] Elizabeth Fernandez, *6,000 UCSF Patients' Data Got Put Online*, San Francisco Chronicle (2008, May 2), at A1.

[22] Jay Cline, *530M Records Exposed, and Counting*, Computerworld (2008, September 9), at http://computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=Privacy&articleId=9114176&taxonomyId=84&pageNumber=1 (last visited on 9 September 2012).

Since 1997, the Electronic Privacy Information Center (EPIC), located in the US and Privacy International, located in the UK, have researched worldwide privacy policies. The 2007 EPIC report revealed that DPSIP legal standards had diminished. The US and UK were some of the weakest data protectors, with AU being in the second worst category. CA was one of the best data protectors, the EU was declining, and SA was in the development phase. The report showed "an increasing trend amongst governments to archive data on the geographic, communications and financial records of all their citizens and residents. This trend leads to the conclusion that all citizens, regardless of legal status, are under suspicion."[23] The researchers examined constitutional protections, privacy enforcement, and statutory protections. A world map graphically illustrates the relevant privacy ratings of the study:

Figure 1.2 State of Privacy Map



[23] Privacy International, *Leading Surveillance Societies in the EU and the World 2007*. (2007, December 28), at http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559597 (last visited on 2 January 2012).

[24]

The map illustrates global surveillance levels per se, but this study also addressed the key issues of *constitutional protection, communications data retention, communication interception, data-sharing, democratic safeguards, government access to data, privacy enforcement, statutory protection, surveillance of medical, financial and movement and found safeguards lacking worldwide.*

The advent of modern computer technology provided businesses and governments the ability to amass, through grand mechanisms, the means to collect and build on data that left the owner–giver less control.[25] Alexander Rosenberg[26] described a "degenerate case of the peeping tom's invasion of our privacy" where "suffering is caused just by the voyeur's acquiring the information." A tension existed between the enlightened self-interest of the owner–giver and the economic or political advantage of the data collectors, who used an argument of social benefit and economic efficiency. Information gatherers tended to decay the value of the information and thus produced allocation of resource distortions.[27] The data controllers argued that the pattern of ignoring DPSIP legal standards was in the name of efficiency and public order. The impact was to destabilize the essential boundaries among governments, individuals, and society.[28] DPSIP legal standards are a public good[29] that the government must control to preserve democratic objectives.[30]

---

[24] *Id.* at 1.

[25] Hal R. Varian, Economic Aspects of Personal Privacy, in *Privacy and Self-Regulation in the Information Age* (U.S. Department of Commerce ed.eds., U.S. Department of Commerce 1996); Hal R. Varian, *The Information Economy: How Much Will Two Bits Be Worth in the Digital Marketplace?* (1996), at http://www.sims.berkeley.edu/~hal/pages/sciam.html (last visited on 4 July 2012).

[26] Alexander Rosenberg, Privacy as a Matter of Taste and Right, in *The Right to Privacy* (Ellen Krankel Paul, et al. eds., Cambridge University Press 2000).

[27] Roger V. Clarke, Computer Matching by Government Agencies: The Failure of Cost/Benefit Analysis as a Control Mechanism, 4 *Information Infrastructure and Policy*, 1, 29 (1995).

[28] David Lyon, *Surveillance Society: Monitoring Everyday Life*, (Open University ed. 2001). *See also* David Lyon, *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination* (David Lyon ed., Routlegde ed. 2003).

[29] An economics term for a good or service that enhances the well-being of the public and society.

Over 30 years ago, Jack Hirshleifer[31] maintained that respecting privacy rights provided an evolutionary advantage for people and societies. More recently Richard Epstein[32] argued that information privacy is a form of private property so that any taking or confiscation must be compensated. The legal challenge is to develop laws to rebalance informational asymmetries.

1.3 Purpose of the Study and Approach

The purpose of the study was to explore and evaluate the legal implications of DPSIP issues. The comparative study data were intended to be used to assist attorneys, business executives, judges, legal academics, governmental officials, and policy makers on both best practices and areas of improvement based on the experience of the international community—specifically, AU, CA, SA, the UK, and the US.

The approach involved three classic levels of policy analysis: macro, mezzo, and micro. The macro level of analysis involved looking at general theory and principles of international legal standards and generally accepted principles. The mezzo level involved research on the DPSIP laws, policies, and practices in AU, CA, the UK, and the US Finally, at the micro level, certain DPSIP law specifics were examined and then compared. The conclusions and recommendations were based on an integration and selection of best practices on all three levels.

Not all countries share a common interest or concern about DPSIP legal issues, and some do not even agree on the terminology or definitions. Accordingly, a range of legal responses was identified. This thesis examines the strict DPSIP legal standards of the E.U. and the UK, the "inadequate"

---

[30] David Brin, *The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?* (Basic Books ed. 1998).

[31] Jack Hirshleifer, Privacy: Its Origin, Function and Future, 9 *Journal of Legal Studies* 4, 649 (1980).

[32] Richard A Epstein, Deconstructing Privacy: And Putting It Back Together Again, in *The Right to Privacy* (Ellen Krankel Paul, et al. eds., Cambridge University Press 2000).

protections of AU, the "adequate" protections of CA, the sectoral "patchwork" pattern of protection laws in the US, and the evolving approach found in SA.[33]

As indicated above, key legal policies were not always common across these countries, and some terms were ill-defined. Thus, the study used the qualitative research strategy of textual analysis to help define essential terms. The texts included laws, treaties, court decisions, and authors who have focused on DPSIP. In addition to addressing poorly defined terms with linguistic-based approaches, essential common concepts were determined. Both linguistic and statistical techniques were used to derive useful categorical definitions and comparative insights.

1.4 Theoretical Framework

DPSIP issues cross a number of academic disciplines, including data, research, and theory from business, economics, jurisprudence, law, philosophy, political science, psychology, sociology, and technology. A multidisciplinary-systems thinking approach was appropriate as it was the standard in social science research. Thus, although the general focus of the study involved a comparative law research approach, the justification for concern was based on a sociolegal[34] approach.[35]

A comparative law research approach was used to focus on a legal analysis of various DPSIP approaches to the legal and policy issues. Academic research resources, black letter law, cases, and statutes presented a basis for comparison. A goal was to elucidate general approaches and results as distillation of essential lessons that would be legally and socially useful in legal policy reform. Lessons learned from other jurisdictions aided in establishing effective legal regulation. The approach involved critical

---

[33] Privacy International (2007, December).
[34] Some writers in the field, hyphenate sociolegal as Socio-legal.
[35] Roger Cotterrell, Subverting Orthodoxy, Making Law Central; A View of Socio-Legal Studies, 29 *Journal of Law and Society* 4, 675 (2002). *See also* Denis J. Galligan,

questioning of different legal practices, examination of legal effectiveness, and exploration of conflicts and differences using both primary and secondary sources.

The comparative law approach has both its supporters and critics.[36] The approach used in the current study attempts to maximize the strengths and compensate for the weaknesses of the model. The comparative law approach uses qualitative research methods; however, it also uses the rigor of the experimental approach.[37] The study compares worst case and best case approaches in building to a set of DPSIP legal recommendations.

1.5 Questions and Objectives Investigated

The basic questions and objectives investigated in this thesis were based on Sir Edward William Cooke's legal interpretation standards set in the *Heydon's Case.*[38] The issues must be addressed as they relate to the legal challenges of DPSIP. The Cooke tasks, as reworded for modernization and specificity, are:

1. "What was the common law before the making of the act." **What were the laws and international standards related to DPSIP legal principles before the advent of personal information becoming a commodity and means of social control?**
2. "What was the mischief and defect for which the common law did not provide." **What was the mischief and defect that allowed**

Socio-Legal Studies in Context: The Oxford Centre Past and Future (Journal of Law and Society Special Issues) (Denis J. Galligan ed., Wiley-Blackwell ed. 1995).

[36] Rudolf B. Schlesinger, *The Past and Future of Comparative Law*, 43 American Journal of Comparative Law 3, 477 (1995); Alan Watson, *Law Out of Context*, (University of Georgia Press ed. 2000). For a critical review, *see* George A Bermann, *The Discipline of Comparative Law in the United States.*, 51 Ruevu Internationale De Droit Compare' 4, 1041 (1999).

[37] Martin Shapiro, *Courts: A Comparative and Political Analysis.* (The University of Chicago Press. 1986).

[38] *Heydon's Case* 76 Eng. Rep. 637, (1584) (UK).

businesses and governments to violate DPSIP standards that the law did not adequately provide?

3. "What remedy the Parliament hath resolved and appointed to cure the disease of the commonwealth." **What comparative legal principles and procedures formed the "cure for the diseases" of the invasions of DPSIP?**
4. "The true reason of the remedy; … to make such construction as shall suppress the mischief, and advance the remedy, and to suppress subtle inventions and evasions for continuance of the mischief, and add force and life to the cure and remedy." **How can SA best respond to the DPSIP law principles?**

These issues and legal challenges must also be examined with a clear understanding of the context within which they emerged. The Internet began as an establishment[39] response to the need for connectivity between computer users. The early developmental phase was open and at times liberating. A policy decision was made to allow commercial activities on the Net, and access and activities grew internationally. Those who believed in behavioral control (Neo-Conservatives[40]) claimed that the Net and the information economy must be controlled using Industrial Age legal concepts. Claims were made that the Internet was a chaotic "Western wilderness." Commercial interests demanded historic protections and new opportunities. Then politicians, legislators, lawyers, and judges entered the fray, but fundamental DPSIP issues and questions remained unresolved. Initial responses ranged from the legally naive to the technologically and

[39] A government sponsored project between the military and academic establishments.

[40] A legal and political philosophy that resurrects fascist, Neo-Nazi, and pro-business positions that support unfettered capitalism, unregulated business, bare-bones government, and distains Judeo-Christian views. See Gary Weiss, *Ann Rand Nation: The Hidden Struggle for America's Soul* (St. Martin's Press ed. 2012) and Steven M. Teles, *The Rise of the Conservative Legal Movement: The Battle for Control of the Law* (Princeton University Press ed. 2008).

developmentally ignorant.[41] This thesis seeks to clarify the issues and principles to escape from the business/legal/political quagmire.

The general research questions were:

1. Could the law effectively respond to the fundamental DPSIP legal principles raised by computer technology and the information economy violations?
2. What were the national and international legal standards related to DPSIP legal principles before the advent of computer technology and the information economy violations?
3. What were the DPSIP mischiefs and defects that computer technology and the information economy opened up that the existing law did not adequately protect?
4. What DPSIP legal principles and procedures should form the "cure of the diseases" of the new information economy violations?
5. How can the law best respond to computer technology and the information economy challenges of fundamental principles of DPSIP law?

Specific research questions were:

1. Can DPSIP be protected from computer technology and the information economy violations?
2. What was the appropriate DPSIP law, and what was it based upon?
3. How are DPSIP legal principles violated?
4. Should DPSIP legal principles ever be violated?
5. Is there a proposal on how to best establish DPSIP law protections?

1.6 Conceptual and Substantive Assumptions

[41] Jonathan Zittrain, *The Future of the Internet and How to Stop It*, (Yale University Press ed. 2008). For an opposing view, see Amitai Etzioni, *The Limits of Privacy*, (Basic Books ed. 1999).

The study was based on a set of conceptual and substantive assumptions. These assumptions influenced the definition of the research problem and primarily directed the finding of relationships, making of comparisons, noting of changes, and identifying of possible cause-and-effect relationships. These assumptions included:

1. The Internet and information economy were in their infancy and would continue to evolve. The law has yet to play a significant role in the evolutionary development of the information economy. The law has understandably been reactive, but must also take a proactive role. The information economy would be better if general legal principles were established even if there were increased costs. DPSIP law must accept that different societies, countries, and groups have conflicts between different methods of and standards for acceptable behavior that must be harmonized. The issues involved major systemic concerns.
2. The law must be normative so that it encourages valued behaviors but does not ignore or fail to conform to data from other fields of study and research. The law must contribute to the evolution of a more orderly and just worldwide society.
3. The law must facilitate the will of the majority and protect the rights of the minority (i.e., the strong must not be able to dominate the weak). The law must openly encourage people to communicate, resolve differences, buy, sell, increase wealth, and protect information privacy data with their rights being predictable and protected. History shows that the law can be ignored, misused, used for oppressive or political purposes, or poorly reasoned.[42]
4. The law must be proactive in protecting data, security, and information privacy. Given that the information economy created much of the problem, this was the time for constructive correction and limitations on the power of the powerful.

[42] Detailed examples are discussed in Chapter Two.

1.7 Legal Rationale

DPSIP law should confront difficult, conflicting, diverse beliefs, and multiple issues, implications, and theories. Yet some legal principles remain constant, including that no people or states ought to profit from their own wrong behavior. People are entitled to dignity and autonomy, and they deserve to have their personal data and information privacy protected. In addition, people—not businesses or governments—must have control over their property and confidentiality rights. The law ought to protect the individual while constraining business and governmental abuses.

Furthermore, the law ought to guard against and eliminate arbitrary, capricious, and oppressive uses of state or business power. Unjustifiable arbiter or judicial decisions are not legitimate as they are not logically derived from generally accepted legal principles. The legal system must be obligatory.

DPSIP law must seek and maintain a high level of legitimacy via the effective and legitimate use of official power with sound checks and balances. Such laws and legal principles must deserve the people's respect.[43]

The law must address the challenges of DPSIP in an Information economy. The law must address the challenges from a multinational comparative analysis perspective.

1.8 Importance of the Study

The debate regarding computer technology and the information economy shifted from participant-determined consensus standards to the external regulators (software producers and business interests), then to nation-state laws and judicial standards, often with little regard for DPSIP. Some conflicts

[43] Tom R. Tyler, *Why People Obey the Law*, (Princeton University Press ed. 2006).

were addressed, but the implications were often ignored.[44] The nature of the new age and technology raised fundamental questions about historic DPSIP legal and policy concepts. Power bases were established and challenged. Nation-state courts and nongovernmental adjudicators issued conflicting, contradictory, and unenforceable decisions.[45]

This study addresses the fundamental issues by examining comparative DPSIP common law principles as the principles may or may not be related to the new legal challenges. The study defines the principles of DPSIP law, then compares and contrasts the DPSIP law found internationally in AU, CA, SA, the UK, and the US. Accordingly, the study provides a basis for clarifying the debates and exploring an action alternative for dealing with complex legal and technological issues on both a national and global basis.

On 20 August 2013, the SA National Assembly passed the Protection of Personal Information Act of 2013 (B9D-2009) (POPI).[46] Professor Graham Greenleaf noted that the POPI was the world's 101st DPSIP related law; the twentieth enacted in this decade, and the eleventh such law in sub-Saharan Africa.[47] The number of statutes is increasing and so are the differences.

1.9 Definition of Terms

The study uses some key terms, variables, and words of art that require clarity and preliminary definitions. Key operational definitions follow, including:

---

[44] *See* Lessig, *supra* note 13 (both works); *see also* Postrel, *supra* note 13.

[45] *See* Chapter Two through Chapter Nine.

[46] At the time of this writing, the bill still had to be translated into Afrikaans and the signature of President Jacob Zuma. The text can be found at http://d2zmx6mlqh7g3a.cloudfront.net/cdn/farfuture/HRSY-yvz5dgSfW8uBeBhCYbXCQLX14dx-YS7wdyFpfc/mtime:1376915982/files/130618b9d-2009.pdf.

[47] David Graham, *Protection of Personal Information Bill will make or break online marketing in SA.* (1 September 2013, at <http://ph.news.yahoo.com/protection-personal-information-bill-break-online-marketing-sa-043852707.html?.tsrc=warhol>.

***Common Law*:** The legal tradition stemming from the use of judicial decisions, based on precedence, to define the law as opposed to a set written code. This tradition is in contrast to the civil law tradition where there is a basic written code. The UK, the US (except Louisiana), CA (except Quebec), and AU have a strong common law tradition. SA, Quebec, and Louisiana have a mixed jurisdiction tradition. The responses of these common law countries to DPSIP vary, and are explored in the study. Each of these countries has developed an increased reliance on comprehensive codes[48] but fundamental concepts of the nature of law and rights generally remain.

***Data Protection*:** Technical security and legal restrictions on the use, release, sale, rent, lease, sharing, and theft of personal information. Most data protection statues require: (1) that the data be accurate; (2) that the collection be adequate, relevant, and not excessive; (3) that the information be fairly and lawfully processed; (4) that the information be kept secure and not be kept longer than necessary; (5) that the information not be transferred abroad without adequate protection; (6) that the data be processed only for limited purposes; and (6) that the data be processed in accordance with informational privacy rights. Although *data protection* refers to computer and data security issues, the term was used in the EU as synonymous with information privacy.

Data Security: Closely related to data protection and information privacy with the concepts and practices being interdependent. *Tasks* cover all administrative, physical, and technical safeguards used in an information system. *Security* involves access to data; its disclosure, disruption, destruction, unauthorized modification, or use; and protection from data corruption. Data backups, encryption, firewalls

---

[48] US Rules of Civil Procedure, *Rules of Civil Procedure*. (2006), at http://www.law.cornell.edu/rules/frcp/index.html (last visited on 25 September 2012). US Rules of Evidence, *Rules of Evidence*. (2006), at http://www.law.cornell.edu/rules/fre/index.html (last visited on 22 September 2012). Uniform Commercial Code, *Uniform Commercial Code*. (2001), at http://www.law.cornell.edu/ucc/ucc.table.html (last visited on 22 September 2012).

controlling access, technical protections, and use are cardinal elements. The International Standard ISO/IEC 1779 addresses these protections as information security. The literature also uses the terms *computer security* and *information assurance.* Data holders must identify the parties who are clearly responsible to protect and control access to the data.[49]

***Information Privacy*:** The right of "individuals, groups, or institutions to determine for themselves when, how, and to what extent information about themselves is communicated to others."[50] The law recognized a legal right to informational privacy and a limited right to access governmental information. Individuals have a legal interest in control over personal information. The only modifier is when there is a significant public need.[51] Information privacy is a form of information control, confidential knowledge control, and an asset that has property right considerations owned by the person—the right to exercise legal control over the person's information.[52] The responsibility for protecting information privacy resides within the law and governments committed to the rule of law. The focus is on personally identifiable information (PII) and data mining that can lead to PII.

---

[49] ISO/IEC, *17799:2005 Information Technology - Security Techniques - Code of Practice for Information Security Management*. (2005), at http://www.iso.org/iso/support/faqs/faqs_widely_used_standards/widely_used_standards_other/information_security.htm (last visited on 1 June 2012). *See also* 44 U.S.C § 3542(b)(1) (2006). (US)

[50] Alan F. Westin, *Privacy and Freedom*, (Atheneum ed. 1967). *See also* Allen F. Westin & Michael A. Baker, *Databanks in a Free Society: Computers, Record-Keeping & Privacy. National Academy of Sciences. Washington. D.C. Project on Computer Databanks*, (Quadrangle Books ed. 1972).

[51] Restatement (Second) of Torts (1977).

[52] See Richard A Epstein, Deconstructing Privacy: And Putting It Back Together Again, in *The Right to Privacy* (Ellen Krankel Paul, et al. eds., Cambridge University Press 2000); Lawrence Lessig, *Code and Other Laws of Cyberspace*, (Basic Books ed. 1999); and Lawrence Lessig, *Code: Version 2.0*, (Basic Books ed. 2006).

***Information Privacy Law*:** "A mosaic of various types of law: tort law, constitutional law, federal and state statutory law, evidentiary privileges, property law, and contract law."[53]

***Privacy*:** The term is used in a broad range of situations. The legal literature notes that there are four types of privacy: decisional, informational, physical, and proprietary.[54] The focus of this work is on information privacy with some consideration of proprietary concepts.

1.10 Description of Research Methodology and Approach

The basic structure of the study involves building on the author's strong professional interest in the topic. A general research strategy was developed that included identifying resources and issues. The research topics were carefully defined, questions were developed, theories were reviewed, and rationales were delineated. Then the collection and organization of additional information was begun, with the process including periodic evaluation of the research questions, methodologies, and data collected. Additional information was organized and evaluated, and interpretive theories were revised. Finally, the results were interpreted and the findings prepared.[55]

This study used a hermeneutic approach in that laws, cases, writings, and policies were interpreted and meanings transcribed. The focus was on understanding the issues and the context that gave them meaning. The textual meaning was considered to be an interaction between the views that meaning was independent from the interpreter and that it was dependent on the interpreter. The source materials were analyzed within a historical context

---

[53] Daniel J. Solove, *The Digital Person: Technology and Privacy in the Information Age*, (New York University Press ed. 2004).

[54] Anita L Allen, Privacy as Data Control: Conceptual, Practical, and Moral Limits of the Paradigm, 32 *Connecticut Law Review* 3, 861 (2000); Anita L. Allen, Privacy in American Law, in *Privacies: Philosophical Evaluations* (Beate Rossler ed., Stanford University Press 2004).

[55] *See* R. Murray Thomas & Dale L. Brubaker, *Theses and Dissertations: A Guide to Planning, Research, and Writing*, (Bergin & Garvey ed. 2000).

but applied to current problems. Martin Packer[56] argued that "The difference between a rationalist or empiricist explanation and a hermeneutic interpretation was like the difference between a map of a city and an account of that city by someone who lives in it and walks its streets." This study used both perspectives.

The focus of the research was on generating knowledge rather than accumulating information. The expressed purpose was to present alternatives and action for legal analysis and change.[57]

The research approach involved an integration of key components of the major social science and legal research approaches and methodologies. Questions were developed based on education, training, and experiences. Data were obtained by a systematic use of primary, secondary, and theoretical sources. The focus was on providing perspectives for evaluating alternative decisions and policies.

Historical approaches were used to accurately and objectively reconstruct key issues and principles as much as possible. The areas of concern were approached from a descriptive methodology to accurately, factually, and systematically describe the DPSIP legal issues and trends. The shift from the industrial economy to an information economy was evaluated from a developmental perspective to identify the changes, patterns, and sequences over time. Causal-comparative or ex post facto approaches were used to observe possible and plausible casual privacy invasion factors. The approach ended with an action orientation to identify approaches to address the information age-related legal challenges as a catalyst for a rational exploration of fundamental DPSIP law principles.[58] The integrated research design was

---

[56] Martin J. Packer, Hermeneutic Inquiry in the Study of Human Conduct, 40 *American Psychologist* 10, 1081 (1985).

[57] Davydd J. Greenwood & Morten Levin, *Introduction to Action Research: Social Research for Social Change*, (Sage ed. 1998).

[58] Stephen Isacc & William B. Michael, *Handbook in Research and Evaluation: A Collection of Principles, Methods, and Strategies Useful in the Planning, Design, and Evaluation*

necessary because of the complexity and importance of the DPSIP legal issues in the current age.[59]

Given that the design depended on historic information written and observed by others, such information was analyzed to determine the accuracy, authenticity, and significance of the materials. The design required a demanding, disciplined, exhaustive, rigorous, and systematic approach so as to collect appropriate, reliable, and unbiased information. Thus, the design required the author to constantly monitor biases, motives, and information that might filter out possible distortions or exaggerations or permit key data to be overlooked. The steps included defining the problem, stating the research objectives, collecting the data, evaluating the information, and reporting the findings. There were sufficient primary and secondary balanced data available for examination of the issues. Attempts were taken to adequately evaluate the historical data. Personal biases were monitored so as to not negatively influence the process. The data were integrated and synthesized in order to reach meaningful conclusions.[60]

This comparison of the international legal, regulatory, and enforcement mechanism of the AU, CA, SA, the UK, and US approaches to DPSIP law or developments was essentially a case study design. A focus included the developing DPSIP privacy law in SA. A case study approach was appropriate for this thesis because it was a "strategy for doing research which involves an empirical investigation of a particular contemporary

---

of Studies in Education and the Behavioral Sciences, (Edits/ Educational and Industrial Testing Services 3rd ed. 1995).

[59] *Id.* at 48–59. The descriptions include **Action:** develop new skills or new approaches and to solve problems with direct application to the world setting **Causal-comparative**: investigate possible cause-and-effect relationships by observing some existing consequence and searching back through the data for plausible causal factors. This was in contrast to the experimental method which collects its data under controlled conditions in the present. **Descriptive:** describe systematically the facts and characteristics of a given … area of interest, factually and accurately. **Developmental:** investigate patterns and sequences of growth and/or changes as a function of time. **Historical:** reconstruct the past systematically and objectively by collecting, evaluating, verifying, and synthesizing evidence to establish facts and reach defensible conclusions often in relation to particular hypotheses.

[60] *Ibid.*

phenomenon within its real life context using multiple sources of evidence."[61] Yin and Campbell declared that "in general, case studies are the preferred strategy when 'how' or 'why' questions are being posed."[62]

The design required describing events, situations, policies, treaties, legal principles, laws, and court decisions. The accumulated efforts resulted in a detailed database, which was used to explain relationships, formulate implications, make predictions, identify meaningful patterns, and test hypotheses. The patterns of the variables were examined to determine their development, growth, and regressions. Interrelated factors and sequences were tracked. A look at the developmental patterns globally and within selected nations avoided possible attribution errors and biases.[63]

The design involved looking at areas of interest that had already occurred. The effort included analyzing "causes, relationships, and their meanings."[64] Classic experimental methods were considered to be inappropriate to the topics. Such methods were also not possible because dependent and independent factors could not be reliably selected, controlled, or manipulated in a non-artificial or realistic manner. However, the design did provide reliable data about the DPSIP legal issues in the information economy.

The design provides practical and relevant information for lawyers, judges, legal scholars, legislatures, business executives, and policy makers. The effort provides a structural model for problem solving, guidelines, and principles for evaluating new developments. In addition, the thesis design provides for a means to avoid fragmentary, impressionistic, short-term, and ill-advised decisions.

---

[61] Colin Robson, *Real World Research: A Resource for Social Scientists and Practitioner-Researchers*, (Blackwell 2nd ed. 2002).

[62] Robert K. Yin, *Case Study Research: Design and Methods*, (Sage Publications 4th ed. 2009).

[63] Isacc & Michael, *supra* note 53.

[64] *Id.*at 54.

1.11 Data Collection Procedures

The data was obtained by the use of phenomenological and more objective data collection procedures. This research was influenced by both sets of approaches.

The phenomenological experiences included the author's experience with information technology, the Internet, and information privacy concerns. The author's first experiences started with the use of the University of Southern California's punch card computer system and the Statistical Package for the Social Sciences (SPSS) to do the statistical analysis for a PhD dissertation[65] and the use of an Apple II Plus floppy disk computer with a 300 baud modem to connect with a regional bulletin board and users' group.

Data and insights that included international perspectives were obtained from the author's years of teaching, consulting, mediating, and arbitrating regarding information age, Internet, and legal issues. Participation in the World Intellectual Property Organization's *WIPO Workshop for Arbitrators* in Geneva showed the intense conflicts and feelings related to the issues. Additional participation in and facilitation of interest groups at three Harvard Law School/Beckman Center for Internet and Society and one Stanford University Law School's Internet Law Summer programs provided data, perspectives, and discussions with faculty and participants from a range of countries. In addition to prior thesis and dissertation research and teaching, the data collection training included participation in the *Legal Research on the Internet* program conducted by the University of Toronto Law School. Assistance was also found at the University of Ottawa Law's *The Internet and the Law: A Global Conversation* program, and Yale University Law School's *The Global Flow of Information: Law, Culture and Political Economy.* Faculty input from the International Association of Privacy Professionals 2006 Privacy Academy and the 2007 Privacy Summit was also used.

Objective data collection included research strategies using Lexis-Nexis, Westlaw, governmental websites, legal research sites, mega and specific search engines, local university and law school libraries, and the law school library at the University of South Africa. Careful notes were taken on desk and laptop computers.

Books, collections, and journals were consulted. Statutory, administrative, and common law sources were reviewed using case reports and digests. Primary sources (including constitutions, declarations, court decisions, regulations, statues, treaties, and hearing records) were consulted to determine mandatory and persuasive authorities. Secondary sources including *American Law Reports Annotated*, commentaries, *Current Law Index,* hornbooks, *Index to Legal Periodicals,* law review articles, legal encyclopedias (*Corpus Juris Secundum* and *American Jurisprudence 2nd)*, *Legal Resource Index*, legal treatises, legislative histories, *Restatements of the Law*, Uniform Laws and Model Acts, *Words and Phrases*, and other writings were researched.

The data collection process followed a structured system approach. The approach included searching: computerized legal research tactics; generalized sources in law, policy, business, and the Internet; known topics; known authorities; descriptive words; descriptive facts; and legal authority updates.[66]

The process was guided by the principles that the purpose of legal research is to examine sets of actual or potential facts to determine the legal consequences. The process included preparation and redefining of the initial issues statement; preparing and refining search terms; outlining potential sources; gathering the facts to narrow the research focus; analyzing the facts;

---

[65] Known as a thesis in SA, the UK and some other countries and institutions.

[66] Christopher G. Wren & Jill R. Wren, *The Legal Research Manual: A Game Plan for Legal Research and Analysis*, 77-78 (Adams & Ambrose Publishing 2nd ed. 1986).

gathering more facts; identifying the legal issues raised by the facts; and arranging the legal issues in a logical order for research.[67]

1.12 Data Processing and Analysis

As much as possible, steps were taken to insure the reliability and validity of the data. Safeguards included obtaining multiple accounts and diverse views as well as integrating social, cultural, political, business, and information technology views as part of the legal analysis. Only respectable sources and authors were consulted. Data and studies were synthesized, diversities were revealed, inconsistencies and exceptions presented, applications illustrated, and principles and propositions were generated.[68]

The analysis and interpretation of the data were subjected to a preset plan. The steps included comparing and contrasting the factors addressed. Where possible, patterns were identified to determine if correlations existed based on explanatory or predictive interpretations. Trends and patterns were identified. Conventional wisdom was challenged, and some alternative meanings proposed. The issues of altering beliefs and behaviors were examined. Business practices, technological events, and legal practices were also evaluated.[69]

The black letter law[70] of the selected nations provided descriptions of the formal legal principles, and rules were applied. Cases and statutes were examined. A formal black letter law approach for this topic was rejected as being too narrow.

---

[67] *Id.* at 29; Amy E. Sloan, *Basic Legal Research: Tools and Strategies*, (Aspen Law & Business ed. 2000).

[68] R. Murray Thomas & Dale L. Brubaker, *Theses and Dissertations: A Guide to Planning, Research, and Writing*, (Bergin & Garvey ed. 2000).

[69] *Ibid.*

[70] Legal principles that are accepted, fundamental, and well-settled. *See* Bryan A. Garner, *Black's Law Dictionary* 163 (Bryan A. Garner ed., West Group 17 ed. 1990).

Use of sociolegal research strategies provided a means to address relevant qualitative and quantitative data. DPSIP law operates within cultural, business, economic, political, psychological, and social contexts, so establishing sound legal standards required an interdisciplinary approach. Thomas argued that "Empirically, law is a component part of the wider social and political structure, is inextricably related to it in an infinite variety of way, and can therefore only be properly understood if studied in that context."[71]

Some elements of a historical approach were used. Understanding the comparative developments of DPSIP law was critical to understanding the issues and current practices. Understanding the context of national and international standards was essential in critically evaluating the success and failure of different national approaches to the issue. The past and present DPSIP issues were part of the legacy and current responses.

The major structure of the approach was a comparative law one. The globalization of DPSIP legal realities dictated the need for understanding and approaching the extant differences in standards in the various countries. The approach provided data for SA to learn from the successes and failures of other national approaches. Academic articles, cases, and statutes from the selected nations were reviewed.

Although the approaches taken by the countries included in this study differ widely, issues confronted by different nations are not unique; therefore, the methodology employed in this study allowed for an examination of parochial assumptions. Although not always binding, different national experiences and standards can be persuasive authority. Conflicts and differences in legal standards and approaches can be used to develop a more common ground approach.[72]

---

[71] Phillip Thomas, Curriculum Development in Legal Studies, 20 *Law Teacher* 2, 110 (1986).

[72] *See* Michael Salter & Julie Mason, *Writing Law Dissertations: An Introduction and Guide to the Conduct of Legal Research*, (Pearson Longman ed. 2007).

The methodology also incorporated the qualitative research strategy of textual analysis. The texts analyzed included laws, treaties, court decisions, and authors addressing DPSIP legal issues. Moreover, both linguistic and statistical techniques were used to derive useful categories of definitions and comparative insights. Version 2.1 of the SPSS Text Analysis and Version 7 of the Nvivo software were used to assist in determining analysis patterns.

The function of the data processing and analysis was to attend to key legal issues and responses to DPSIP. The task was to raise questions and suggest a possible course of action. In the collection of data, treatment, and data processing procedures, the author used standard research and legal scholarship methods.

1.13 Comparative Law Analysis

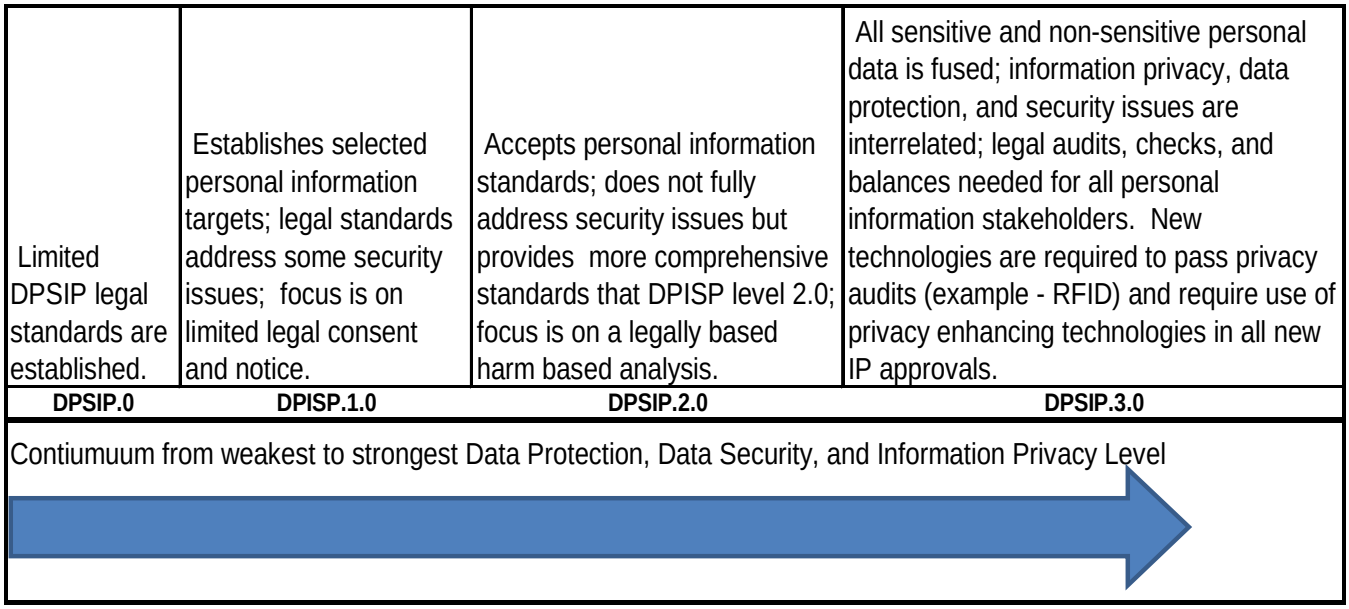
In a comparative law study, a similar set of issues ought to be used to gather information on the laws, jurisprudence, and policies of all of the nations in the study. In this study a number of general factors are considered as questions. A comparative law analysis of the positive law and policies of each country will be reported. The responses include current, historical, and proposed legal standards. The questions are:

1. Do the legal standards in the country provide a legal basis for DPSIP Protections?
2. Does the country provide legal support for corporate privacy and data or property protections?
3. Do the DPSIP declarations provide clear information privacy, data protection, and data security standards?
4. Does the law and policy of the country require DPSIP Regulatory Agencies?
5. Do the laws of the county provide for related consumer protection standards?
6. Are legal standards established that apply to data controllers?
7. Does the country have data processor requirements?

8. Are data subjects legally protected?
9. Does the law provide for strong data security and destruction standards?
10. Does the law address cross-border data flows and transfers?
11. Does the law provide for checks and balances related to exemptions and exceptions?

From an international perspective, DPSIP laws and policies have gone through, at this time, four evolutional stages. The current standards of each country will be evaluated based on a continuum:

Figure 1.3 Continuum of DPSIP Approaches



1.14 Methodological Assumptions

Stephen Isacc and William Michael argued that "measurement of multiple outcomes is preferable to measurement of a single outcome."[73] Thus, this study was based on a set of operational and methodological assumptions that included: (1) no single research or legal methodology could adequately address the legal issues involved; and (2) black letter law, socio-legal, and comparative law research strategies would provide the most comprehensive

research approach. A systematic review of the primary and secondary legal resources could contribute to understanding the issues and address trend concerns. The selected methods and the study could be a preliminary view and call for action. Finally, the study could provide a basis for further work and actions.

The methodology met the fundamental assumptions of the qualitative method.[74] The holistic assumption was that the entirety of the legal issues with DPSIP law were more than and differed from the sum of the parts. The focus of the study sought to address the DPSIP phenomena and to develop a more complete understanding of the issues. The inductive assumption was that the approach could use specific observations as a means toward understanding emerging general patterns. The naturalistic inquiry assumption was that the phenomena could be understood in the natural national and international environment.

1.15 Limitations of Assumptions

As the study included a trend studies approach, the approach may have been "vulnerable to unpredictable factors."[75] The design did not involve any direct control over the variables, but plausible rival data and hypotheses were considered. Accordingly, some relevant causal issues may have been missed. Some other combinations or interactions may have occurred, and cause-and-effect relationships may have been misinterpreted. Although every effort was made to be thorough, DPSIP is an emerging field of study, and some other factors may not have been recognized. Specifically, some of the factors and issues may have been too political, unclear, variable, or transitory.[76] In addition, some of the sources relied upon may have been "incomplete or badly biased."[77]

---

[73] Isacc & Michael, *supra* note 53, at 100.
[74] Michael Quinn Patton, *Qualitative Research & Evaluation Methods*, (Sage 3rd ed. 2001).
[75] Isacc & Michael, *supra* note 53, at 100.
[76] *Ibid.*
[77] R. Murray Thomas & Dale L. Brubaker, *Theses and Dissertations: A Guide to Planning, Research, and Writing*, (Bergin & Garvey ed. 2000).

1.16 Summary of Problem

Advances in computer technology (including data collection, uses, abuses, and cost reductions) impacted data protection and security concerns. Personal information became a valuable commodity. Businesses and governments used and abused their access to and use of personal data. Traditional views, powers, and legal abilities of nation-states to deal with emerging DPSIP legal issues became inadequate. The legal response was understandably slow, with the law generally not being timely in responding to the technology-driven evolution.

The law could respond to the changes by denying the change and imposing traditional legal standards. Alternatively, the law could adopt technology-specific standards, and specialized courts of special jurisdiction could be established. The law could accept the view that technology issues often mask complex legal issues. A comparative evaluation of international and different national legal traditions could provide direction to SA's approach to establishing DPSIP legal standards. The legal standards, approaches, and problems of AU, CA, SA, the UK, and the US were selected for evaluation.

1.17 Summary of Literature and Issues Reviewed

Chapter one introduced the importance DPSIP law and many of the problems related to it since the development of computer technology and the information economy. Private data has always been collected, but massive abuses and potentials of abuse were evident. During World War II, Germany was the first nation-state to use computers and data to help identify and kill millions. More modern governments and business concerns used the process to further power goals. Private information became a valuable commodity that was bought and sold without the individuals involved being aware. The problems of DPSIP law were introduced, and the concerns for people's privacy were examined. Data on security flaws were presented along with business use and abuses that went along with governmental use and abuses.

The grab for power over information and knowledge was described. DPSIP law threats and problems were explored, and the background of the problem was examined. Finally, the advantage of a comparative study of DPSIP law approaches was documented.

The study rationale and theoretical framework have been addressed. The study questions and objectives, conceptual and substantive assumptions, and legal rationale have been described. The research approach, study questions, importance of the study, definition of terms, and methodology overview were presented. The research design, data collection procedures, data processing and analysis have been described. The methodological assumptions, limitations of assumptions, and null conceptual and research questions have been described.

The methodology involved the integrated use of classic action, causal-comparative or ex post factor, descriptive, developmental, and historical designs. The work involved collection, review, and analysis of theoretical, policy, legislative actions, and court cases related to DPSIP issues. A major focus was on activities in common law countries. Developments in AU, CA, the E.U., the UK, and the US along with related international actions were introduced.

The focus of this thesis was to compare the background, models, and laws of selected jurisdictions that had taken different approaches to the issues. The work presents the best practices found in each area to help make recommendations for changes and adoptions regarding each system. The work looks at the errors of the DPSIP approach in each country to formally address the issues while the thesis looks at the SA experience in the hope that it did not repeat the errors of others in its efforts to establish greater protections. The thesis made recommendations for changes for each national and international approach.

1.18 Outline of the Thesis

The thesis chapters follow a consistent organizational structure that involve macro, mezzo, and micro levels of analysis. The chapters address specific DPSIP legal issues confronted by computer technology and the information economy.

Each of the issue chapters addresses the topics from both a legal and multidisciplinary (legal, political, technology, cyber culture, psychosocial, and business) perspective. Generally, each contains an overview followed by a presentation of historical definitions, developmental history, and historic and current legal and policy standards. Information economy challenges and evolving information economy legal standards are addressed. Present and predicted future policy concerns are delineated. Each chapter concludes with a summary of the findings and issues reviewed with a preview of the next chapter.

The chapter topics addressed include:

- "Chapter Two: Data Protection and Security Law: Socio-Legal Issues," which looks at the question: What are the multidisciplinary contributions to understanding DPSIP legal issues?
- "Chapter Three: International Legal Standards and Guidelines" wrestles with the question: What international legal standards, governmental guidelines, and nongovernmental guidelines address DPSIP issues?
- "Chapter Four: Australian Legal Standards and Approaches" presents and critically evaluates this national approach to DPSIP issues and experience, with both success and failures being examined.
- "Chapter Five: Canadian Legal Standards and Approaches" presents and critically evaluates this national approach to DPSIP issues and experience, with again success and failures being examined.
- "Chapter Six: South African Legal Standards and Approaches" presents and critically evaluates this national approach to DPSIP issues and experience, as always success and failures are examined.

- "Chapter Seven: United Kingdom Legal Standards and Approaches" presents and critically evaluates this national approach to DPSIP issues and experience; success and failures are examined.
- "Chapter Eight: United States Legal Standards and Approaches" presents and critically evaluates this national approach to DPSIP issues and experience, and also examines success and failures.
- "Chapter Nine: Data Protection and Security Law: Comparative Evaluation" presents an interdisciplinary comparative analysis of the insights and legal principles gained in the prior chapters and perspectives. The results of case study, linguistic analysis, positive law, qualitative, quantitative, and sociolegal research approaches are presented.
- "Chapter Ten: Data Protection and Security Law: Gold Standard Proposal" presents proactive implementation recommendations based on recent and current DPSIP experience, legal developments, literature, and research. The chapter argues that SA ought to seriously consider the new gold standard in its DPSIP legal approach. The chapter further argues that the nation states and regions addressed in the study ought to learn from one another and adopt the new DPSIP gold standard.

CHAPTER TWO: DATA PROTECTION AND SECURITY LAW: SOCIOLEGAL ISSUES

> *An ideal system of law should draw its postulates and its legislative justification from science. As it is now, we rely upon tradition, or vague sentiment, or the fact that we never thought of any other way of doing things, as our only warrant for rules, which we enforce with as much confidence as if they embodied revealed wisdom. … How much has reason had to do in deciding how far, if at all, it is expedient for the State to meddle.*
> Oliver Wendell Holmes, Jr.[1]

2.0 Overview

Chapter two examines DPSIP issues from a sociolegal perspective. The psychosocial research relevant to DPSIP and public concerns for increased legal involvement are explored. Data is presented from AU, CA, SA, UK, and US research. The chapter presents an analysis of the psychosocial and legal factors related to DPSIP problems.

Data is presented that considers the psychosocial factors of DPSIP issues and establishes the need for legal regulations to address DPSIP problems. The majority of those surveyed in the five target countries wanted increased data protection and data security legal standards. The research showed that personal information had become a valuable commodity. The sociolegal literature revealed that businesses and governments had not adequately addressed DPSIP issues. A number of analogous legal principles support the need for strong DPSIP legal and regulatory standards. The principles include informed consent, confidentiality, impact assessments, and the need for

---

[1] Oliver Wendell Holmes, *Collected Legal Papers*, at 139 (Harcourt Brace and Company 1920).

audits. The research showed that governments had even granted intellectual property protections for technological innovations without assessing or examining the DPSIP implications. Research is presented that shows that data protection and security violations threatened basic legal principles and the security of individuals, businesses, and even governments. Asset protection standards, contract law issues, information and knowledge control law issues, intellectual property law issues, personal property law issues, tort law issues, and privacy law conflicts are assessed. The chapter ends with a summary of the sociolegal literature and issues.

2.1 Psychosocial Factors of Data Protection, Security and Information Privacy

Data protection and security is more than a legal debate. The concepts, principles, and laws form legal standards, yet psychological and psychosocial realities also exist. The law must recognize relevant psychological and psychosocial research findings. Psychologically, the ability to control personal information is critical for human development and functioning. Such control impacts on the public self's ability to influence the boundaries between the self and others.[2]

DPSIP has been the focus of study from a range of disciplines. Ideally, the law should integrate aspects of theory, research, and data from legal history, business practices, political science, philosophy, psychology, and sociology. Eric Fromm, the famous psychoanalyst, wrote about issues of freedom and liberty, and data protection. He declared that freedom, liberty, and privacy controls impact individual and group functioning. Having faith in oneself and life are essential. *Utmost vigor* is required to ensure people's sensitive information remains under their control. The issues are quantitative and qualitative.[3] Many prominent legal scholars, philosophers, psychologists, and

---

[2] Bradley J. Alge, Effects of Computer Surveillance on Perceptions of Privacy and Procedural Justice, 86 *Journal of Applied Psychology* 4, 708 (2001), at 798.

[3] Eric Fromm, *Escape from Freedom*, at 126 (Holt, Rinehart & Winston, Inc. 1941).

other thinkers have weighed in on these issues; a summary of the most important positions with commentary from the current author follows.

Oscar Ruebhausen and O. Brim support the Fromm position. The authors found that people need to have the power to determine when and with whom personal information is shared. People function at a higher level when they can control the sharing or withholding of information on attitudes, behavior, beliefs, and options. Privacy control is a freedom essential to *personal dignity*.[4]

Perhaps the best description of the psychological and psychosocial principle supporting the need for data protection and information privacy was argued by Immanuel Kant. He explained, “Man is inclined to be reserved. ... Everyone has a right to prevent others from watching and scrutinizing his actions."[5]

Writing from a legal perspective, Charles Fried expanded the Kantian view. He maintained that information privacy is critical to maintaining functional relationships. Such privacy and control is a means and an end to respect and trust.[6]

Information privacy represents and performs a vital psychological and social function. Individuals are more than social and political entities. Individuals are discrete human beings with rights. Information privacy has a vital psychological aspect that is an integral part of functional autonomy and self-development.

---

[4] Oscar M. Ruebhausen & O. G. Brim, Privacy and Behavioral Research, *65 Columbia Law Review* 2, 1184 (1965), at 1211.

[5] Immanuel Kant, *Ethical Duties Toward Others: Truthfulness*, at 225 (Louis Infield trans., Hackett Publishing Company 1930).

[6] Charles Fried, *Privacy (A Moral Analysis),* in *Philosophical Dimensions of Privacy: An Anthology* at 205 (Ferdinand David Schoeman ed., Cambridge University Press 1984).

Abraham Maslow[7] wrote about human needs. The basic need, the one upon which all other psychological needs are based, was security. Information privacy is an element of security. Julie Inness wrote that privacy infringements resulted in a sense of harm including a fundamental loss of agency and even violation.[8] Privacy allowed people to interact with others on the basis of individual demands and to influence interpersonal relationships. Protections against the public gaze were seen as essential for a functional emotional life. A lack of information privacy violations crippled relationships for other productive purposes.[9]

Alan Westin argued that all animals, including humans, have mechanisms that protect privacy between other members of the species.[10] Robert Ardrey[11] established a biologically based need for a range of privacy protections. Louis Hodges[12] argued that privacy was necessary for civilization and sound human relationships.

Louis Fried supported the psychological need for information privacy in social relations. Fried argued that information was a moral capital that people can choose to share or not share.[13] Ruth Gavison took the need for information privacy a step further, arguing that information privacy allowed autonomy, human relations, liberty, and the survival of a free society.[14]

The importance of and correlation of information privacy and psychological well-being have been the subject of a number of scientific studies. The two principles and dynamics are connected. Judee Burgoon established the psychological and

---

7 Abraham H. Maslow, *Toward a Psychology of Being* (3rd ed., John Wiley & Sons 1999).

8 Julie C. Inness, *Privacy, Intimacy and Isolation*, at 3 (Oxford University Press 1992).

9 Thomas Nagel, Concealment and Exposure, 27 *Philosophy and Public Affairs,* 1, 3 (1998), at 17 & 20.

10 Alan Westin, *Privacy and Freedom*, at 8 (Atheneum 1967).

11 Robert Ardrey, *The Territorial Imperative* (Atheneum 1966).

12 Louis W. Hodges, The Journalist and Privacy, 9 *Journal of Mass Media Ethics*, 4, 97 (1994), at 200.

13 Charles Fried, Privacy, 77 *Yale Law Journal* 75, 475 (1968), at 492.

14 Ruth Gavison, Privacy and the Limits of Law, 89 *Yale Law Journal* 3, 421 (1980), at 423.

psychosocial significance of people having control over information release and *subsequent distribution and use*.[15] Irwin Altman clearly documented the need for information privacy as a psychological imperative for psychosocial well-being and functioning. Privacy involved access control for the individual and the group.[16]

Sandra Petronio showed the psychological importance of having control over one's personal information. She found that historically, people had established criteria and rules to protect themselves and those things seen as critical. Modern technology did not eliminate the need for information control.[17] Petronio also argued that privacy management was a demand-response between at least two people. When given the right to disclose, people used five factors in deciding when to release data: the "(1) need to tell, (2) predicted outcome(s), (3) riskiness of revealing the specific information, (4) privacy level of the specific information, and (5) degree of emotional self-control."[18]

Valerian Derlega and Alan Chaiken defined privacy from a psychological and psychosocial perspective. The essential feature of information privacy was control over all aspects of self-disclosure and was a psychological imperative. Maintaining regulatory control over the use and release of personal information protected one from vulnerability and others' control.[19]

From a psychological and psychosocial perspective, information privacy was an imperative. Information privacy has had powerful consequential and meaningful impacts on personal and societal wellbeing.[20] Research in

---

15 Judee K. Burgoon, *Privacy and Communication*, in *Communication Yearbook* 6 (Michael Burgoon & Noel E. Doran eds., 1982), at 230.

16 Irwin Altman, *The Environment and Social Behavior: Privacy, Personal Space, Territory, Crowding*, at 18 (Brooks/Cole Publishing Company 1975). Also see Irwin Altman, Privacy: A Conceptual Analysis, 8 *Environment and Behavior*, 1, 7 (1976).

17 Sandra Petronio, S. (1991). Communication Boundary Management: A Theoretical Model of Managing Disclosure of Private Information between Marital Couples 1 *Communication Theory,* 4, 311, at 311.

18 *Id.* at 314–316.

19 Valerian J. Derlega & Alan L. Chaiken, Privacy and Self-Disclosure in Social Relationships, 33 *Journal of Social Issues* 3, 102 (1977), at 102,103, 109.

20 Gary B. Melton, The Significance of Law in the Everyday Lives of Children and Families, 22 *Georgia Law Review* 851 (1988); James Rachels, Why Privacy is Important, 4

anthropology, architecture, design professions, law, political science, psychology, and sociology supports that conclusion.[21] "Respect for another's privacy is a legitimate expectation in all social relationships. As a value, privacy does not exist in isolation, but is part and parcel of the system and values that regulates action in society."[22]

Alan Westin summarized the psychological and sociological research related to information privacy. People had a need for autonomy, avoidance of manipulation, and protection from dominance by others. Inner zones of privacy control were essential to survival.[23] Westin also noted cases where information privacy violations caused damage including nervous breakdowns and suicides. The sources of violation included governments and businesses. He argued that only grave policy needs could be used to justify information privacy exemptions.[24]

Robert Laufer and Maxine Wolfe[25] maintained that information privacy involved information and interaction management. The study found that individuals whose private data were violated reported significant levels of loss of control not only of the information but also in interaction boundaries.

Ferdinand Schoeman[26] analyzed the psychological and psychosocial research related to information privacy. He found that both the information content and the role

---

Philosophy & Public Affairs, 4, 323 (1975); Charles R. Tremper & Mark A. Small, Privacy Regulation of Computer-Assisted Testing and Instruction, 63 *Washington Law Review* 3, 841 (1988).

21 Irwin Altman, Privacy: A Conceptual Analysis, 8 *Environment and Behavior* 1, 7 (1976), at 7.

22 Arnold Simmel, *Privacy Is Not An Isolated Freedom*, in *Privacy (Nomos, XIII)*, at 71 (J. Ronald Pennock & John W. Chapman eds., Atherton Press 1971).

23 Alan Westin, *Privacy and Freedom*, at 33 (Atheneum 1967). Also see Allen F. Westin & Michael A. Baker, *Databanks in a Free Society: Computers, Record-Keeping & Privacy*. National Academy of Sciences. Washington. D.C. Project on Computer Databanks (Quadrangle Books 1972).

24 *Id.* at 33–34.

25 Robert S. Laufer & Maxine Wolfe, Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory, 33 *Journal of Social Issues* 3, 22 (1977).

26 Ferdinand D. Schoeman, *Privacy and Intimate Information*, in *Philosophical Dimensions of Privacy: An Anthology,* at 405-406 (Ferdinand D. Schoeman ed., Cambridge University Press 1984).

that the information played were critical to an individual's sense of self and relationships with others.

As this brief review of the major psychosocial and legal factors related to DPSIP problems clearly establishes, legal regulation of DPSIP issues is justified by psychological and sociological research including the benefits such regulation has for individual, family, group, and governmental survival and growth.

2.2 The Majority of People want Data Protection and Security Legal Standards.

In a democracy, republic, or even a corporate republic, the attitudes of the people toward DPSIP legal issues ought to be considered. Studies in AU, CA, SA, the UK, and the US that illustrate attitudes in those countries are considered below.

2.2.1 Australia

The AU Office of the Federal Privacy Commission conducted research on public privacy concerns for a number of years. In 2001, the levels of privacy concerns were higher than a similar 1997 study. In the 2001 study,[27] ninety-one percent of the sample thought that businesses should ask permission prior to collecting personal data even if it was inconvenient. The sample reported that businesses that collected data should inform customers regarding the uses of the data (eighty-nine percent). Over ninety-two percent reported that privacy violations included businesses transferring personal data without permission and using the data for purposes other than that claimed at the time of collection. The highest support was that businesses ought to show *'respect for, and protection of, my personal information.'*[28]

---

[27] Australian Office of the Federal Privacy Commission, *Privacy and the Community* (Author 2001).

[28] *Id.* at 4.

The research showed that in AU, citizens and even business executives were concerned about DPSIP concerns and violations. Representative governments should establish laws that reflect citizen concerns rather than special interests.

2.2.2 Canada

The Federation Nationale des Associations de Consommateurs du Quebec/Public Interest Advocacy Centre[29] surveyed 2,000 Canadians in Ontario and Quebec. Over fifty percent of the subjects reported that they had privacy violations as a concern and high information privacy concerns. The research of Smith, Milberg, and Burke[30] showed that the major privacy concerns were improper access and unauthorized secondary use. Another study of 7,088 adults, by Ipsos/Queen's University[31] found that sixty-nine percent of Canadians were concerned about the protection of personal information.

In 2009, the Canadian Office of the Privacy Commissioner conducted a public research project. The data showed that eighty-seven percent of Canadians distrusted businesses in the protection of their private information, especially during hard economic times. Seventy-one percent of the sample favored stronger privacy protection laws. The vast majority (eighty-three percent) were concerned about genetic privacy.[32]

---

[29] Federation Nationale Des Associations De Consommateurs Du Quebec/Public Interest Advocacy Centre, *Surveying Boundaries: Canadians and their Personal Information* (Author 1995).

[30] H. Jeff Smith, et al., Information Privacy: Measuring Individuals' Concerns About Organizational Practices, 20 *Management Information Systems* 2, 167 (1996, June).

[31] Ipsos / Queen's University, *Interviews with 7,088 Adults in Brazil, Canada, France, Hungary, Mexico, Spain and the United States* (2006), http://www.angus-reid.com/polls/view/13849 (last visited on 3 March 2012).

[32] Office of the Privacy Commissioner of Canada, *Canadians Concerned Corporate Cost Cutting Could Affect their Privacy: Poll* (2009, April 27), http://www.priv.gc.ca/information/survey/2009/ekos_2009_01_e.cfm (last visited on 28 April 2012).

2.2.3 The Republic of South Africa

Research on public concerns regarding data protection and security concerns in SA covered a period of many decades after the EU data protection directive standards. A survey conducted in SA revealed that seventy-three percent of those sampled reported concerns about the loss of control over their personal information.[33]

Data protection and security concerns in SA showed that organizational leaders ranked amongst the world's most informed about issues related to data protection and security. Sixty-seven percent reported that such concerns were critical, yet twenty-four percent expressed concerns about the effectiveness of current DPSIP efforts in that country. The majority noted governmental policy motivated business interest.[34]

The research conducted in SA revealed that the majority of people wanted DPSIP legal protections. The data also showed that business organizations in the country were behaving below international standards.[35] The lack of governmental DPSIP laws and regulatory agencies compounded the problem.

2.2.4 United Kingdom / European Union

Almost seventy-five percent of Europeans reported that they were worried about their lack of control of personal information. While more than fifty percent trusted employers, financial institutions, local governments, medical services, police, social security, and tax authorities to follow data protection

---

33 Jaco Van Der Walt, *Trust and Privacy are the Cornerstones of Successful Relationships between Consumers and Business*. (2003, March 13), http://www.ey.com/GLOBAL/content.nsf/South_Africa/15_May_03_Trust_And_ Privacy (last visited on 5 June 2012).

34 Ernst & Young, *South African CEOs are Getting More Hands-On with Information Security Issues*, Tech News (2004, November), http://cbr.co.za/article.aspx?pklArticleId=3290&pklCategoryId=378 (last visited on 22 March 2012).

35 *Ibid.*

and security standards, less than half trusted credit card agencies, credit reference agencies, mail order companies, marketing companies, nonprofit organizations, opinion research companies, and travel businesses. The loss of personal data for 25 million persons by the UK Government was a strong area of concern.[36] The Angus Reid[37] data showed that fifty-nine percent were concerned about new technology being used to violate personal privacy standards.

A study by the European Commission found that eighty percent of the youths studied were concerned about governments and businesses using their personal data without permission and sharing it with third parties. The sample also thought governmental regulation was necessary and that few use current protection technology.[38]

2.2.5 United States of America

Kim Sheehan[39] did a meta-analysis of studies of forty-three established and respectable public opinion poll studies related to information privacy views in the US. The data showed a number of population concerns regarding information privacy. The Sheehan mega-data showed that the majority of those polled in the various studies maintained that the government should pass laws that protect information privacy and that individuals should have the power to protect their rights, including private causes of action. The data supported the view that information privacy was in trouble in the US. The

---

[36] Aoife White, *EU Poll Shows Three Out of Four Europeans Worried about Personal Data Online* (22 January 2008), http://news.theage.com.au/technology/eu-poll-shows-three-out-of-four-europeans-worried-about-personal-data-online-20080122-1nba.html (last visited on 22 April 2012).

[37] Angus Reid Global Monitor, *Five Countries Review Privacy, Technology* (2006), http://www.angus-reid.com/polls/view/11915 (last visited on 31 March 2012).

[38] Judith Crosbie, *Commission Seeks External Advice on Internet Privacy* (2009, April 28), http://www.europeanvoice.com/article/2009/04/commission-seeks-external-advice-on-internet-privacy/64717.aspx (last visited on 29 April 2012).

[39] Kim Bartel Sheehan, *How Public Opinion Polls Define and Circumscribe Online Privacy*, 9 *First Monday*, 7 (2004), http://www.firstmonday.org/issues/issue9_7/sheehan/ (last visited on 24 June 2012).

people studied maintained that there was or should be a right to privacy, and control over who gets information and over the collection of information. The subjects were concerned about information theft and about the lack of Internet privacy.

A Harris[40] poll found eighty-three percent of Americans reported that they would stop doing business with a company that did not protect personal information. Ninety percent wanted a transparent privacy policy. Sixty-two percent wanted an independent monitor on the practices, and ninety-one percent would do business with such a firm if the practices were audited.

Susannah Fox and Oliver Lewis[41] have conducted a number of relevant studies. They found that seventy percent of Americans supported new laws to protect information privacy. Fox found that eighty-six percent favored opt-in to data collection processes and expressed the opinion that companies should ask permission prior to using personal data. Fifty-four percent reported that web site tracking of activities was harmful and a privacy violation. Ninety-four percent argued for legal punishment for privacy violators. Eleven percent wanted violating company owners sent to prison. Twenty-seven percent wanted violating owners fined. Twenty-six percent wanted any violating web site shut down. Thirty percent wanted a published list of privacy violating fraudulent web sites.[42]

Independent research in all of the countries addressed in this study revealed that citizens and business executives were significantly concerned about

---

[40] Harris Interactive, *Privacy On and Off the Internet: What Consumers Want* (Study No. 15229) (Author 2002).

[41] Susannah Fox & Oliver Lewis, *Fear of Online Crime: Americans Support FBI Interception of Criminal Suspects' Email and New Laws to Protect Online Privacy*, Pew Internet & American Life Project (2001), http://www.pewinternet.org/~/media//Files/Reports/2001/PIP_Fear_of_crime.pdf.pdf (last visited on 24 May 2012).

[42] Susannah Fox, et al., *Trust and Privacy Online: Why Americans Want to Rewrite the Rules*, Pew Internet & American Life Project (2000), http://www.pewinternet.org/~/media/Files/Reports/2000/PIP_Trust_Privacy_Report.pdf.pdf (last visited on 7 June 2012).

DPSIP issues. Many of the concerns were counter to national legislation and court decisions.

2.3 Personal Information as a Valuable Commodity

That people in all the countries addressed in this study are concerned about DPSIP issues is one illustration that personal information is a valuable commodity, and the research confirms this fact. This section summarizes relevant research and findings on the issue.

Richard Mason[43] argued that the increased interests in DPSIP were related to new technology that allowed increased information storage and retrieval. A second factor was increased information value.

Of the nations studied, the US was one of the leaders in information technology. In 1951, the US Census Bureau purchased the first commercial electronic computer – UNIVAC – to collect and process massive data.[44] Starting in the 1950s and 1960s, marketing firms and government bureaucracies started programs that involved massive amounts of data collection, storage, and selling. Robert Smith explained that data collection was related to other cultural experiences including countries becoming credentialed societies based on personal data.[45]

Alan Westin showed that in 1966, the Federal government owned 2,600 computers – more than any other organization. As a little boy with a new hammer who finds all kinds of things to pound, the government started to collect more data. "Once an organization purchases a giant computer, it inevitably

---

[43] Richard O. Mason, Four Ethical Issues for the Information Age, 7 *MIS Quarterly* 2, 4 (1986).

[44] Charles T. Meadow, Online Database Industry Timeline, 11 *Database Magazine* 5, 23 (1988).

[45] Robert Ellis Smith, *Ben Franklin's Web Site: Privacy and Curiosity from Plymouth Rock to the Internet*, at 314 (Privacy Journal 2004).

begins to collect more information."[46] In 1981, with the massive introduction of personal computers, the demand to access personal information increased.

George Duncan, Thomas Jabine, and Virgina deWolf published a report of the Panel on Confidentiality and Data Access. The report found that computer and communication advances allowed data users to demand more individual or micro-data. The development of large databases was the result of lower storage costs, improved transmission, computerized data entry, and software developments. Confidentiality became more important, but businesses and governments ignored the threats to it.[47]

Pricilla Regan found that both businesses and governments had an insatiable hunger for more individual information. As information became an increasingly valuable commodity, DPSIP concerns were ignored or circumvented.[48]

David Burnham warned of the loss of personal information privacy and showed the danger of the power differential between individuals' ability to protect their privacy and the combined ability of businesses and governments to violate it.[49] Pricilla Regan[50] agreed with Westin and Baker that the catalyst for the change was the computer, but the computer was not the source of the problems. Businesses and governments joined forces to destroy information privacy and eliminate individual control over the collection, use, and transfer of personal information.[51]

Although businesses and government ignored the concerns expressed by individuals, people recognized that their personal information was valuable

---

46 Alan Westin, *Privacy and Freedom*, at 160 (Atheneum 1967).

47 George T. Duncan, et al., *Private Lives and Public Policies: Confidentiality and Accessibility of Government Statistics*, at 52 (National Academy Press 1993).

48 Pricilla M. Regan, *Legislating Privacy: Technology, Social Values, and Public Policy*, at 69 (University of North Carolina Press 1995).

49 David Burnham, *The Rise of the Computer State*, at 9 (Weidenfeld & Nicolson 1983).

50 Pricilla M. Regan, (1995).

51 Allen F. Westin & Michael A. Baker. *Databanks in a Free Society: Computers, Record-Keeping & Privacy*. National Academy of Sciences. Washington. D.C. Project on Computer Databanks, at 75 (Quadrangle Books 1972).

from the earliest use of computers to collect and store such data. In 1965, the US Federal government proposed a comprehensive governmental database. The public reaction was so negative that the proposal was limited and essentially went underground. A similar pattern was revealed when Lotus developed and tried to market a program called Marketplace that included massive personal information.[52] Private businesses obtained government technology. The businesses were encouraged to create massive databases and thus, the data aggregator industry was privately born. The government then accessed the data that it could not collect by itself.

Simson Garfinkel argued that the rejection of a governmental database was a mistake. Stronger controls, checks and balances, and a process for redress could have prevented business and governmental abuses, errors, and kept the practices debatable in public.[53] The flaw in his thinking was that private businesses and the government got access anyway. Even when controls, checks, and balances were established, businesses and governments still failed to protect the data

Governments compelled people to surrender personal information and then sold it to private companies. The companies added additional information. The government often purchased the new records, thus by-passing the citizen's rejection of a central database. The symbiotic government - private business relationship was more than political. Governments made fortunes selling their information on individuals to marketing and other business firms.[54]

---

[52] Laura J. Gurak, *Persuasion and Privacy in Cyberspace: The Online Protests over Lotus Marketplace and the Clipper Chip* (Yale University Press 1997). Also see Laura J. Gurak, *Logging in with Laura J. Gurak: Minnesota Professor Takes a Critical Look at Online-Privacy Issues*, The Chronicle of Higher Education (19 February 2002), http://chronicle.com/free/2002/02/2002021901t.htm (last visited on 4 May 2012).

[53] Simson Garfinkel, *Database Nation: The Death of Privacy in the 21st Century*, at 35 (O'Reilly 2000).

[54] Charles J. Sykes, *The End of Privacy: Personal Rights in the Surveillance Society*, at 29 (St. Martin's Press 1999).

Technological progress reached the point where knowledge discovery in databases (KDD) was a reality. Such private information was a commodity. The technology involved data mining and dataveillance. Several large data aggregator companies established data dossiers on billions of people. Acxiom, ChoicePoint, Experian, Equifax, LexisNexis, and Trans Union purchased data and data companies to expand data resources.[55] In the US, since September 11, 2001, the government had gained increased access to the data aggregator's records. The data had been collected by the government and repurchased for a fee, to protect against terrorists and maintain social control.

Knowledge based databases used s*ubject-oriented link analysis* to collect data behavior, intentions, lifestyles, and relationships. Correlation pattern analysis revealed new patterns. *Pattern matching* subject classes used algorithms in large databases to identify individuals and patterns.

James Dempsey and Laura Flint argued that pattern analysis was the most significant threat to civil liberties and privacy in decades. Daily lawful behaviors were examined using a massive surveillance monitoring strategy. The approach ignored the legal principles that prior to a search, individual suspicion must be established. Fundamental legal constructs including a presumption of innocence were ignored.[56]

Private information in digital dossiers became "commodities, bought and sold like bags of potato chips and six packs of beer."[57] Cees Hamelink[58] argued that advanced data-mining technology became a tradable commodity, especially in capitalistic countries.

---

55 Robert O'Harrow, *No Place to Hide* (Free Press 2006).

56 James X. Dempsey & Lara M. Flint, Commercial Data and National Security, 72 *George Washington Law Review* 6, 1459, 1476 (2004), at 1466–1467.

57 Andrew J. Mcclurg, *A* Thousand Words are Worth a Picture: A Privacy Tort Response to Consumer Data Profiling, 98 *Northwestern University Law Review* 1, 63 (2003), at 142.

58 Cees J. Hamelink, *The Ethics Of Cyberspace* (Sage 2000).

The real owners of the data, the data subjects, were compelled to release the data, fraudulently induced to share it, not compensated for its collection or use, and all without informed consent. The process created data shadows which were free of controls all over the world. The shadows did not even have to be correct or accurate. People and even institutions became vulnerable subjects that could be punished or retaliated against even for behavior that was never committed.[59]

Anita Allen[60] explained that information privacy referred to the right to control the use of personal data or information, and that privacy law should empower an individual's control over such information. The principle also applies to access to public records data.

Daniel Solove declared that the mutual collection and sale of private data between governments and businesses violated basic DPSIP legal principles and demonstrated that marketers and businesses collect sell, and use massive amounts of public data unlawfully.[61]

Another factor in the massive collection, sale, and use of data was the speed of data transfer. As memory became less expensive, larger databases could be maintained. Steven Miller demonstrated the impact of the increased speed of transfer when he described that transmitting the *Encyclopedia Britannica* took more than eighty-four hours, in the 1980's; by 1994 it took less than five seconds.[62] Personal data was at higher risk as database size, digitization, manipulation, replication ability, and speed of transfer increased. A couple of seemingly insignificant pieces of personal data could quickly lead to a massive dossier. Similarly, Andre Bacard showed the need for strong information

---

[59] Garfinkel, 2000, at 70.

[60] Anita L Allen, Privacy as Data Control: Conceptual, Practical, and Moral Limits of the Paradigm, 32 *Connecticut Law Review* 9, 861 (2000), at 863. See also Anita L. Allen, *Privacy in American Law*, in *Privacies: Philosophical Evaluations* (Beate Rossler ed., Stanford University Press2004).

[61] Daniel J. Solove, Access and Aggregation: Public Records, Privacy, and the Constitution, 86 *Minnesota Law Review* 6, 1137 (2002), at 1194-1195.

[62] Steven E. Miller, *Civilizing Cyberspace: Policy, Power, and the Information Superhighway*, at 36 (ACM Press 1995).

privacy legal intervention because of technology changes including (1) vast memory capacity; (2) permanent, de-contextualized data; (3) sophisticated search and matching capabilities; and (4) ease of transferability.[63]

In addition to the lack of control over the collection, sale, and use of their personal data, people had little to no ability to correct data errors because they had no access to information in the massive databases that were aggregated and because the law did not establish their right to such access for all databases and transfers. Richard Spinello proclaimed many data files were incomplete and even outdated. Larger data bases compound the problems exponentially. As data is shared, corrections become almost impossible.[64]

Richard Miller described the issue of data aggregation, mining, and profiling from a historical perspective. Data bits were scattered and transient. Any attempt to collect the data was arduous, complicated, labor intensive, and slow. When the data was electronically stored, data from a range of sources were combined and cross tabulated. No checks and balances were in place to ensure accuracy.[65]

Such practices had the effect of making people objects and assaulted human autonomy and dignity. Error correction and data context were an essential part of the management of databases that contained information privacy data, and DPSIP law must address these issues. The opportunity that the advent of computers presented to make personal data a commodity was similar to the tort law principle of an attractive nuisance.[66]

---

63 Andre Bacard, *The Computer Privacy Handbook*, at 36 (Peachpit Press 1995).

64 Richard A. Spinello, *Ethical Aspects of Information Technology*, at 119 (Prentice Hall 1995).

65 Miller, 1995, at 264.

66 Creating an attractive situation that could lure a person into a situation that could be harmful.

2.4 Governments and Businesses failed to Adequately Address DPSIP Issues

Clearly people wanted their personal information protected and objected to its commoditization and use without their knowledge or consent, and while they may have had no expectation that businesses would serve their interests, citizens might have expected more from their governments. The information economy placed value on data, information, and knowledge. New information markets opened and business laid claim to them. Businesses pushed technologies for targeting consumers and manipulating markets - usually without informed consent - in the name of improved marketing and saving free markets.

Governments colluded in the information theft that ensued. Some policy makers, special interest groups, and judges argued that the outdated principle of *caveat emptor* or public waiving of DPSIP rights applied. Consumer protection standards were ignored, and conflicting laws and court decisions created additional DPSIP issues.

2.4.1 Business Issues

Because of this failure to adequately address DPSIP issues, modern corporations, with the assistance of some questionable court decisions, had considerable power to divert the will of the people. The majority of the 100 world's largest economies were corporations (fifty-one percent corporations, forty-nine percent countries). The top 200 corporations had more economic and political power than all but nine countries, controlling twenty-five percent of international economic activities. Thirty-three percent of all world trade involved corporate transfers within the same company.[67] Large corporations influenced not only economic decisions but also legal ones.

---

[67] Sarah Anderson & John Cavanagh, *Top 200: The Rise of Global Corporate Power*, (Global Policy Forum 2000),

The warnings about business and corporate power and the beacon call to regulate and limit business and corporate power on the law was not new. The pattern in the US is a prime example. Thomas Jefferson, President of the US from 1801 to 1809 made the first declaration. "I hope we shall crush in its birth the aristocracy of our monied corporations which dare already to challenge our government to a trial by strength, and bid defiance to the laws of our country."[68]

On November 21, 1864, Abraham Lincoln, President of the US from 1861 to 1865, prophetically shared his concerns on corporations, the law, and government. He wrote:

> I see in the near future a crisis approaching that unnerves me and causes me to tremble for the safety of my country... Corporations have been enthroned and an era of corruption in high places will follow, and the money power of the country will endeavor to prolong its reign by working upon the prejudices of the people until all wealth is aggregated in a few hands and the Republic is destroyed.[69]

In 1888, Rutherford Birchard Hayes, President of the US from 1877 to 1881, made a similar corporate pronouncement. He declared:

> All laws on corporations, on taxation, on trusts, wills, descent, and the like, need examination and extensive change. This is a government of the people, by the people, and for the people no longer. It is a government of corporations, by corporations, and for corporations.[70]

---

http://www.globalpolicy.org/component/content/article/221/47211.html (last visited on 15 June 2012).

[68] Thomas Jefferson, *Letter to George Logan*, in *The Writings of Thomas Jefferson* at 69 (Paul Leicester Ford ed. G. P. Putnam's Sons 1816).

[69] Abraham Lincoln, *Letter to Colonel William F. Elkins, November 21, 1864*, in *The Lincoln Encyclopaedia* (1950) (Archer H. Shall ed., Macmillan 1864), at 1.

[70] Rutherford Birchard Hayes, *Diary and Letters of Rutherford Birchard Hayes*, in *U.S. President. Diary and Letters of Rutherford Birchard Hayes: Nineteenth President of the United States,* at 374 (Charles Richard Williams ed., The Ohio State Archaeological and Historical Society 1888).

In the same year, Grover Cleveland, President of the US from 1885 to 1889 and 1892 to 1896 mirrored the concern, but little was done. He declared, "Corporations, which should be the carefully restrained creatures of the law and the servants of the people, are fast becoming the people's masters."[71]

In 1906, Theodore Roosevelt, President of the US from 1901 to 1910 proclaimed:

> Behind the ostensible government, sits enthroned an invisible Government, owing no allegiance and acknowledging no responsibility to the people. To destroy this invisible Government, to dissolve the unholy alliance between corrupt business and corrupt politics, is the first task of the statesmanship of the day.... This country belongs to the people. Its resources, its business, its laws, its institutions, should be utilized, maintained, or altered in whatever manner will best promote the general interest.[72]

Franklin D. Roosevelt, President of the US from 1933 until his death in 1945, addressed a similar legal concern:

> The first truth is that the liberty of a democracy is not safe if the people tolerate the growth of private power to a point where it becomes stronger than their democratic state itself. That, in its essence, is fascism - ownership of government by an individual, by a group, or by any other controlling private power.[73]

The power of business interests over data protection, information privacy law, and corporate social responsibility was not new. The historic four dimensions of legal public policy – the executive branch of government, congress, courts,

---

[71] Grover Cleveland, *Fourth Annual Message to Congress, 3 Dec. 1888*, in *Messages and Papers of the Presidents*, at 773-774 (James D. Richardson ed., Government Printing Office 1888).

[72] Theodore Roosevelt, *Declaration of Principles of the Progressive Party* (1906), http://www.pbs.org/wgbh/amex/presidents/26_t_roosevelt/psources/ps_trprogress.html (last visited on 4 July 2012), at 5.

[73] Franklin D. Roosevelt, *Message to Congress on the Concentration of Economic Power* (1938, April 29), http://informationclearinghouse.info/article12058.htm (last visited on 27 July 2012), at ¶ 2.

and the press – ignored powerful corporate and wealth holdings. Corporate interests in the US controlled the press and corporate power and belief systems influenced, if not controlled all four dimensions. The corporate mindset was not new.

Cornelius (Commodore) Vanderbilt, the patriarch of the Vanderbilt family, responded to the business versus law struggle. He declared the universal corporate mindset, "What do I care about the law? Haven't I got the power?"[74]

In 1882, the railroad magnate and *robber baron*[75] William Henry Vanderbilt declared "The public be damned! I work for my stockholders."[76] The stockholders were not independent, all knowing agents. Stockholders responded to what management communicated.

The mindset continued through the 1901 US market crash caused by the battle between J. Pierpont Morgan and J.P. Harriman which destroyed thousands of investors. J. P. Morgan was asked by a reporter "Don't you think, that since you are being blamed for a panic that has ruined thousands of people and disturbed a whole nation, some statement is due the public?" Morgan replied, "I owe the public nothing"[77] Morgan continued the view that "Men owning property should do what they like with it."[78]

The graft, corruption, and control of the robber baron era did not just influence the executive and legislative branches of the US government. The influence also included the judiciary. The Supreme Court railroad commission opinion was actually a consolidation of three railroad, county, and state taxation cases

---

74 Matthew Josephson, *The Robber Barons: The Great American Capitalists, 1861-1901*, at 15 (Harcourt, Brace & World 1962).

75 A reference to exploitive, powerful, and unethical business leaders.

76 Rufus Hatch, *Hatch on Vanderbilt*, Chicago Daily Tribune. (1882, October 17), at 12.

77 New York Herald – World, *Giants of Wall Street, in Fierce Battle Over Mastery, Precipitate Crash that Brings Ruins to Hordes of Pygmies* New York Herald – World (1901, May 11), at 22.

78 Lewis Corey, *The House of Morgan: A Social Biography of the Maters of Money*, at 289 (G. Howard Watt 1930).

on property given to the railroads. The three cases were the *California v. Central Pacific Railroad Company*, *California v. Southern Pacific Railroad Company,* and *Santa Clara County v. Southern Pacific Railroad Company* cases.[79]

In 1886, twenty-one years after Lincoln's assassination, Justice John Marshal Harlan (appointed by Rutherford B. Hayes) and his clerk legally established what Lincoln so feared. The case of *Santa Clara County v. Southern Pacific Railroad* [80] gave powerful corporations the legal status of personhood. The Court not only sided with the robber barons but granted corporations the legal status of a legal person. Corporations were no longer state created but persons under the Fourteenth Amendment.

Prior to hearing oral arguments, Chief Justice Morrison R. Waite made a unique declaration. The statement was included above the opinion and thus technically had no legal importance except that Courts and authors accepted it as persuasive. He stated:

> The court did not wish to hear argument on the question whether the provision in the *Fourteenth Amendment* to the Constitution, which forbad a State to deny to any person within its jurisdiction the equal protection of the laws, applies to these corporations. We are all of the opinion that it does.[81]

The statement was entered into the summary record by a court reporter. The reporter added a syllabus statement that

> The defendant Corporations are persons within the intent of the clause in section 1 of the Fourteenth Amendment to the Constitution of the

---

79 *Railroad Commission Cases*, 116 U. S. 307, 331 (1886). (US)
80 118 US 394-417, (1886). (US)
81 *Id.* at 394.

> US, which forbids a State to deny to any person within its jurisdiction the equal protection of the laws.[82]

The result was to grant unprecedented legal power to corporations. No challenges succeeded. The court never addressed the issue. The error spread internationally. The SA constitution even accepted the same flawed political reasoning.

In the *Wheeling Steel Corporation v. Glander*[83] case, a state tax case, Justices Douglas and Black dissented. The case was a combination of the *Wheeling Steel Corporation v Glander, Tax Commissioner of Ohio and National Distillers Products Corporation, N.Y. v Glander, Tax Commissioner of Ohio*[84] Justices Douglas and Black's opinion cited the statement in Justice Waite's 1886 opinion and replied "There was no history, logic, or reason given to support that view. Nor was the result so obvious that exposition was unnecessary."[85] Note that the opinion was in dissent of the majority of the Court.

The dangerous legal fiction continued. In *Buckley v Valeo,*[86] the US Supreme Court extended corporate constitutional rights to include First Amendment free speech rights. By making political contribution limits unconstitutional, the Court determined that the corporations could use corporate money to influence elections as a matter of free speech. The right did not require stockholder permission.

The mentality of corporate robber barons and neo-conservatives continued. The Courts continued to perpetuate the legal fiction of deference to corporate

---

82 *Id.* at 1.

83 337 US 562, (1949). (US)

84 *Id.* at No. 447 - 478.

85 *Id.* at Dissent, at 2.

86 (No. 75-436) No. 75-36, 171 U.S.App.D.C. 172, 519 F.2d 821, affirmed in part and reversed in part; No. 75-437, 401 F.Supp. 1235, affirmed, (1976). (US)

power. Robert Reich, the Secretary of Labor during the Clinton[87] administration showed the continued impact of the judicial verdict in *Santa Clara County v. Southern Pacific Railroad* over 120 years later. In 2008, Reich declared:

> There's no longer any countervailing power in Washington. Business is in complete control of the machinery of government. The House, the Senate and the White House are all run by business-friendly Republicans who are deeply indebted to American business for their electoral victories.[88]

Business organizations that made money on the collection, use, and sale of private information represented a large and powerful legislative lobby. Business concerns argued that privacy was a special issue and that the concerns were exaggerated and costly to business. Without opt-in informed consent, people gave information away to business concerns. Privacy issues, framed as trivial, resulted in considerable money being spent protecting business rights to use private information without payment or informed consent. After all, business was only magnanimously helping people. Consumers were not aware of the unique ways that their lives were scanned and data collected.[89]

Businesses collected more and more private information to make more money. Many also joined to meet competitive pressures and to sell more ill gotten data. Tracing transfers became impossible.[90] Jeff Smith[91] found that

---

87 Behaviourally, Clinton was the youngest neo-conservative – Republican / Democrat president in US history.

88 Robert Reich, *Corporate Power in Overdrive*, New York Times. (2001, March 18), http://query.nytimes.com/gst/fullpage.html?res=9D04E2DA153DF93BA25750C0A9679C8B63&sec=&spon=&pagewanted=1 (last visited on 20 August 2012), at 2. The current situation is no different with a Democratic President. See Lawrence Lessig, *Republic, Lost: How Money Corrupts Congress - and a Plan to Stop It*, (Twelve - Hachette Hook Group ed. 2011).

89 Winnie Chung & John Paynter, *Privacy Issues on the Internet* (2002), http://csdl2.computer.org/comp/proceedings/hicss/2002/1435/07/14350193b.pdf (last visited on 10 June 2012), at 2.

90 Gurpreet S Dhillon & Trevor T. Moores, Internet Privacy: Interpreting Key Issues, 14 *Information Research Management Journal* 4, 33 (2001).

corporations in a range of industries did not have any standard ways of dealing with personal information. Self-regulation resulted in no regulation.

Some business organizations used collected data to sell goods. Other businesses used data mining to influence *democratic* elections. The corporation named Aristotle bought voter information from counties and states. Candidates and special interest groups then bought the expanded data. The company openly sold a powerful database that included:

> information about a voter's address and the number of children he or she has, but also a lot of other information that may include how much your house is worth, what kind of car you drive, what Web sites you visit, and whether you went to college, attend church, own guns, have had a sex change, or have been convicted of a felony or sex crime.[92]

A more traditional business approach was RealJukeBox's sale of personal data without permission. The information included customer's name, e-mail address, musical preferences, amount of music on hard disks and other data.[93]

The Direct Marketing Association,[94] an industry lobby group, advocated for an opt-out option for data collection to make it less expensive for members.

---

91 Jeff Smith, *Managing Privacy: Information Technology and Corporate America* (The University of North Carolina Press 1994).

92 Kim Zette, *Voter Privacy Is Gone -- Get Over It* (2008, January 31), http://blog.wired.com/27bstroke6/2008/01/voter-privacy-i.html (last visited on 3 February 2012), at 6.

93 Eric C. Turner & Subhasish Dasgupta, Privacy on the Web: an Examination of User Concerns, Technology, and Implications for Business Organizations and Individuals, 20 *Information System Management* 8 (2003).

94 Direct Marketing Association, *Direct Marketing Association's Online Marketing Guidelines and Do the Right Thing Commentary* (2006), http://www.the-dma.org/guidelines/onlineguidelines.shtml (last visited on 12 August 2012).

However, the majority of non-industry funded research showed that the majority of people preferred an opt-in approach to data collection.[95]

Marketers suggested that some businesses offered privacy protections. Those that wanted information privacy protections could pay more for non-disclosure (blackmail?).[96] People who wanted information privacy protections could pay collectors for not collecting the data.[97] The major problem with the libertarian–market approach was that it was impossible to know all of the sources that had collected personal data, so contracting was a practical impossibility. John Hagel[98] and Kenneth Laudon[99] suggested that consumers should be paid for use of their information.

Corporations often claimed that DPSIP standards should be balanced with the argument of computer cost saving and business profits. Research in the field showed that the cost cutting claims were unfounded.[100] Don Tapscott and David Ticoll maintained that, "Corporations have the right to have secrets - called information security. As individuals we have a right to something different - privacy."[101] "Consent, limiting collection, identifying purpose,

---

95 George R. Milne & Andrew J. Rohm, Consumer Privacy and Name Removal Across Direct Marketing Channels: Exploring Opt-in and Opt-out Alternatives, 19 *Journal of Public Policy and Marketing* 2, 238 (2000); A. D. Miyazaki & A Fernandez, Internet Privacy and Security: An Examination of Online Retailer Disclosures, 19 *Journal of Public Policy and Marketing* 1, 54 (2000).

96 David D. Friedman, *Future Imperfect: Technology and Freedom in an Uncertain World* (Cambridge University Press 2008); Mary J. Culnan & Sandra J. Milberg, *Consumer Privacy*, in *Information Privacy: Looking Forward, Looking Back* (M. Culnan, et al. eds., Cambridge University Press1999); Mary J. Culnan, Protecting Privacy Online : Is Self-Regulation Working, 19 *Journal of Public Policy Marketing* 1, 20 (2000).

97 Jerry Berman & Deirdre Mulligan, The Internet and the Law: Privacy in the Digital Age: Work in Progress, 23 *Nova Law Review* 2, 549 (1999); George J. Stingler, An Introduction to Privacy in Economics and Politics, 9 *Journal of Legal Studies* 4, 623 (1980).

98 John Hagel, The Coming Battle for Customer Information, 75 *Harvard Business Review* 4, 53 (1997).

99 Kenneth C. Laudon, Markets and Privacy, 39 *Communications of the Association for Computing Machinery,* 9, 92 (1996, September).

100 Ann Cavoukian & Don Tapscott, *Who Knows: Safeguarding your Privacy in a Networked World* (Random House of Canada 1995); John Shattuck, Computer Matching is a Serious Threat to Individual Rights, 27 *Communications of the ACM* 6, 538 (1984).

101 Don Tapscott & David Ticoll, *The Naked Corporation: How the Age of Transparency Will Revolutionize Business*, at 312 (Free Press 2003).

limiting use, disclosure, and retention" standards were ignored by corporations and the government.[102]

Justified concerns about governments abusing personal information and even ignoring privacy laws existed. Timothy Schoechle[103] showed that in capitalistic countries, large corporations and information processing firms posed a more significant concern. Profit, self-interest, and wealth accumulation were the only corporate values sought in the absence of strong legal regulation.

In the first seven months of 2008, more data breaches were reported than in the entire prior year. The reason so many data protection and information privacy breaches was that businesses did not care. There was no "real incentive to invest more than the minimum required in security."[104] The Chief Security Technology Officer at the BT Group, Bruce Schneier commented on the state of affairs in a *Wall Street Journal* article, he proclaimed that "For the most part a company doesn't lose its data, they lose your data."[105] The real victims had no power to punish the businesses involved.

Self-regulation had failed. While everyone could contribute, "individual businesses don't have a reason to do anything about it."[106] Bruce Schneier argued that the best way to improve security is a governmental incentive. The incentive should be strong civil fines, criminal actions, or a private cause of action.[107] There was a forth alternative however – this was to do all three.

---

102 *Id.* at 181.

103 Timothy D Schoechle, Privacy on the Information Superhighway: Will My House Still Be My Castle? 19 *Telecommunications Policy* 6, 435 (1995).

104 Ben Worthen, *Why All The Data Breaches? Businesses Just Don't Care* (2008, September 9), http://blogs.wsj.com/biztech/2008/09/09/why-all-the-data-breaches-businesses-just-dont-care/ (last visited on 9 September 2012), at 3.

105 Bruce Schneier, *What Our Top Spy Doesn't Get: Security and Privacy Aren't Opposites* (2008, January 24), http://www.wired.com/politics/security/commentary/securitymatters/2008/01/securitymatters_0124?currentPage=all (last visited on 24 January 2012), at 4.

106 *Id.* at 6.

107 *Id.* at 8.

Over the past four decades, a major cultural revolution had taken place in economics, politics, business, and the law. Corporate republics replaced representative democratic republics. "Corporate republic" was a term coined by James Galbraith.[108] Milton Friedman led the free market cult in academic circles. Alan Greenspan, former Chairman of the Board of Governors of the US Federal Reserve System took the lead in monetary policy. In every case where the model was applied, it failed. In Congressional testimony on the 2008 market crash, Greenspan admitted that there was "a flaw in a lifetime of economic thinking and that he was in a 'state of shocked disbelief."[109] Greenspan had two gurus he followed – one was Friedman, the corporate controlled free market advocate and the other was the Social Darwinist, Ayn Rand.[110]

The political coup establishing corporate republics began with the elections of Margaret Thatcher in the UK and Ronald Reagan in the US. An unproven and questionable theory became a political plan. Regulatory checks and balances stopped, services were privatized, and corporate representatives controlled governmental regulatory boards. The fiction spread to AU and CA. In the US, the program progressed through both Presidents Bush and Clinton.[111] At the time of this writing, the US was a *Corporate Republic*.[112]

---

108 James K. Galbraith, *The Predator State: How Conservatives Abandoned the Free Market and Why Liberals Should Too* (Free Press 2008).

109 Alan Greenspan, *Greenspan Admits 'Mistake' that Helped Crisis* (2008, October 23), http://www.msnbc.msn.com/id/27335454/ (last visited on 24 October 2012), at 1.

110 See Gary Weiss, *Ann Rand Nation: The Hidden Struggle for America's Soul* (St. Martin's Press ed. 2012). Rand did not believe in the rule of law, opposed any governmental regulations of business, and advocated for untrammelled capitalism. She advocated that government should only have three functions: 1. The armed services for internal and external defence, 2. the police to control any dissent, and 3. the courts to serve a partisan agenda. There should be no income taxes and no human rights protections. at 262.

111 See David Osborne & Ted Gaebler, *Reinventing Government* (Plume 1992).

112 A term describing when big business determines and profits from a governmental coalition that diminished the will and accountability of the people. Businesses take control of historical governmental functions. See Interview by Bill Moyers with James K. Galbraith (8 October 2008), http://www.pbs.org/moyers/journal/10242008/transcript2.html (last visited on 8 October 2012); James K. Galbraith, *The Predator State: How Conservatives Abandoned the Free Market and Why Liberals Should Too* (Free Press 2008).

The pattern has continued with the election of Barack Hussein Obama II, as the US President.

The business establishment either structured or took advantage of the coup as business interests took precedence over a range of human rights, consumer protections, civil liberties, environmental safeguards, data security, data protection, and information privacy legal concerns. Business and business interests groups controlled regulatory boards and public discourse. The new standard was that if some business could make money, then traditional legal standards should be abandoned.[113] The cult mantra was that if a business model was not artificially maintained or was restricted, then the world would cave in - like *Chicken Little*.[114] The argument was that if those few who control the wealth of the world did not maximize their profits, the entire world would end. In 2008, the projections failed.

The law, which was theoretically above such shifts, succumbed to the coupe. The principle abandonment was both legislative and judicial. The reality was that laws were passed by politicians as indentured servants to business interests and their own self-illusions. Business and business interests groups, rather than legislators, wrote much of the legislation. From the beginning of the coup, judges were appointed to advance the coup's political and legal agendas.[115]

A legal fiction argued that basic legal and constitutional rights were balanced against greed, profit, and business concerns. A second legal fiction argued

---

[113] See Timothy P Carney, *The Big Ripoff: How Big Business and Big Government Steal Your Money* (John Wiley & Sons, Inc. 2006); John W. Dean, *The Rehnquist Choice: The Untold Story of the Nixon Appointment that Redefined the Supreme Court* (The Free Press 2001); John W. Dean, *Broken Government: How Republican Rule Destroyed the Legislative, Executive, and Judical Branches* (Viking 2007); Mark Green, *Losing Our Democracy: How Bush, the Far Right and Big Business are Betraying Americans for Power and Profit* (Sourcebooks, Inc. 2006).

[114] A reference to the children's story based on an African folktale about an animal that made a faulty judgment and hysterically proclaimed that the sky was falling resulting in mass hysteria.

[115] See Steven M. Teles, *The Rise of the Conservative Legal Movement: The Battle for Control of the Law* (Princeton University Press 2008).

that possible business and security interests are balanced against data protection and information privacy law concerns. A third legal fiction argued that business interests should not be held to a standard of data protection or general legal principles. The legislative and judicial history shows that in almost all reported cases, the balance is in favor of business or the government.[116]

A classic and relevant example is the issue of protecting children on the Internet. Of course, the issue ignored parental monitoring of such activities. The business response was that the free market could develop adequate protections. Although the research showed that most abused children were abused by family members, close relatives, and friends, the response of law enforcement and business was to establish a business focus on monitoring and privately controlling children's data - at a cost of course. A new market opportunity was created and several firms jumped into the mix.

One such firm was eGuardian of Ontario, California. The company met and even sold its services in the name of protecting children on the Internet. The company collected fees from parents, in the hope of secure protections. Parents entered key personal data on the child which was then compared to data provided to and by the schools. In prior contexts, this would be considered an illegal protection scheme. The company signed up 750,000 children. The company then sold the data to data miners and advertizing firms without consent or constraints.[117] What is the law to balance? The issue

---

116 Joel Bakan, *The Corporation: The Pathological Pursuit of Profit and Power* (Free Press 2004); Mark Green, *Losing Our Democracy: How Bush, the Far Right and Big Business are Betraying Americans for Power and Profit* (Sourcebooks, Inc. 2006); Thom Hartmann, *Unequal Protection: The Rise of Corporate Dominance and the Theft of Human Rights* (Rodale. 2002); Arianna Huffington, *Pigs at the Trough: How Corporate Greed and Political Corruption are Undermining America* (Crown Publishing Group 2004); Wade Rowland, *Greed, Inc: Why Corporations Rule Our World* (Arcade Publishing 2006); David Sciulli, *Corporate Power in Civil Society: An Application of Societal Constitutionalism* (New York University Press 2001); Benjamin Wittes, *Law and the Long War: The Future of Justice in the Age of Terror* (The Penguin Press 2008).

117 Brad Stone, *Online Age Verification for Children Brings Privacy Worries* (2008, November 15),

was whether to enforce historical and individual rights or allow business interests to negate fundamental legal principles. Business interests prevailed.

In the US, special interest groups pushed for the passage of the Video Privacy Protection Act of 1996 that allowed release of mailing lists and subject selections unless the customers chose to opt-out (at considerable hassle). Magazine publishers could sell subscription list data.[118] The Cato Institute (a powerful rightwing conservative think tank) argued that companies should have a near-absolute right to sell customer collected information.[119]

A Federal Trade Commission[120] study found that ninety percent of child oriented sites illegally collected information, and only four percent required parental permission. In 1998, the situation was not much better, eighty-nine percent of the sites collected information, only half disclosed their practices, and fewer than ten percent provided parental control.

Banks in the US moved into traditional police activities by fingerprinting non-customers who wished to cash checks. Banks and other businesses used cards that contained name, address, identification numbers, photographs, and fingerprints stored on magnetic strips or microchips.

Business data was also abused. On the day GeoCities[121] claimed voluntary TRUSTe privacy self-regulation, the FTC settled a case with GeoCities for selling collected information, contrary to their stated policy.

---

http://www.nytimes.com/2008/11/16/business/16ping.html?_r=1&partner=rss&emc=rss (last visited on 17 November 2012).

118 *Shirley v. Time, Inc.,* 45 Ohio App. 2d 69, 341 NE2d 337 (Ohio App. 1975). (US)

119 B. Hiawatha, *Europe's View of Online Privacy*, The Boston Globe. (1998), at http://www.law.wayne.edu/litman/classes/cyber/1998/nov5.html (last visited on 22 July 2012).

120 Federal Trade Commission, *Kids* (1997), www.ftc.gov/opa/1997/9712/kids.htm (last visited on 20 February 2012).

121 Geocities, *Truste* (1998), www.ftc.gov/opa/1998/9808/geocitie.htm (last visited on 22 May 2012).

A study by the University of Washington found 1.9 billion documented data breaches of personal information between 1980 and 2006. The 2007 rate was over 200,000 per month. Businesses accounted for sixty-one percent of the breaches. Thirty-one percent were from external sources. An IT Policy Compliance Group study found that seventy-five percent of the breaches were by businesses. Twenty-five percent were from external sources. A Computer World study found that only eleven percent of breaches were from external sources.[122]

In California, a supermarket company used loyalty card data to threaten a plaintiff with data on how much alcohol he had purchased from the store. In another jurisdiction, law enforcement officials – with a subpoena – accessed "club card" purchase information to discover if a person had purchased large numbers of plastic garbage bags. The Selective Service used ice cream marketing data to track eighteen year olds who were required to register for a possible draft. Governmental agencies had secretly purchased marketing data for investigations.[123]

In a sample of Fortune 500 companies, twenty-five percent released confidential information to government agencies without a subpoena. Seventy percent did the same to credit agencies.[124] In 2006, US telephone companies turned over private information to the government without any warrant. The action was part of the major debate on the passage of a Machiavellian wiretapping bill.[125]

---

122 Jaikumar Vijayan, *Forget Hackers; Companies Responsible for Most Data Breaches, Study Says* (2007, March 10), http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9013142&intsrc=news_list (last visited on 2 January 2012).

123 David Banisar, *Big Brother Goes Hi-Tech*, Covert Action Quarterly (2003), http://mediafilter.org/caq/CAQ56brother.html (last visited on 11 June 2012).

124 Rodger Doyle, Privacy in the Workplace, *Scientific American* (1999), http://www.scientificamerican.com/article.cfm?id=privacy-in-the-workplace (last visited on 1 June 2012).

125 Richard Martin, *Carriers Try to Avoid the Warrantless Eavesdropping Spotlight: The Telecoms, Including AT&T, Verizon, and Qwest, Face What AT&T Officials Have Called "A Maelstrom" of Civil Lawsuits Over the Eavesdropping Program* (2007, November 19),

In 2006, the Federal Trade Commission (FTC) found that Choice Point had released personal information related to 163,000 customers.[126] In a similar situation, Tower Records allowed the personal data of 5,225 customers to be released.[127] Two years after the FTC Choice Point original settlement agreement, the data revealed that over 100 million persons' privacy had been violated. The sources of the data included Boeing, Atena, and several universities.[128]

On 6 September 2006, Starbucks discovered that four "retired" laptop computers were missing and waited until November 4 to report the loss. The computers had the personal data of 60,000 employees in the US and 80 Canadian partners. A company representative made light of the breach, since the computers contained no secret coffee recipes.[129]

Poor data protection efforts by the T.J. Maxx and Marshalls retail stores allowed the release of 45.7 million personal data files. An additional 455 million records for customers who returned merchandise were open.[130] By May 16, 2007, the parent company reported to Security regulators that it had spent $25 million related to dealing with the breach and expected to pay even

---

http://www.informationweek.com/security/showArticle.jhtml?articleID=203103309 (last visited on 31 December 2012).

126 Federal Trade Commission, *ChoicePoint Inc.* (2006 December 6), http://www.ftc.gov/os/caselist/choicepoint/0523069complaint.pdf (last visited on 1 August 2012). (US)

127 Federal Trade Commission, *MTS, Inc., d/b/a Tower Records/Books/Video, a corporation, and Tower Direct, LLC, d/b/a TowerRecords.com, a corporation. (DOCKET NO. C-4110)* (2004, June 2), http://www.ftc.gov/os/caselist/0323209/040602comp0323209.pdf (last visited on 21 July 2012) (U.S.).

128 Tom Zeller, *An Ominous Milestone: 100 Million Data Leaks* (2006, December 18), http://www.nytimes.com/2006/12/18/technology/18link.html?_r=1&oref=slogin (last visited on 26 December 2012).

129 Martin H. Bosworth, *Starbucks Data Loss No Laughing Matter: Company Loses Laptops Containing 60,000 Employees' Information* (2006, November 6), at http://www.consumeraffairs.com/news04/2006/11/starbucks_data.html (last visited on 1 January 2012).

130 Jenn Abelson, *Breach of Data at TJX is Called the Biggest Ever* (2007, March 29), http://www.boston.com/business/articles/2007/03/29/breach_of_data_at_tjx_is_called_the_biggest_ever/ (last visited on 5 December 2012).

more when litigation began.[131] A report, three months later, showed the costs had mounted to 256 million generally in technology correction efforts. The corporation's stock had gone down but the next quarter sales figures were up nine percent.[132] Yahoo turned personal information over to the Chinese government. The sharing of e-mail information resulted in a 10 year sentence for Chinese journalist Shi Tao, who summarized his government's directive to media outlets to downplay the 15th anniversary of the Tiananmen Square crackdown in an email using his Yahoo! account.[133]

Certegy Check Services a subsidiary of Fidelity National Information Services Inc. sold personal information on 8.5 million people to marketing companies. Senior management claimed that the sale was not authorized.[134]

The State of California in the US, had a privacy constitutional amendment and the most advanced privacy laws in the country. In 2005 and later in 2006, Hewlett Packard [HP] instituted a privacy violating spying program on employees and its board of directors. When the State Attorney General investigated, HP agreed to pay a $14.5 million (USD) fine to settle the case.[135] Privacy laws showed that they could and did work.

Marketing companies wanted full access to all information. A 2007 study of 300 marketing professionals conducted by the Ponemon Institute found that

---

131 Ross Kerber, *TJX Puts Cost for Breach at $25m So Far* (2007, May 16), http://www.boston.com/business/personalfinance/articles/2007/05/16/tjx_puts_cost_for_breach_at_25m_so_far/ (last visited on 2 January 2012).

132 Ross Kerber, *Cost of Data Breach at TJX Soars to $256m: Suits, Computer Fix Add to Expenses* (2007, August 15), http://www.boston.com/business/globe/articles/2007/08/15/cost_of_data_breach_at_tjx_soars_to_256m/ (last visited on 15 August 2012).

133 Joe Lewis, *Digital Privacy a Shattered Utopia* (2006, October 30), http://www.webpronews.com/topnews/2006/10/30/digital-privacy-a-shattered-utopia (last visited on 1 January 2012).

134 Tampa Bay Business Journal, *Californian Sues Certegy Over Data Theft* (2007, August 16), http://tampabay.bizjournals.com/tampabay/stories/2007/08/13/daily45.html (last visited on 2 January 2012).

135 Scott Ferguson, *HP Settles Civil Complaint for $14.5M*, PCMAG.Com. (2006, December 8), http://www.pcmag.com/article2/0,2704,2070117,00.asp (last visited on 26 December 2012).

seventy percent thought that privacy standards added unnecessary marketing costs. Fifty-one percent thought that privacy standards made marketing more difficult. Twenty-six percent found no issues. Ninety-four percent reported that privacy standards reduced possible easy leads. A mere forty-four percent had worked with their privacy office in mounting a campaign.[136]

Some businesses established privacy statements, but few followed them. Many focused on protecting the company rather than the consumer.[137] Few users trusted such statements.[138]

Current privacy legislation in all of the countries in the study had approaches that were inadequate, and privacy legislation was misused. Diminished legal standards were established. For example, in the US the standards for illegal data collection rejected strict liability principles over a negligence or reasonable care standard.[139] The data showed a need to have DPSIP laws apply to business. While businesses objected, the data showed that such regulation was in the long-term interests of business survival. John Schwartz made the issue very clear. The key abuse issue was that businesses were the problem rather than the claimed fears of governmental regulation.[140]

Corporations influenced the enactment and implementation of DPSIP laws and regulations. Corporate power was a global phenomenon. The focus of

---

136 Charles Giordano, *Use Privacy to Build Customer Trust, Loyalty*, DM News, 4-5. (2007, March 22), http://www.dmnews.com/Use-privacy-to-build-customer-trust-loyalty/article/94933/ (last visited on 2 January 2012).

137 Zizi Papacharissi & Jan Fernback, Online Privacy and Consumer Protection: An Analysis of Portal Privacy Statements, 49 *Journal of Broadcasting & Electronic Media* 3, 259 (2005, October); Anne Kandra, *The Myth of Secure E-Shopping*, 19 PC World 7, 29 (2001).

138 J. Reagle & L.F. Cranor, The Platform for Privacy Preferences, 42 *Communications of the ACM* 2, 48 (1999).

139 *Cahlin v. General Motors Acceptance Corporation*, 936 F2d 1151 (11th Cir. 1991). (US)

140 John Schwartz, *DoubleClick Takes It On The Chin; New Privacy Lawsuit Looms; Stock Price Drops*, The Washington Post E1 (2000, February 18), at A1.

those with power was on increasing their power, not sound legal and public policy.[141]

2.4.2 Governmental Issues

Business interests worked against individuals' rights to information privacy, and the circumstances surrounding DPSIP issues and the governments of the US and CA illustrates how global DPSP laws remain largely ineffective. The Canadian Privacy Act was passed in 1983 to set up some rules for dealing with personal information; it also established the federal office of Privacy Commissioner. In 2008, Jennifer Stoddart, then current Privacy Commissioner of CA, reported that the government's desire for more information and businesses wanting more profits were threatening privacy. Privacy rights were becoming more fragile and CA was moving into a surveillance society. Government privacy complaints dropped from 839 to 759 in the current 2008 year. The number still showed that the DPSIP legislation was not working well. The Stoddart conclusion was that the "*Privacy Act* needs to be overhauled."[142] A number of Canadian governmental offices received privacy violation complaints.[143] Updating the

---

[141] See Katherine Albrecht & Liz Mcintyre, *Spychips: How Major Corporations and Government Plan to Track Your Every Move with RFID* (Nelson Current 2005); Joel Bakan, *The Corporation: The Pathological Pursuit of Profit and Power* (Free Press 2004); and Wade Rowland, *Greed, Inc.: Why Corporations Rule Our World* (Arcade Publishing 2006).

[142] Jennifer Stoddart, *Annual Report to Parliament 2007-2008: Report on the Privacy Act* (2008), http://www.privcom.gc.ca/information/ar/200708/200708_pa_e.asp (last visited on 6 December 2012), at 29.

[143] The list included Agriculture and Agri-Food Canada, Canada Border Services Agency, Canada Post Corporation, Canada Revenue Agency, Canada School for Public Service, Canadian Air Transport Security Authority, Canadian Food Inspection Agency, Canadian Human Rights Commission, Canadian Security Intelligence Service, Canadian Space Agency, and Canadian Transportation Agency. Citizenship and Immigration Canada, Correctional Service Canada, Environment Canada, Department of Justice Canada, Export Development Corporation, Fisheries and Oceans, Foreign Affairs and International Trade Canada, Freshwater Fish Marketing Corporation, Health Canada, Human Resources and Social Development Canada, Immigration and Refugee Board, Indian and Northern Affairs Canada, and Industry Canada received violation notices. The Office of the Inspector General of the Canadian Security Intelligence Service, Library and Archives Canada, National Defence, National Parole Board, Office of the Chief Electoral Officer, Privy Council Office, Public Safety Canada, Public Service Commission Canada, Public Works and Government Services Canada, and even the Royal Canadian Mounted Police were

Privacy Act was only a beginning. The data showed significant compliance problems.

The common law traditional *Zone of Privacy,* was diminishing. Virtually every major change in life was recorded and shared somewhere in government databases directly or purchased from private firms. California's criminal database had more listings than the state's entire population. Under current law, discovered DPSIP violations were useless unless there was a finding of individual harmful effects.[144] The legal standard resulted in few to no enforceable checks and balances on abuses.

Recent US federal administrative policies favored governmental and business interests over personal or private interests. For example, the Computer Matching and Privacy Protection Act[145] gave federal agencies the power to match or bar use of data with no private right of action.

The government could publish personal data based upon arrest (not just conviction) records.[146] Florida matched registration, notification, driver license, vehicle titles, geo-matching, and imaging software. The data was open to the public, in the name of public safety.[147] During the first Bush[148] campaign, the Florida system used data mining program databases to delete voters that could potentially vote Democratic.[149] An increasing number of states were publishing name, address, and photographs of released sex offenders on the net.[150]

---

violators. Service Canada, Statistics Canada, Transport Canada, Treasury Board of Canada Secretariat, and Veterans Affairs Canada finished the list.

144 *Whalen v. Roe*, 429 U.S. 589, (1977). (US)

145 5 USC 552a (1988). (US)

146 *Paul v. Davis*, 424 U.S. 693, (1976). (US)

147 James T. Moore, *Sexual Predators Can't Hide Thanks to Public Safety Information Act*, 6 Community Policing Exchange Phase V, 21, 8 (1998).

148 Aka George W Bush, Bush 43, Bush Junior, or Bush the Second.

149 John W. Dean, *Broken Government: How Republican Rule Destroyed the Legislative, Executive, and Judicial Branches* (Viking. 2007).

150 Charisse Jones, *States Name Sex Offenders on Net*, US TODAY (1999, January 19), http://sige260.tripod.com/megnet.html (last visited on 20 July 2012).

Fractions within the US government itself used the Internet to limit, shape discourse, and propagandize, with relative immunity. Speaker of the House Gingrich used Thomas, a government site, over which he had significant control, for partisan political purposes.

The Digital Telephony Act[151] gave officials power to "tap" any voice, text, data, or digital technology. All telephone companies had to comply when presented with a warrant. Under Federal policy, police officials could eavesdrop-record telephone conversations, without a court order, if one of the parties consented. Wiretapping was on the rise - 600 percent from 1968 to 1996 in the US. The data from 1996 to 2006 showed a 1996 report of almost 600 instances of wiretapping that increased to over 1300 in 2006 reports. Beginning in 1997, state courts issued more wiretapping warrants than federal courts.[152]

The Terrorist Identities' Datamart Environment (TIDE) was US President George W Bush's effort to collect data on potential terrorists. At first, the list only included foreigners but the policy changed to include US citizens. The database grew from 100,000 in 2003 to over 435,000 in four years. Once a person was on the list, it was almost impossible to get off. There was no uniform standard for inclusion. Russ Travers, the TIDE director reported that the biggest problem related to the list was quality control. He further disavowed any responsibility for how governmental agencies use the data.[153]

---

151 Digital Telephony Act aka, Communications Assistance for Law Enforcement Act 1994 § 18 USC 2510-2522 (1994). (US)

152 Office Of The United States Courts, *Report of the Director of the Administrative Office of the United States Courts on Applications for Orders Authorizing or Approving the Interception of Wire, Oral, or Electronic Communications* (2007), http://www.uscourts.gov/wiretap06/2006WT.pdf (last visited on 31 December 2012), at 7.

153 Karen Deyoung, *Terrorism Database is Ballooning, Keepers Say* (2007, March 26), http://www.boston.com/news/nation/washington/articles/2007/03/26/terrorism_database_is_ballooning_keepers_say/ (last visited on 2 January 2012).

Evidence of governmental agencies not following the law was rampant, for example illegal use of wiretaps and use of governmental powers. Governments established rules that did not necessarily apply to them. When an Internal Revenue Service (IRS) employee exceeded his authorized access to view the files of several persons, the courts ruled that he did not misuse the federal computer or violate any laws.[154]

Federal agencies even ignored the principle of data accuracy. Only twenty-five percent of Federal Bureau of Investigation (FBI) criminal files were accurate or complete. There was little computer security or control. Abuses occurred regularly.[155]

In May of 2006, the Veterans Administration (VA) lost control of personal data of 26.5 million veterans. In February 2007, the VA lost control of personal data for 535,000 veterans and 1.3 million doctors. Much of the data was not encrypted.[156]

The Californian State Retirement Board allowed the publication of 445,000 names, addresses and social security numbers. The Board complied with state notification laws and decided to review privacy practices.[157]

During his Presidency, George W. Bush signed and issued over 750 signing statements,[158] which in essence, stated that the law did not apply to him.

---

[154] *U.S. v. Czubinski*, 106 F3d 1069 (1st Cir.), (1997). (US)

[155] United States Government Accountability Office, *Information: FBI Needs to Address Weaknesses in Critical Network*. (2007), http://www.gao.gov/new.items/d07368.pdf (last visited on 31 December 2012).

[156] Sharon Gaudin, *Missing Hard Drive Holds Sensitive Data On 535K Vets, 1.3M Doctors*, Information Week: The Business Value of Technology (2007, February 13), http://www.informationweek.com/news/showArticle.jhtml?articleID=197005769 (last visited on 1 January 2012).

[157] Jaikumar Vijayan, *Oops! Calif. State Pension Fund Admits Breach of Retiree Data* (2007, August 22), http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9032159&intsrc=hm_list (last visited on 2 January 2012).

[158] President Reagan wanted a line item veto on any signed legislation. This power was denied as the Constitution only gave the president three options; do nothing, sign the bill, or veto the entire bill. Regan invented another option – giving a signing

When the 2006 postal renewal legislation was re-authorized, George W. Bush's signing statement included the power to open first class mail without a court warrant. No prior authority to do this existed in the entire history of the country.[159]

In 2003, Congress stopped a Pentagon data-mining program because of privacy violations voiced by the public. In 2007, the Department of Homeland Security (DHS) tested a similar program. The DHS test used real citizen data including hotel reservations and flight information. According to the Government Accountability Office (GAO), the Analysis, Dissemination, Visualization, Insight and Semantic Enhancement (ADVISE) program violated data protection and information privacy legal principles. There was no notification, the agency lied about the data source, and the data analysis included a purpose other than that for which the data was collected.[160]

From 2003 through 2005, the FBI used administrative subpoenas, called national security letters which were not subject to judicial review to obtain personal information on over 142,000 citizens. There were no legal controls, checks, or balances over the data collection. The Office of the Inspector General reviewed the practices and found that the FBI under reported the actual data by at least twenty-two percent. The FBI data was stored in data bases open to 12,000 governmental agencies including foreign governments.[161]

---

statement that declared that the law would or would not be followed. Bush I and Bush II, and even Obama have continued the practice. The practice under minds the principles of the rule of law and separation of powers under the Constitution.

159 Associated Press, *Bush's Statement Opens Up Mail Privacy Debate* (2007, January 7), http://www.sptimes.com/2007/01/07/Worldandnation/Bush_s_statement_open.shtml (last visited on 2 December 2012).

160 Ellen Nakashima & Alec Klein, *New Profiling Program Raises Privacy Concerns* (2007, February 28), http://www.washingtonpost.com/wp-dyn/content/article/2007/02/27/AR2007022701542.html (last visited on 3 December 2012).

161 R. Jeffrey Smith, *Report Details Missteps in Data Collection* (2007), http://www.washingtonpost.com/wp-dyn/content/article/2007/03/09/AR2007030902353.html (last visited on 2 January 2012).

DPSIP legal issues related to government were unsettled. Moves to lower the privacy protection standard came from both business and government. Meanwhile in 2007, 162 million personal records were violated: three times more than the 49.7 million the year before.[162] The current DPSIP approach was not working.

The GAO reported that, contrary to law, the federal government did not consistently provide privacy protections on the collection and use of data. The report found that the federal government was not "Ensuring that collection and use of personally identifiable information is limited to a stated purpose."[163] Agencies did not justify the collection and use of personally identifiable information. The use of the Federal Registry, the federal government's public notice release, was difficult to decode and was not an effective manner to release information to citizens.

A follow-up report found that contrary to law, federal agencies did not consistently have a designated senior privacy officer who had authority to monitor all key privacy issues. Fifty percent of the agencies studied failed to meet legal mandates.[164]

The GAO called for major revisions of the Privacy Law[165] and the E-Government Act.[166] The acts were too narrowly defined so that massive privacy violations are legally possible. Personal information was collected

---

[162] Byron Acohido, *Theft of Personal Data More Than Triples This Year* (2007, December 9), http://www.usatoday.com/money/industries/technology/2007-12-09-data-theft_N.htm?POE=click-refer (last visited on 2 January 2012). See Jaikumar Vilayan, *Forget Hackers; Companies Responsible for Most Data Breaches, Study Says* (2007, March 10), http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9013142&intsrc=news_list (last visited on 2 January 2012).

[163] United States Government Accountability Office, *Alternatives Exist for Enhancing Protection of Personally Identifiable Information* (2008, April 19), http://www.gao.gov/new.items/d08536.pdf (last visited on 19 June 2012), at 2.

[164] United States Government Accountability Office, *Agencies Should Ensure that Designated Senior Officials Have Oversight of Key Functions* (2008, May 30), http://www.gao.gov/new.items/d08603.pdf (last visited on 18 June 2012).

[165] Privacy Act of 1974. 5 U.S.C. § 552(a)(4) (1974). (US)

[166] E-Government Act of 2002 amend. 44 USC 101 (2002). (US)

and used beyond a stated purpose. There was no "effective mechanisms for informing the public about privacy protections."[167]

Not only did governments not protect the privacy rights of their citizens, the governments themselves violated citizens rights. As noted in this section, data from CA and the US revealed patterns of governmental abuses of DPSIP legal principles. Data on governmental abuses in the other countries in this study are found in the appropriate country chapters.

2.5 Data Protection and Security Violations; Analogous Legal Issues Including Informed Consent, Confidentiality, Impact Assessments, and Audits

Although businesses and governments colluded to prevent the creation of effective DPSIP laws, there are related basic legal principles, that are typically ignored but, that should apply to DPSIP law. These legal principles come from two different legal traditions. The first is health care law, where the legal standard is informed consent. The second comes from environmental law, where the legal standard is the requirement to conduct an environmental impact study and get approval prior to acting. Both legal principles can be applied to the topic at hand.

Prior to collecting, storing, using, distributing, or selling personal information data, the data subject of the information should give an informed consent. The informed consent should meet the legal requirements for any lawful informed consent. Prior to using any business method or the government granting any intellectual property protection, the party should conduct and gain approval of the proposal through a privacy impact study and approval.

---

167 United States Government Accountability Office, *Congress Should Consider Alternatives for Strengthening Protection of Personally Identifiable Information* (2008, June 18), http://www.gao.gov/new.items/d08795t.pdf (last visited on 18 June 2012) at 2.

2.5.1 Informed Consent and Confidentiality Issues

A body of legal literature addresses the right and obligations of clients, consumers, customers, patients, and research subjects to give consent to the nature of the effects of products and services. The nature of such rights and obligations should certainly expand to data protection and information privacy law.

Informed consent is a legal concept that is best known in medical and research law. The basic structure of a duty of care also applies to DPSIP law. The advent of computer technology and the interdependence of technology, people, and holders of data create a tension. Transparency helps to resolve the tension and helps to keep all parties honest. Informed consent establishes that prior to collecting, using, or distributing sensitive data the holder should obtain consent from the subject, the real personal owner of the data. Informed consent includes giving people sufficient information about the process, so they can make an aware, educated choice or decision. The process is essential when it puts people at risk or the holder obtains financial or strategic gains that were not compensated.[168] Owners of the raw data should be compensated if taken without consent,

Informed consent law promotes personal autonomy and a sense of control. Tom Beauchamp and James Childress define autonomy as a "personal rule of the self that is free from both controlling interferences by others and from personal limitations that prevent meaningful choice."[169] Research in the field shows that when informed consent is instituted, there are better deliberations,

---

[168] Jessica W. Berg, et al., *Informed Consent: Legal Theory and Clinical Practice* (2nd ed., Oxford University Press 2001); Ruth Faden & Tom L. Beauchamp, *A History and Theory of Informed Consent* (Oxford University Press 1986); E.S. Glass, Restructuring Informed Consent: Legal Therapy for the Doctor-Patient Relationship, 179 *Yale Law Journal* 8, 1533 (1970).

[169] Tom L. Beauchamp & James F. Childress, *Principles of Biomedical Ethics,* at 121 (4th ed., Oxford University Press 1994).

decreased stress, less litigation, more consumer respect, more positive relationships, mutual decision making, and negotiations.[170]

In the medical field, informed consent honors and safeguards patients' bodily integrity, and fosters deliberation, negotiation, and mutual decision making. Informed consent is also important for pragmatic reasons because studies showed practitioner disclosures positively related to outcomes such as patients' post-procedure adjustment, patient attitudes toward medical staff, treatment efficacy, and decreased stress.[171] The principle of informed consent protects the individual from unknown decision-making knowledge and risks. The principle also protects the holder of the information or service provider from litigation due to a lack of transparency. All the characteristics of informed consent would hold true where DPSIP issues are at stake.

From an ethical perspective, informed consent is an Immanuel Kant[172] categorical imperative of treating all people as ends rather than simply means applied. Using coercion, deception, misdirection, or not providing knowledgeable consent was a significant violation. Failing to provide informed consent was a form of manipulation. A corollary was the principle of liberal individualism. The principle was defined as “the conception that in a democratic society a certain space must be carved out within which the individual is protected and allowed to pursue personal projects."[173]

---

170 *Ibid.*

171 Irving L. Janis, *Psychological Stress: Psychoanalytic and Behavioral Studies of Surgical Patients* (Wiley & Sons 1958); R. T. Mills & D. S. Krantz, Information, Choice, and Reactions to Stress: A Field Experiment in a Blood Bank with Laboratory Analogue, 37 *Journal of Personality and Social Psychology* 4, 608 (1979); David T. Vernon & Douglas A. Bigelow, Effects of Information About a Potentially Stressful Situation on Responses to Stress Impact, 29 *Journal of Personality and Social Psychology* 1, 50 (1974).

172 Immanuel Kant, The Metaphysics of Morals. (Originally published in two parts in 1797 as the *Doctrine of right* and the *Doctrine of virtue*) (Mary Gregor trans, Cambridge University Press 1797/1996).

173 Tom L. Beauchamp & James F. Childress, *Principles of Biomedical Ethics*, at 70 (4th ed., Oxford University Press 1994).

Several national Federal Courts have recognized the concept of consent and limiting business activities. The District Court of Wyoming ordered Abika.com, an Internet company, to "stop selling telephone records without owners' consent and to turn over nearly $200,000 in profits from the operation."[174] The Company had been using "false pretenses, fraudulent statements, fraudulent or stolen documents or other misrepresentations to induce telecom carriers to disclose the confidential records."[175] The court found that the company's ways of obtaining phone records, without consumers' consent, was "necessarily accomplished through illegal means, and those defendants knew that the phone records were being obtained surreptitiously."[176] The action was justifiable under an administrative law fact finding directive of the Federal Trade Commission that was supported by the courts. The Court clearly established that consent applied to collecting, storing, and selling or distributing personal data. The court also established the principle that the Courts can force businesses to cease-and-desist practices that were a violation of DPSIP law.

The legal principle of informed consent was a comparatively recent development. The standards had been clearly established in research standards with human subjects; counseling, psychotherapy, and medicine practices; and consumer protection laws. Many of the regulatory principles applied, in principle, to DPSIP law.

Constitutional and tort law in many jurisdictions have established individual privacy rights as the right to be left alone by business, commercial,

---

174 Grant Gross, *Update: Court Bars Company from Online Sale of Phone Records* InfoWorld. (2008, January 28), at http://www.infoworld.com/article/08/01/28/Court-bars-company-from-online-sale-of-phone-records_1.html (last visited on 28 January 2012), at 2.

175 *Id.* at 1.

176 *Id.* at 8.

governmental, individual, and professional sources.[177] The UK case of *Slater v Baker and Stapelton*[178] established consent requirements prior to medical treatment. Since that time, courts have determined that deceptive, fraudulent, or misleading disclosures violate the legal standard of consent.[179]

In *Whalen v. Roe*[180] the US Court ruled that each individual had the constitutional right to "avoid the disclosure of personal matters." The case involved a New York state law that required physicians to inform the state of individuals' prescribed addictive medications. The ruling limited the government's role in obtaining, accessing, and analyzing personal information. The government circumvented this ruling by buying information from data collecting companies that it helped to form. The restrictions needed to expanded to include governments and businesses.

Informed consent should be a minimum for most if not all data collection, and confidentiality principles also apply to DPSIP issues. When discussing the collection and use of information data, Justice John Paul Stevens ruled that "The right to collect and use (personal information) for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures . . . in some circumstances that duty arguably has its roots in the Constitution."[181] Justice Stephens further ruled: "The cases sometimes characterized as protecting *privacy* have in fact involved at least two different kinds of interests. One is the individual interest in avoiding disclosure of personal matters, and another is the interest in independence in making certain kinds of important decisions."[182] Under the Fourteenth Amendment, Justice Stevens argued that the New York statute "threatens to impair both (patients') interest in the nondisclosure of private information and

---

177 W. Page Keeton, et al., *Posser and Keeton on the Law of Torts* (West Publishing 1984).

178 *Slater v. Baker & Stapelton*, 95 English Reporter 860 (K. B.), (1767) (UK).

179 See *Hunt v. Bradshaw*, 88 S.E. 2d 762 (N.C. 1955); *Paulsen v. Gundersen*, 260 N.W. 448 (Wis. 1935); *Wall v. Brim*, 138 F.2d 478 (5th Cir. 1943); *Waynick v. Reardon*, 72 S.E.2d 4 (N.C. 1952). (US)

180 *Whalen v. Roe,* 429 U.S. 589, (1977) at 600. (US)

181 *Id.* at 589.

182 *Id.* at 589-600.

also their interest in making important decisions independently."[183] The decision had limited global impact because Justice Stephens also declared that the case did not "decide any question which might be presented by the unwarranted disclosure of accumulated private data whether intentional or unintentional or by a system that did not contain comparable security provisions."[184]

The *Nixon v. Administrator of General Services*[185] case cited the "Whalen case." Nixon was fighting the release of records under the 1974 - Nixon specific - Presidential Recordings and Materials Preservation Act.[186] Justice William Brennan wrote that the law provided safeguards to protecting President Nixon's private papers. Justice Brennan wrote that "One element of privacy has been characterized as 'the individual interest in avoiding disclosure of personal matters . . . public officials, including the President, are not wholly without constitutionally protected privacy rights in matters of personal life unrelated to any acts done by them in their public capacity."[187]

As early as 1980, Willis Ware[188] wrote about the importance of control over personal and confidential information. Ware argued that confidentiality needed to protect on three levels. The first was that sensitive information should be protected against improper use. The second was that there must be an agreement establishing an agreement between the people dealing with sensitive information. The third was granting a legal confidentiality privilege that covered those involved in handling sensitive data.

2.5.2 Privacy Impact Assessment

---

183 *Id.* at 600.

184 *Id.* at 605-606.

185 *Nixon v. Administrator of General Services*, 433 U.S. 425, (1977). (US)

186 Presidential Recordings and Materials Preservation Act (PRMPA) amend. 44 U.S.C. § 2111 (1974). (US).

187 *Nixon v. Administrator of General Services*, at 457. (US)

188 Willis H. Ware, Privacy and Information Technology — The Years Ahead, *in Computers and Privacy in the Next Decade* (Lance J. Hoffman ed. Academic Press1980).

In addition to establishing informed consent in laws governing data collection and use, the laws should require those who would use personal information for gain to conduct impact studies and get approval prior to acting in some circumstances. Over the past several decades, a growing mistrust of the interaction between governments, business–industry, and technology have grown. Responses to problems have resulted in the development of new legal and regulatory standards. A classic example began in environmental law with the establishment of a requirement that an environmental assessment, impact and studies must be done. Similar standards can be applied to DPSIP law. The fields shared issues of technology, governmental failures, business abuses, and the need for protection. Each must address risk assessment, communication, and management.

A number of authors had defined "impact assessment" and studied the approaches followed in this regard. Each definition contributed to understanding the process and its relevance to DPSIP legal issues. Gordon Duinker and Peter Beanlands offered a definition of "a process or set of activities designed to contribute pertinent environmental information to a project or program decision-making."[189] Dipper suggested that the process was a "systematic procedure for enabling the possible environmental impacts of developments to be considered before a decision is made on whether the project should be given approval to proceed."[190]

Draper and Reed concluded that such assessments involved sound scientific research and documentation to reveal potential consequences of the proposed action, product or process.[191] Gibson suggested such assessments should consider environmental, financial, political, and technical factors in the

---

189 Gordon E. Duinker & Peter N. Beanlands, *An Ecological Framework for Environmental Impact Assessment in Canada*, at 18 (Institute for Environmental Systems, Dalhousie University 1983).

190 Ben Dipper, et al., Monitoring and Post Auditing in Environmental Impact Assessment: A Review, 41 *Journal of Environmental Planning Management* 6, 731 (1998), at 731.

191 Dianne Louise Draper & Maureen G. Reed, *Our Environment: A Canadian Perspective*, at 554 (Thompson Nelson 2006).

decision making process.[192]

Robert Munn proffered that assessments address issues such as identifying, interpreting, predicting, and communicating impacts.[193] Ortolano and Shepherd maintained that impact assessments are an effective means to evaluate and predict unintended consequences of project approvals.[194] Smith suggested that such an approach is a resource management process that aids in the introduction of sound system changes.[195]

The UK Department of the Environment defined Environment Impact Assessments as:

> essentially a technique for drawing together in a systematic way, expert qualitative assessment of a project's environmental effects and presenting the results in a way that enables the importance of the predicted effects and the scope for integrating or mitigating them, to be properly-evaluated by the relevant decisions making bodies before a decision is given.[196]

Macha and Makaramba provided a United Nations (UN) definition. Impact assessments were:

> a technique and a process by which information about the environmental effects of *a* project is collected, both by the developer and from other sources and taken into account by the decision making authority in forming a

---

[192] Robert B. Gibson, Environmental Assessment Design: Lessons from the Canadian Experience, 15 *The Environmental Professional*, 12 (1993), at 12.

[193] Robert Edward Munn, *Environmental Impact Assessment: Principles and Procedures: Scope Report 5* (United Nations Environment Program; Environment Canada; United Nations Educational, Scientific And Cultural Organization 1985), at 159.

[194] Leonard Ortolano & Anne Shepherd, Environmental Impact Assessment: Challenges and Opportunities, 13 *Impact Assessment*, 1, 3 (1995), at 3.

[195] L. Graham Smith, *Impact Assessment and Sustainable Resource Management*, at 95 (Longman Scientific and Technical 1993).

[196] United Kingdom Department of The Environment, *Environmental Assessment, Circular 15/1988* (FaLSO 1988), at 7.

judgement on whether the development should go ahead.[197]

The public and impacted stakeholders needed a forum where they could express concerns, gain education and information, and have an impact on decision-making. The process makes sure that all of the relevant factors are considered in the decision making process.[198] The law should allow individual, class action, and public interest causes of action. A range of options provided a means to adapt to public ignorance about the issues, other survival concerns, time concerns, lack of connection to interest groups that may have adequate resources, and lack of political will.

William Sheate established that early assessment and public involvement were critical, because it would result in essential issues not being ignored.[199] The decision-making process and data would become more accountable, effective, responsible, and transparent. Checks and balances require compliance on the part of all parties and decision-makers. Corruption must be illegal.

DPSIP law impact processes should follow the Canadian environmental standards. Under the Canadian law, the federal and provincial governments had a shared responsibility. Each province had the power to set standards while the federal government addressed inter-provincial issues and international compliance. The legal standards should function to "restore the social equilibrium, to set forth the legal consequences of actions, and to educate people in order that they be aware of emerging social problems."[200] Fines and other interventions must be a real deterrent and "satisfy (the) public demand for aggressive governmental intervention."[201] Courts and administrative agencies must apply the

---

[197] V. Macha & R. Makaramba, *The Development and Harmonization of EIA Regulations — Tanzania Country Report*, in *The Development and Harmonization of Environmental Laws in East Africa: Development and Harmonization of EJA Regulations*, at 117 (Joint Project on Environmental Law And Institutions In Africa ed. 1999).

[198] Neil A. F. Popovic, The Right to Participate in Decisions That Affect the Environment, 10 *Pace Environmental Law Review* 2, 683-709 (1993, Spring), at 698.

[199] William R. Sheate, Public Participation: The Key to Effective Environmental Assessment, 21 *Environmental Policy and Law* 3/4, 156 (1991), at 156.

[200] David Trezise, Alternative Approaches to Legal Control of Environmental Quality in Canada, 21 *McGill Law Journal* 404 (1975), at 404.

[201] *Id.* at 406.

statutory fines and requirements. Similar to environmental standards, DPSIP law should establish that no injury in fact is required for liability. Strict liability principles should apply to the purchase or sale of DPSIP data. Failure to follow DPSIP standards is presumptively unsafe.[202]

While some argued there should be a different response to DPSIP violations based upon degree of damage, this approach could be difficult to determine in the immediate period. Determining if a violation would result in a temporary impairment, permanent impairment, or complete destruction was not always clear-cut. No violation was insignificant or acceptable. An individual violation could result in cumulative effects. The US Court of Appeals (9th Circuit) set a key impact assessment standard. The court ruled that such assessments must consider "unrelated but reasonably foreseeable future actions."[203] In a similar case, the same court ruled that the plaintiff only needed to allege, not conclusively prove, significant impact potentials in an impact assessment.[204]

Manufacturers of new products and products for use in CA needed to provide an environmental risk assessment and be approved by the appropriate regulatory body. The major legislation in this area included the Canadian Environmental Assessment Act (CEAA),[205] Canadian Environmental Protection Act (CEPA),[206] and Pest Control Products Act (PCPA).[207] The standards were based on the UK Robert May[208] guidelines. Early assessment and intervention based on sound principles, review, and

---

202 David Wright & Paul. De Hert, *Privacy Impact Assessment* (Springer ed. 2012).

203 *Save the Yaak Committee v. Block*, 840 F.2d 714 (9th Cir., (1988), at 720. (US)

204 *Sierra Club v. United State Forest Service*, 843 F.2d 1190 (9th Cir. 1988). (US)

205 Canadian Environmental Assessment Act (CEAA) amend. S.C. 1992, c. 37 (1992). S.C. 1992, c. 37 (CA)

206 Canadian Environmental Protection Act (CEPA) amend. c. 15.31 (1999). (CA)

207 Canadian Pest Control Products Act (PCPA) amend. S.C. 2002, c. 28 (2002). (CA)

208 Robert May, *Guidelines 2000: Scientific Advice and Policy Making* (UK Office of Science and Technology 2000).

accountability were critical. The same principle of impact audits should apply to DPSIP legal principles and issues.

The Supreme Court of CA, in *R. v. Edwards Books and Art Ltd*[209] clarified a key issue related to impact statements and information privacy. The Court ruled that the government and even private firms that held data were open to regulation.

The Provincial Environmental Bill of Rights[210] registration legislation supported impact assessments. The Act generally protected personal privacy data and trade secrets. Malcolmson and Myers[211] maintained that impact assessments and the Charter of Rights respected individual privacy rights.

Canada is not the only country included in this thesis to have well established legal principles incorporating impact assessment. In 1990, AU started using a privacy impact assessment program. The in-depth approach was used through the project life cycle and engaged all stakeholders.[212] However, the business sector and some governmental agencies endeavored to weaken privacy protections and the power of the privacy impact assessment approach.[213]

The UK approach used privacy impact assessments at various stages of development of the process. Standards were established for the initial assessment, full-scale, and small-scale situations. The approach examined privacy law and data protection compliance.[214]

---

209 *R. v. Edwards Books and Art Ltd*., (1986) 2 S.C.R. 713 at 779, (1986) (CA).

210 See http://publications.gc.ca/Collection-R/LoPBdP/BP/bp281-e.htm

211 Patrick Malcolmson & Richard Myers, *The Canadian Regime: An Introduction to Parliamentary Government in Canada* (3rd ed., University of Toronto 2005).

212 David Wright & Paul. De Hert, *Privacy Impact Assessment* (Springer ed. 2012) at 121.

213 Id. at 147.

214 David Wright & Paul. De Hert, *Privacy Impact Assessment* (Springer ed. 2012).

The use of privacy impact assessments is limited to selected governmental actions. The E-Government Act of 2002[215] focused on developing or procuring information technology. The use of the privacy impact approach was limited and not effective.[216] The implementation was limited due to problems with access, technical knowledge, and supervision that lacked regulatory intensity.[217]

The acceptance of impact assessments became an internationally recognized and generally enforced approach to addressing DPSIP issues. Impact assessments were a preventive management tool for governments and private businesses. The function was to analyze, identify, quantify, and mitigate the effects of activities, planning, policies, and projects. The goal was to prevent damaging impacts through mitigation of technology and privacy practices.

Impact and risk assessments included the application of scientific principles to logically evaluate the probability of decisions and technology to have a harmful effect. The focus was on accountability, information, transparency, and examining unintended consequences prior to implementation of a policy or technology.

In the 1970s, the US federal government started implementing formal risk impact assessment standards.[218] The assessment, conducted by governmental agencies, businesses, or industries, corrected or prevented hazards. The World Health Organization[219] established international risk assessment standards. The assessments included computer modeling, data monitoring, or historical data. The process involved objective examination of

---

215 *E-government Act* amend. (Pub.L. 107-347, 116 Stat. 2899, 44 U.S.C. § 101, H.R. 2458/S. 803) § (2002). (US)

216 David Wright & Paul. De Hert, *Privacy Impact Assessment* (Springer ed. 2012).

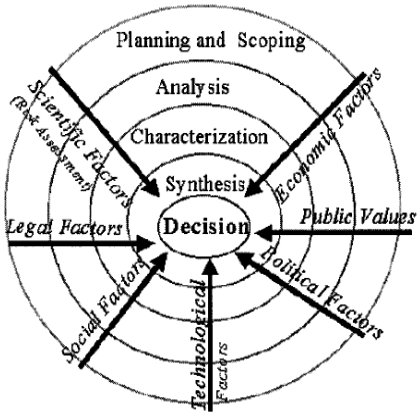
217 Spiros Simitis, Reviewing Privacy in an Information Society, 135 *University of Pennsylvania Law Review* 3, 707 (1987, March).

218 Commission on Risk Assessment and Risk Management, *Risk Assessment and Risk Management in Regulatory Decision-Making: Final Report* (Volume 2) (Government Printing Office 1997).

219 World Health Organization, *Risk Assessment - The Programme* (2008), www.who.int (last visited on 2 March 2012).

alternatives considered, bias, information, context, key conclusions, perspective, policy choices, research needs, scientific assumptions, sensitive subpopulations, strengths uncertainty, variability, and weaknesses.[220] The following figure graphically shows the decision making process.

Figure 2.0 Impact Assessment Decision Making Model



This risk assessment decision-making model provided a structured process to determine areas of concerns and policy directions. No model or process was ever one hundred percent accurate. In the more complex models, there were always concerns about data errors, human errors, lack of independence, political or economic agendas, political or economic incentives, technological illiteracy, uncertainly, and value judgments that must be controlled.

The legal and regulatory principles included the supremacy of the individual including the ability to offer free and informed consent. Respects for the rule of law formal and material legitimacy were essential. Continuous scrutiny was a major part of establishing and monitoring the actor's duty and liability. This model required that government and business processes must be transparent,[221] that the process must be free from intimidation and political pressure, that the legal and regulatory process must be a democratic

---

[220] United States Environmental Protection Agency, *Science Policy Council Handbook: Risk Characterization* (Government Printing Office 2000).

[221] Jeffery Hutchings, et al., Is Scientific Inquiry Incompatible with Government Information Control? 54 *Canadian Journal of Fisheries and Aquatic Sciences* 5, 1198 (1997).

safeguard.[222] And that the risk assessment must be independent and not a duplication of stakeholder interests.[223]

The US 1974 Privacy Act[224] requires that all federal agencies conduct Privacy Impact Assessments on new programs. The reality is that compliance is slow. Two major problems with the law exist. The first is that the principle only applied to federal agencies, not all governmental and business organizations. The second is that the principle does not apply to government issued protections such as trademarks, patents, or copyright. A sound data protection and information privacy law must correct the problems found in the US approach.

2.6 Technological Innovations Received Governmental Approval and Protection without Examining Information Privacy, Data Protection, and Data Security Assessments

Not only were appropriate impact assessments not conducted, the research showed that governments had even granted intellectual property protections for technological innovations without assessing or examining the DPSIP implications.

Many Internet businesses used "cookies" and click streams[225] to monitor and collect information.[226] In 1994, Netscape developed cookies in response to interest from business concerns to help make on-line shopping easier. Greed

---

222 Robert May, *Guidelines 2000: Scientific Advice and Policy Making* (UK Office of Science and Technology 2000).

223 Jeremy D. Fraiberg & Michae J. Trebilcock, Risk Regulation: Technocratic and Democratic Tools for Regulatory Reform, 43 *McGill Law Journal* 4, 835 (1998).

224 5 U.S.C. 552a. (US)

225 Technological methods to track and record activities by collecting use information. The data is collected without notice and IP protection was afforded without an impact audit.

226 When Netscape first introduced cookies in October 1994, the corporation obtained intellectual property protection in 1998 with no legal review or privacy impact audit. See European Patent Office, *Persistent client state in a hypertext transfer protocol based client-server system. European G06F17/30W9; H04L29/08N1; U.S. US19950540342 19951006* (1998, June 30), http://v3.espacenet.com/publicationDetails/biblio?CC=US&NR=5774670&KC=&FT=E

and power took over. Some sites (e.g. Microsoft) would not allow entry *without* cookies. Some sites required that users provide their name, address, and other personal information prior to allowing entry. Most did not ever state information on how the data collected will be used or shred with other parties. Many businesses had not accepted "anonymous profiling."[227] One firm established a single identification card for all net activities. The database could track all related transactions.[228]

Netscape introduced cookies as a default feature of its new browser without getting informed consent of the customer or even letting customers know that cookies will be used. Cookies were hidden and not transparent by design. No documentation provided information on cookies or the privacy implications. The practices violated a range of contract, tort, and privacy law standards with legal protections. The Netscape program existed for two years before it was discovered that cookies were used. Jackson broke the story in the London *Financial Times*.[229]

The effect of cookies on protection of privacy on the Internet is illustrated by the statement of John Schwartz agreeing with Lawrence Lessig that “Before cookies, the Web was essentially private. After cookies, the Web became a space capable of extraordinary monitoring."[230]

Persistent Client State HTTP Cookies were developed. Rather than just assisting in shopping, these types of cookies tracked considerable personal information and shared it with unknown sources. So called “attached referrer information” made privacy right violations much higher. Without consent,

---

227 Demographic information is released, but not personally identifying data.

228 Jon Healey, *California Firm Develops Single ID for Users of Online Services* (1999, November 2), http://www.accessmylibrary.com/comsite5/bin/comsite5.pl?page=library&item_id=0286-5612708&override=Y&zip=92706&authtime= (last visited on 9 September 2012).

229 Tim Jackson, *This Bug in Your PC is a Smart Cookie*, Financial Times (1996, February 12), at A1.

230 John Schwartz, *Giving the Web a Memory Cost Its Users Privacy*, New York Times (2001, September 4), http://www.nytimes.com/2001/09/04/technology/04Cook.html (last visited on 10 May 2012), at 4.

environmental impact studies, or any reasonable regulatory response, cookies were everywhere. Collection, storage, and sharing of personal information ignored that data subjects must retain control over ones personal information and even consideration of the question of ownership. These are part of the core DPSIP law principles. Since HTTP cookies could be blocked or removed, flash cookies were developed that were harder to remove or block. Fifty-four of the top one hundred web sites quickly adopted the new flash cookies.[231]

The Internet Engineering Task Force (IETF) was determined to set standards for state management of the Internet. The Netscape standard won the process. The Task Force erroneously rejected the proposal by Kristol[232] that information available to the state be limited to the immediate site only. When the visit was over, the data would be destroyed and there was no allowance for third party cookies. IETF accepted the rejection of third party cookies but Netscape objected. The US Federal Trade Commission (FTC)[233] held hearings on cookies but lacked the minimal technological sophistication to make a sound decision. Netscape lied to the commission with no ramifications. Governmental regulators, legislators, and the courts did nothing to require that the user must consent to processing, or to require that impact studies be done, or that computer privacy must be protected. Microsoft's Internet Explorer, also used default cookies and allowed third party cookies. At the time of this writing, Netscape was out of business, but cookies continued to impact information privacy worldwide with no constraints.

Many in the computer field argued that universities rather than business organizations should develop web browsers and computer infrastructures.

---

231 Angela Moscaritolo, *Top Websites Using Flash Cookies to Track User Behavior*, SC Magazine for IT Security Professionals (2009, August 11), http://www.scmagazineus.com/Top-websites-using-Flash-cookies-to-track-user-behavior/article/141486/ (last visited on 12 August 2012).

232 David M. Kristol, HTTP Cookies: Standards, Privacy, and Politics, 1 *ACM Transactions Internet Technology* 2, 151 (2001).

233 Federal Trade Commission, *Privacy Workshop '97 Hearings Transcripts for Session 2, panel 2, part 3*. (1997), http://consumer-info.org/FTCpriv97/FTCprivacyw.asp (last visited on 2 March 2012).

Batya Friedman, Daniel Howe and Edward Felten[234] reported on university activities that focused on building privacy into browsers and other basic computer code. Laura Gurak made the same argument and called for a comprehensive discussion about the issues involving key stakeholders.[235] The calls remained academic (in the negative sense) and government action was made subservient to the business interests.

Entrepreneurial web site owners collected user information without a full informed consent. Advertising firms bought and mined data for more information and use the information for profit.[236] Moreover, governments protected the violating technologies without considering the impact. No one seemed to be asking the right questions because of the overall ignorance of DPSIP legal issues.

2.7 Data Protection and Security Violations Threatened Related Legal Principles and the Security of Individuals, Businesses, and Governments

DPSIP violations threaten the legal rights, obligations, and security of individuals, businesses, and governments. The issues include asset protection, consumer protection law, contract law, information control, intellectual property law, property law, tort law, and privacy law conflicts.

---

234 Batya Friedman, et al., *Informed Consent in the Mozilla Web Browser: Implementing Value-Sensitive Design*, Proceedings of the Thirty-Fifth Annual Hawaii International *Conference on System Science* (2002, January 7-10), http://csdl2.computer.org/comp/proceedings/hicss/2002/1435/08/14350247.pdf (last visited on 4 May 2012).

235 Laura J. Gurak, *Logging in with Laura J. Gurak: Minnesota Professor Takes a Critical Look at Online-Privacy Issues*, The Chronicle of Higher Education. (2002 February 19), http://chronicle.com/free/2002/02/2002021901t.htm (last visited on 4 May 2012).

236 B. Jerry Kang, Information Privacy In Cyberspace Transactions, 50 *Stanford Law Review* 4,1193 (April 1998).

2.7.1 Asset Protection Standards

The asset protection standard is a comprehensive managerial strategy to proactively mitigate risk while safeguarding information, people, and property assets. During the 1990s, the data management industry and businesses desired more personal information control, under the claim that more targeted marketing would be a public good. Paul Schwartz[237] declared that information privacy was a "personal right to control the use of one's data." Anita Allen suggested a paradigm of a bundle of information privacy rights that included promoting personal control over personal information and data.[238]

The asset protection model suggests that data protection and information privacy is an individual right, but more importantly, it is a societal protection from misuse of power. The focus is on the relationship with the government and third parties who have access to the information.[239] The model empowers the individual to have access to and control personal data. The model increases the need for state of the art data protection security upon those who held the data. In terms of this model, the collection and use of personal information should involve an informed consent on the part of the data subject. Furthermore, the law must provide means to control the use of the data. An even greater danger developed as soon as the information becomes knowledge.

The prophetic warning of Orwell's *1984* and Big Brother evolved to include Kafka's *The Trial.* Daniel Solove made the distinction that "[i]nformation consists of raw facts, while knowledge is information that has been sifted,

---

237 Paul M. Schwartz, Internet Privacy and the State, 32 *Connecticut Law Review* 3, 815 (2000), at 838.

238 Anita L Allen, Privacy as Data Control: Conceptual, Practical, and Moral Limits of the Paradigm, 32 *Connecticut Law Review* 3, 861 (2000), at 863.

239 Daniel J. Solove, Access and Aggregation: Public Records, Privacy, and the Constitution, 86 *Minnesota Law Review* 6, 1137 (2002a), at 1194.

sorted, and analyzed."[240] The shift better described a "more thoughtless process of bureaucratic indifference, arbitrary errors, and dehumanization, a world where people feel powerless and vulnerable, without any meaningful form of participation in the collection and use of their information."[241] This description included data held by businesses, not just governments. Privacy as knowledge control was an advancement that covered not only information privacy but also included data in databases, and data mining practices. Large databases destroyed the concept of practical obscurity when information was available but difficult to find practically.[242]

Benn and Gaus[243] noted that the central factor in information privacy was information access. They argued that information violations are related to who benefits and suffers from access abuses, who consents, and who gains power or economic rewards.

Judith DeCew saw information privacy as a means of keeping certain information from the public discourse. She declared that "information about one's daily activities, personal lifestyle, finances, medical history, and academic achievement, whether written or not, part of the public record or not, may be viewed by an individual as information he or she need not divulge and can expect others to guard as well."[244] DeCew further argued that the "expectation of privacy is grounded in the fear concerning how the information might be used or appropriated to pressure or embarrass one, to damage one's credibility or economic status, and so on."[245]

---

240 Daniel J. Solove, Privacy and Power: Computer Databases and Metaphors for Information Privacy, 53 *Stanford Law Review* 6, 1393 (2001), at 1456.

241 *Id.* at 1398.

242 *U.S. Department of Justice v. Reporters Committee for Freedom of the Press*, 489 U.S. 749, (1989). (US)

243 Stanley I. Benn & G. F. Gaus, *The Public and the Private: Concepts and Action*, in *Public and Private in Social Life*, at 8 (Stanley I. Benn & G. F. Gaus eds., Croon Helm, Ltd1983).

244 Judith W. Decew, The Scope of Privacy in Law and Ethics, 5 *Law and Philosophy* 2, 32 (1986), at 75.

245 *Ibid.*

Arthur Miller argued that personal privacy legal standards protect the right of a person to live in different roles. One's aspirations and performance in one context should not be placed in another context without permission. The rights include the individual control over the flow of information not only concerning him but describing him.[246]

David Flaherty classified the information privacy issue as one of "information self-determination."[247] Flaherty also showed that the US approach was not as adequate as data protections laws in other countries.

Steven Spinello described how governments and private businesses had appropriated private personal information without consent or payment. Information was no longer confidential. "Rather, information has become a commodity to be bought and sold for a reasonable fee."[248]

Governments and corporations had taken private information for commercial gain, taken possession of personal information, and exercised control over this form of intangible personal property. Such behavior constituted a tort in some countries.[249] Steven Miller supported the legal principle that a person owns their personal data that includes control over the collection or use of personal data. Such "people deserve a royalty payment any time information about them is sold."[250]

---

246 Arthur R Miller, Personal Privacy in the Computer Age: The Challenge of a New Technology in an Information-Oriented Society, 67 *Michigan Law Review* 6, 1089 (1969), at 1107.

247 David H. Flaherty, On the Utility of Constitutional Rights to Privacy and Data Protection, 41 *Case Western Law Review* 3, 831 (1991), at 832.

248 Richard A. Spinello, *Ethical Aspects of Information Technology*, at 111 (Prentice Hall 1995). The term originated in German law: the German constitutional court declared that an individual has the right of informational self-determination.

249 SA law does not accept this legal position.

250 Steven E. Miller, *Civilizing Cyberspace: Policy, Power, and the Information Superhighway*, at 279 (ACM Press 1995).

According to Don Tapscott, "all personal information, from your weight to your social security number, belongs to you."[251] He argues that people had to assert the ownership right or have it asserted for them. "If people stop giving away their information and started thinking about it as they do other forms of property, expecting to have some control over it, and get paid for its use, then things would begin to change."[252] Unless and until people begin to see their personal data as the asset it is, effective DPSIP protections will not be established.

2.7.2 Contract Law Issues

The concept of applying fundamental principles of contract law to information privacy originated in the UK, and these principles were the basis for contract issues in AU, CA, SA, and the US. The contract law model saw DPSIP issues in contractual terms, which allowed people to negotiate the use of their personal property. The model argued that the default position would be for all holders of personal information to have contractual ownership. Richard Murphy argued, “Because information is voluntarily disclosed, there is no reason both sets of consumers [i.e. the people whose data is held and those that collect, hold, and use it] cannot be satisfied through a contracting process.”[253]

Charles Sykes declared that:

> We can begin to give individuals that control by creating a presumption of privacy as the default setting of the Information Age. Our presumption of privacy should be as strongly held—and jealously guarded—as our presumption that we have free speech, freedom to worship, the right to own private property, and equality of opportunity,

---

251 Don Tapscott, *The Digital Economy: Promise and Peril In The Age of Networked Intelligence,* at 282 (McGraw-Hill 1995).

252 Ann Cavoukian & Don Tapscott, *Who Knows: Safeguarding your Privacy in a Networked World,* at 90 (Random House of Canada 1995).

253 Richard S. Murphy, Property Rights in Personal Information: An Economic Defence of Privacy, 84 *Georgetown Law Journal* 2381–2417 (July, 1996), at 2406.

> all values that are deeply ingrained in our culture, law, and politics. In the case of the presumption of privacy, the burden should be on others to say why they have any right to know about our lives. Absent that, the presumption should be that each of us has control over such information. In practical terms that means that we should not be required to *opt-out* of a system that invades our privacy; the presumption of privacy would dictate that no one is allowed onto our zone of privacy without our specific choice to *opt-in*.[254]

Eugene Volokh made a free speech cautionary argument. He ignored the fact that free speech was not unlimited and not a legal standard in all countries. He did agree that personal information privacy protection was viable under contract law.[255]

For the contract model to have legal influence, the issue of data ownership is essential. The Liberty Alliance, using the EU Model, makes a cautious ownership declaration. The Liberty Alliance conference[256] evaluates the issue of who owns information privacy – personal data. The following chart summaries the Alliances' Personally Identifiable Information (PII) findings.

Table 2.0 PII Ownership[257]

Term	Description
Data subject	The person or entity *referred to* by some data. In the case of PII, the data subject is more or less identified by that data; in the case of transaction records, the data itself may not identify the data subject but may provide a log of historical activity that records behavior. Used in conjunction

[254] Charles J. Sykes, *The End of Privacy: Personal Rights in the Surveillance Society*, at 246 (St. Martin's Press 1999).

[255] Eugene Volokh, Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People From Speaking About You, 52 *Stanford Law Review* 5, 1049 (2000), at 1073.

[256] Liberty Alliance, *Privacy summit*. (2007), at www.projectliberty.org/ liberty/ content/ download/ 3114/ 20838/ file/ Privacy-Summit-Final.pdf (last visited on 9 July 2012), at 5. The Alliance is an organization of 30 organizations and businesses that addresses information concerns.

[257] *Ibid.*

	with PII, the behavior could be ascribed to a specific entity.
Data 'owner'	This reflects the concept that a data subject may have some kind of right (perhaps a statutory one) to know what data someone else has about them. Thus, although someone else has the data, the data subject might be said to have some degree of *ownership* of it.
Data controller	A legally defined role expressed in the EU Data Protection Directive; the person who determines how and why personal data are to be processed.
Data custodian	A legally defined role providing for the controlled disclosure of PII through a form of *trusted proxy*. For instance, in Germany a company could be legally prohibited from disclosing the PII of its employees, but might legally do so by entrusting the disclosure mechanisms to an independent *data custodian* within the organization. This could serve as a good example of privacy protection through a combination of legal, policy and structural measures.

Critics of the model suggested that seeing privacy as only a contractual issue would side-step constitutional principles. The critics made a logical error in that not all countries had the same constitutional arguments. In fact, SA had a much stronger privacy protection in their current constitution than other countries in the study. The critics suggested that each model was independent and that the issues were a zero-sum game. This was not the case. The principles of each model could be integrated, especially if a data protection and information privacy ombudsman was involved in the regulation of the problems.

When information privacy was subjected to contract law, each party's rights and responsibilities were defined and even negotiated. A privacy contract would establish clear obligations on the use, trade, or sale of the data. The contractual default was one of a presumption of privacy. The burden of establishing the right to know was on the government or business that wanted the data. The default for all data sharing should be an *opt-in* based on reliable information.[258] Such an *opt-in* default position empowers individuals to deal with larger, more powerful organizations. The opt-out model rejects the scientific data on people's neuropsychological programming.

[258] Charles J. Sykes, *The End of Privacy: Personal Rights in the Surveillance Society*, at 246 (St. Martin's Press 1999).

Business and marketing firms did not like an *opt-in* standard because when given a full choice, most people did not *opt-in*. Such organizations wanted to take advantage of healthy people's neurologically based decision-making processes that prefer *not to decide*. Such organizations were exploiting a known human defect to increase profits.

Anne Branscomb described the increased value of personal information. She showed that information that was historically considered worthless became valuable. New conflicts, issues, and tensions evolved because businesses want to take control and make profits while ignoring and rejecting data subjects' interests.[259]

Richard Spinello made it very clear that "when a consumer provides personal information, he or she does not assign to that vendor a right to use the information for other purposes."[260] David Barron made it clear that data collected for one purpose could be used for another without checks, balances, regulation, or recourse.[261]

Agreement, confidentiality, due process, and privacy legal principles must apply to all data protection and information privacy recordkeeping systems. These principles must consider whenever an information privacy contract is formed. That the collection and use of personal information required a contract was clearly affirmed through standard contacting principles. A valid offer, acceptance, consideration,[262] intent to be bound, specific terms, and performance should be required.

---

259 Anne Wells Branscomb, *Who Owns Information? From Privacy to Public Access*, at 3 (Basic Books 1994).

260 Richard A. Spinello, *Ethical Aspects of Information Technology*, at 118 (Prentice Hall 1995).

261 David W Barron, *People, Not Computers*, in *Privacy*, at 321 (J. B. Young ed. John Wiley & Sons 1978).

262 Consideration is not required unde SA law.

2.7.3 Information and Knowledge Control Law

In addition to considering asset protection standards and contract law issues, there is considerable research in the field on information and knowledge control law issues; the following provides a summary of this research.

Whalen v. Roe[263] established a new contextual definition of information privacy law. The US court established that people had a declared right to avoid the disclosure of personal matters – in other words, they had a right to control over their information. The right included the process of accessing and even analyzing personal information. Information control had evolved into a duty of data holders to respect the person's confidentiality. In *Whalen*, Justice Stevens declared that "The right to collect and use (data) for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures … (I)n some circumstances that duty arguably has its roots in the Constitution."[264] For example in one case the police had access to computer databases that stored confidential patient data.

Justice Stevens further wrote that privacy cases actually had different interests. "One is the individual interest in avoiding disclosure of personal matters, and another is the interest in independence in making certain kinds of important decisions."[265] The case applied the Fourteenth Amendment, thus the court must balance the interest in collecting the information and any infringement on the privacy right. Intermediate scrutiny rather than the principles of strict scrutiny was applied.[266] The highest level of protection applied to medical information related to sex and essential corporate information. General medical and financial data involved mid-level protection.

---

263 *Whalen v. Roe,* 429 U.S. 589, (1977), at 600. (US)

264 *Id.* at 605.

265 *Id.* at 598-600.

266 Under US constitutional law, the court can apply three levels of scrutiny. The highest is strict which requires a compelling governmental interest, be narrowly tailored and be the least restrictive approach. The intermediate approach requires an action that furthers an important governmental interest. Rational basis is the lowest standard that reflects a legitimate interest like due process or equal right protection.

Data that was a matter of public record involved the lowest protection. Why some medical and corporation data involve higher protection than individual information remained unclear. This issue needs revisiting. The government's (or data holder's) interest must be established as legitimate, substantial, and compelling.

Neil Richard wrote on the way that the government avoided any judicial or constitutional standards. He noted that the government funded and then purchased data from private-sector firms. The scheme was not considered a state action,[267] but in reality the government outsourced surveillance of citizens with legislative and constitutional immunity.[268] Where entangled interaction existed, then any such behavior would be a state action.[269] An alternative was to make both parties responsible for data protection and information privacy legal protections.

In *Miller v. Taylor*[270] Justice Yates delivered the judgement that was on point. "It is certain every man has a right to keep his own sentiments, if he pleases. He has certainly a right to judge whether he will make them public, or commit them only to the sight of his friends."

Grant Hammond argued that legally, personal information was not relative or static.[271] The reality was that the issue was protecting personal information from government and business misuse. Mendes identified five types of potential privacy violations: "(1) aggregation (the "unauthorized collection of information" to create profiles of individuals); (2) intrusion (surveillance or tapping of transmissions);

---

267 Under US law, a state action is necessary for addressing the Constitutional rights of individuals.

268 Neil M. Richards, Reconciling Data Privacy and the First Amendment, 52 *UCLA Law Review*, 4, 1149 (2005), at 1158-1159.

269 See *Norwood v Harrison* 413 U.S. 455, (1973); *Burton v. Wilmington Parking Authority,* 365 U.S. 715, (1961). (US)

270 *Miller v. Taylor*, 4 Burr. 2303, 2379, (1769), at 2379. (UK)

271 R.Grant Hammond, The Misappropriation of Commercial Information in the Computer Age, 64 *Canadian Bar Review 2,* 342 (1986), at 352.

(3) misuse; (4) piracy (use authorization, usually for profit); and (5) unauthorized access."[272] The focus of his thesis was on aggregation misuse.

Concerns regarding technology and privacy were not new. In looking at electricity in the nineteenth century, Carolyn Marvin wrote about concerns that the technology threatened the private secrets and public knowledge balance.[273] Subsequent history showed the concerns warranted. On the other side of the debate were those that claimed that new information technology provided advantages to democracy. Such technology provided better access and even networking of interested parties.

The Panel on the 1967 Privacy and Behavior Research Report by the President's Office of Science and Technology addressed the information privacy issue. The conclusion was that "The right to privacy is the right of the individual to decide for himselve how much he will share with others his thoughts, his feelings, and the facts of his personal life."[274]

The concept of privacy as the right to be left alone was not just based on Warren and Brandeis.[275] The concept was a reference to McIntrye Colley's Treatise on the Law of Torts.[276]

Ithiel Pool argued that "electronic technology is conducive to freedom …it is not computers but policy (law) that threatens freedom."[277] Hope can be found in communication advances, individual rights, and pluralism.[278]

---

272 M. Mendes, *Privacy and Computer-Based Information Systems*, in *Issues in New Information Technology* (Benjamin M. Compaine ed., Ablex Publishing 1988), at 193-264.

273 Carolyn Marvin, *When Old Technologies Were New: Thinking About Electric Communication in the Late Eighteenth Century*, at 64 (Oxford University Press 1988).

274 Executive Office of the President - Office of Science and Technology, *Privacy and Behavioral Research* (Government Printing Office 1967), at 8.

275 Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, 4 *Harvard Law Review,* 5, 193 (1890).

276 Thomas Mcintyre Cooley, *Treatise of the Law of Torts: Or the Wrongs Which Arise Independent of Contract* (Callaghan 1888).

277 Ithiel De Sola Pool, *Technologies of Freedom: On Free Speech in an Electronic Age* (Harvard University Press 1983).

278 *Id.* at 251.

In *US Department of Defense v. Federal Labor Relations Authority*, Justice Thomas wrote for the majority in the case involving the Federal Freedom of Information Act. Thomas argued that just because information may be made publically available, it does not mean that a person does not have a legal right to control dissemination of the information.[279]

Pricilla Regan defined privacy as a collective, not just an individual value. The value was based on the economic view of collective and public goods. One can not benefit from a collective good without others benefiting.[280] Free riders, governmental or business, should not use information without legally obtaining consent and paying for it.[281]

Oscar Gandy studied the issues of DPSIP protection. Gandy wrote that "it is in the area of private corporate action that the law is most in need of attention."[282] Powerful business forces had access to the inner halls of governmental power and opposed data protection and information privacy legal standards in the private sector. Arguments in opposition of data protection included the alleged sanctity of commercial marketplace freedom, free commercial speech, and freedom from governmental restrictions. However, governmental regulations and restrictions exist for other social values and legal principles - some of which are related to privacy. Violations should be subject to the legal principles of strict liability and the burden of proof should be placed on the defendant(s).

Without competent DPSIP laws and regulations, business organizations and marketers would draw their own boundaries. The boundaries were self-serving and

---

279 *U. S. Department of Defense v. Federal Labor Relations Authority*, 114 S.Ct. 1006, (1994), at 1015. Thomas generally supports business, then government, and rarely individual rights. (US)

280 Pricilla M. Regan, *Legislating Privacy: Technology, Social Values, and Public Policy* (University of North Carolina Press 1995), at 227.

281 *Id.* at 228.

282 Oscar H. Gandy, *The Panoptic Sort: A Political Economy of Personal Information*, at 178 (Westview Press 1993).

ignored privacy concerns with the exception of trade secrets. L. Graham Smith[283] showed that business organizations did not take a proactive stance and only dealt with privacy concerns when confronted with organizational risks or threats. Those few organizations that showed some concern about the issues, relied on self-regulation, which lacked any systematic approach or consistency. The codes provided inadequate coverage, consumer awareness, and sanctions.[284]

Alan Vickery argued for information privacy and tort reform, based on breach of confidence. The tort violation included all "un-consented, unprivileged disclosure to a third party of nonpublic information that the defendant has learned within a confidential relationship."[285] Contract and fiduciary legal principles were the basis for this UK tort.[286] The purpose was to compensate those whose information was breached and experienced damage to reputation and some emotional distress. A very limited public's-right-to-know privilege existed, but enforcement and clarification needed to be stronger.

Susan Gerety proposed an information privacy definition based on information control. "Privacy will be defined here as an autonomy or control over the intimacies of personal identity."[287]

When an employer released employee Social Security Numbers (SSN) to a third party, the Ohio Supreme Court ruled that the release violated information privacy legal standards. The court in *Beacon Journal Publishing v. Akron* ruled that:

> Thanks to the abundance of data bases in the private sector that include the SSNs of persons listed in their files, an intruder using an SSN can

---

283 L. Graham Smith, *Impact Assessment and Sustainable Resource Management* (Longman Scientific and Technical 1993).

284 Ann Cavoukian & Don Tapscott, *Who Knows: Safeguarding Your Privacy in a Networked World* (Random House of Canada 1995).

285 Alan B. Vickery, Breach of Confidence: An Emerging Tort, 82 *Columbia Law Review* 1426 (November, 1982), at 1455.

286 Susan M. Gilles, Promises Betrayed: Breach of Confidence as a Remedy for Invasion of Privacy, 43 *Buffalo Law Review,* 1 (Spring, 1995).

287 Tom Gerety, Redefining Privacy, 12 *Harvard Civil Rights–Civil Liberties Law Review* 2, 233 (1977), at 236.

> quietly discover the intimate details of a victim's personal life without the victim ever knowing of the intrusion.[288]

Business practices that used covert data collection, matching, and profiling, without the person's consent was found unlawful. The marketplace of ideas theory did not apply to private data.

As early as 1941, Zechariah Chafee argued that information privacy was a significant social value similar to free speech. The value was so important that only critical national needs should be a legal balance. The harm or damages were not just individual but related to the social value of data protection and information privacy.[289]

Alan Westin advocated the need for individuals to have control over their personal information. He argued that free societies recognize a personal information privacy right. Only extraordinary exceptions should trump this right.[290]

Gary Melton argued that information privacy involved the "maintenance of active decisional control over the disclosure of personal information contained in documents or known by other parties."[291] The law must provide "protection from nonconsensual examination of such information."[292]

DPSIP principles have been violated and the person(s) involved were damaged by a number of events. David O'Brien argued that causal and interpretive access compromises privacy.[293] O'Brien also argued that the law should provide "limitations on the accumulation and disclosure of information

---

288 70 Ohio St. 3d 605, (1994), at 611. (US)

289 Zechariah Chafee, *Free Speech in the United States* (Harvard University Press 1941).

290 Alan Westin, *Privacy and Freedom*, at 42 (Atheneum 1967).

291 Gary B. Melton, Minors and Privacy: Are Legal and Psychological Concepts Compatible? 62 *Nebraska Law Review,* 455 (1983), at 459.

292 *Ibid.*

293 David M. O'brien, *Privacy, Law, and Public Policy,* at 18 (Praeger 1979).

about an individual … In most situations, privacy is valuable."[294]

William Parent maintained that information privacy was "the condition of not having undocumented personal information about oneself known by others."[295] Such information did not belong in the public domain. Parent showed that "privacy is control over when and by whom the various parts of us can be sensed by others."[296]

Bruce Schneier made a strong case that security and privacy are not opposites. These legal and policy issues are not a zero-sum game. Police states provide security but there are no major immigration trends to those states.[297] He further explained that the two must work together.[298] Anti-privacy security tactics do not significantly improve security and often do harm. Government claims for security are wrong or address fake cases.[299] The issue is one of a false dichotomy based on fear. The reality is that "There is no security without privacy. And liberty requires both security and privacy."[300] Data mining efforts were secret and had no legal controls.

The issue was not one of individual rights against the great communal good but one of maintaining everyone's freedom from interference and governmental – business control. Everyone, including the body incarnate, had the right to structure the terms on the use of personal information held by third parties. The principle should apply to governmental and business parties.

---

294 *Ibid.*

295 William A. Parent, A New Definition of Privacy for the Law, 2 *Law and Philosophy* 3, 305 (1983), at 306.

296 *Id.* at 281.

297 Bruce Schneier, *What Our Top Spy Doesn't Get: Security and Privacy Aren't Opposites* (2008, January 24), http://www.wired.com/politics/security/commentary/securitymatters/2008/01/securitymatters_0124?currentPage=all (last visited on 24 January 2012), at 4.

298 *Id.* at 6.

299 *Id.* at 8.

300 *Id.* at 12.

Colin Bennett and Rebecca Grant argued that privacy was a fundamental right to retreat.[301] A second issue was "the right to control information about oneself, even after divulging it to others."[302] Jean Camp agreed that people had a right to control their information.[303] Research conducted by Cathy Goodwin indicated that people were concerned about the collection of personal information and its secondary use.[304]

Anita Allen identified a couple of market failures associated with information privacy law based on personal control over the information. Many people shared personal information with little knowledge or awareness of the consequences. Thus, information privacy laws must include an informed consent requirement prior to third parties doing anything with the data. Significant constraints must be on governments and business organizations that used data mining or shared data without meaningful informed consent. Individuals did not have the resources to track the uses of their personal data. Information privacy law must re-allocate economic structures, relationships, power, and social structures.[305]

Businesses take personal information claiming that it has no value and works against legal personal privacy control protections. Yet, when the same businesses use the information for profit, the businesses claim that the information has economic value and demand protection of business privacy and secrets. The businesses do not pay any type of asset taxes on the data.

---

301 Colin J. Bennett & Rebecca Grant, *Visions of Privacy: Policy Choice for the Digital Age*, at 101 (University of Toronto Press 1999).

302 *Ibid.*

303 L. Jean Camp, Web Security and Privacy: An American Perspective, 15 *The Information Society* 4, 249 (1999).

304 Cathy Goodwin, Privacy: Recognition of a Consumer Right, 10 *Journal of Public Policy and Marketing* 1, 149 (1991, Spring).

305 Anita L Allen, Privacy as Data Control: Conceptual, Practical, and Moral Limits of the Paradigm, 32 *Connecticut Law Review* 3, 861 (2000); Anita L. Allen, *Privacy in American Law*, In *Privacies: Philosophical Evaluations* (Beate Rossler ed., Stanford University Press 2004).

After carefully reviewing a hundred years of privacy law, Ken Gromley found four major concepts and needs for protection. The concepts include privacy as (1) "An expression of one's personality or personhood, focusing upon the right of the individual to define his or her essence as a human being." (2) Linked to "autonomy - the moral freedom of the individual to engage in his or her own thoughts, actions, and decisions" (3) "Citizens' ability to regulate information about themselves," and (4) a "mix-and-match approach" of specific issues.[306]

David Richards saw information privacy as essential to the democratic experiment in that it supported self-governing. Having control over personal information is a form of self-government that protects the individual against more powerful forces.[307] Ruth Gavison argued that DPSIP laws help to protect free societies by aiding autonomy, liberty, human relationships, and selfhood.[308] While some argued that public policy and social interests may trump information privacy, the argument ignored the "functions privacy has in our lives."[309]

Sissela Bok made a necessary bifurcation of privacy and secrecy. "Privacy need not hide, and secrecy hides far more than what is private."[310] Privacy is "the condition of being protected from unwanted access by others."[311] Bok maintains that secrecy is "intentional concealment."[312]

Communications Canada examined the issues of informational privacy. The study found that in terms of telecommunications, privacy was "protection against unwanted intrusion that is the right to be left alone and not to be

---

306 Ken Gormley, One Hundred Years of Privacy, 1992 *Wisconsin Law Review*, 1335 (September/October, 1992), at 1337.

307 David A. J. Richards, Liberalism, Public Morality, and Constitutional Law: Prolegomenon to a Theory of the Constitutional Right to Privacy, 51 *Law and Contemporary Problems* 1, 123 (1988), at 138.

308 Ruth Gavison, Privacy and the Limits of Law, 89 *Yale Law Journal* 3, 421 (1980), at 423.

309 *Ibid.*

310 Sissela Bok, *Secrets: On the Ethics of Concealment and Revelation*, at 11 (Pantheon 1982).

311 *Id.* at 10.

312 *Ibid.*

monitored; the ability to control information about oneself and one's activities; the right to remain anonymous."[313]

In the US, collecting personal information practices, starting with the Nixon administration, has increased. Personal information has been obtained by the government without probable cause and a warrant. Such actions were a violation of the Fourth Amendment. The collection of some personal information was actually self-incrimination, under the Fifth Amendment.

Chief Justice William Howard Taft (former President of the US) modified the application of the Fourth Amendment in the 1928 *Olmstead v. United States*[314] case. He changed the Fourth and Fifth Amendments legal analysis. Telephones could be legally wiretapped as there was, in his mind, no search or seizure. The injustice of Taft's *Olmstead* ruling changed with Justice Potter Stewart's writing for the Court in *Katz v. United States.*[315] The case brought forth the concept of privacy away from space, to a self-defined expectation of privacy, the right to decide what to reveal, reasonable expectations, and eventually to information control.

Justice Thurgood Marshall's dissent in *Smith v. Maryland* laid the ground for further privacy rights. He wrote that "Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes.[316]

Oscar Ruebhausen and O. G. Brim[317] addressed information privacy concerns with research studies and technology. They rejected the view that technology was the problem. The law and policy related to information privacy

---

313 Communications Canada, *Telecommunications Privacy Principles*, at 5 (Supply and Services Canada 1992).

314 277 U.S. 438, 478 S. Ct. 564. 66 ALR 376, 72 L.Ed. 944, (1928). (US)

315 389 U.S. 347, 88 S.Ct. 507, 19 L.Ed.2d 576, (1967). (US)

316 442 U.S. 735, (1979), at 749. (US)

317 Oscar M. Ruebhausen & O. G. Brim, Privacy and Behavioral Research, 65 *Columbia Law Review* 1, 1184 (1965).

was the problem.[318] The authors argued that information privacy involved the right to select with whom information would be shared and the timing of information sharing. One has the right to determine "the extent to which his attitudes, beliefs, behavior and opinions are to be shared with or withheld from others."[319]

From this discussion it is clear that DPSIP laws should establish very clear standards. Furthermore, data controllers must recognize asset protection standards. Ownership of personally identifiable data rests with the person to whom the data relates.

2.7.4 Intellectual Property Law Issues

Intellectual property law issues are closely related to information and knowledge control issues. Intellectual property law created legal protections for information created by the use of a person's mind. The law protects the interests of the author of published and unpublished information.[320] The Copyright Act[321] provides the owner an exclusive right to display, distribute, license, perform, or reproduce all of part of his or her work.[322] An exclusive right to license or produce derivatives of the work is also granted by all of the countries studied.[323] Information privacy data, as defined in this work, certainly meets the definition of a work created through one's writings and behavior. The author has the intellectual property right to publish or not. The Geneva World Intellectual Property Organization (WIPO) Copyright Treaty protects such rights internationally for all signatories.[324] The alternative rationale is that a corporation that collects the pre-written data can claim

---

318 *Id.* at 1190.

319 *Id.* at 1189.

320 U.S. Constitution, Article I, Section 8. (US)

321 U.S. Copyright Act amend. 17 U.S.C. §§ 101-810 (1976). (US)

322 *Id.* at 106.

323 *Id.* at 201(d).

324 World Intellectual Property Organization, *WIPO Copyright Treaty* (1996), http://www.wipo.int/treaties/en/ip/wct/trtdocs_wo033.html (last visited on 15 June 2012).

ownership as an intellectual property right. Is the conclusion, therefore that those corporations can claim a property right when the raw material supplier has none?

Just as copyright law preserves the right to access creative works, the intellectual property model is the model of access to self, as seen in Justice Brandeis's dissent in the *Olmstead* case. He wrote the "makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. . . . They conferred, as against the government, the right to be let alone the most comprehensive of rights and the right most valued by civilized men."[325] The self included beliefs, bodily fluids, body, intellect, personality, and thoughts. From a sociological perspective, Stephen Nock proclaimed that information privacy is a "socially-recognized legitimate right to restrict others from observing or knowing about one's actions."[326] DPSIP law has an intellectual property law dimension that needs to be considered.

Whether by intent, design, or regulatory ignorance, intellectual property law has become a major force negating some DPSIP legal principles. Granting anti-privacy intellectual property protections gave intellectual property owners considerable legal power and protection. The intellectual property codes do not require any type of environmental or technological impact study prior to granting a patent or copyright. Because of this failure, to stay current with regulatory standards in other fields, legal protections as applied to technology or software that violate privacy rights need to be re-considered. Two major problems developed. Software patent protections started, despite a long history against awarding protections to mathematical formulations and business practices. Second, cookies received legal protection without a sound legal review.

---

325 *Olmstead v. U.S.*, 277 U.S. 438, 478 S. Ct. 564. 66 ALR 376, 72 L.Ed. 944, (1928), at 478. (US)

326 Stephen L. Nock, *The Cost of Privacy, Surveillance and Reputation in America*, at 11-12 (Transaction Publishers 1993).

Sissela Bok[327] advanced another intellectual property position. She maintained that information privacy protects one from unwanted access. The law needed to protect one from attention, personal information, or physical access. In *Whalen v Roe*[328] the Court found a constitutionally protected right to control over personal information.

Online profiling by governments, businesses, and Internet Service Providers (ISP) was a reality. ISPs did not ask user's permission to collect, store, share, or sell personal information. Collection included the source and activity of on-line sessions. Firms attached cookies and stored files to the users' computers. Advocates of the ill-gotten information argued that the system helps consumers through on-line profiling of assumed interests. Yet, the data was collected through clandestine maneuvers and those that may attempt to opt-out (not participate) are denied access to the site. A classic example was Microsoft. The National Advertising Initiative suggested guidelines but adherence to the guidelines was voluntary and self-regulating.[329]

Evolving technologies were developed, used, and planned with no legal accountability. Many of the technologies that were developed threatened expansive data protection and security violation problems that governments had not shown a significant interest in preventing or regulating. Examples included the following examples.

Developments in biotechnology raised significant DPSIP concerns. Biotechnology includes biochemical, genetic, and molecular biology records and data based on human tissue samples. Great financial benefits have gone to those developing new technologies, but the developers have been allowed to ignore impact, ownership, and privacy concerns. The advances in this area

---

327 Sissela Bok, *Secrets: On the Ethics of Concealment and Revelation* (Pantheon 1982).

328 429 U.S. 589, (1977). (US)

329 National Advertising Initiative, *Helping You Protect Your Privacy Online* (2009), http://www.networkadvertising.org/ (last visited on 16 August 2012); Michael D. Birnhack, The EU Data Protection Directive: An Engine of a Global Regime, 24 *Computer Law & Security Report* 6, 508 (2008).

are leading to personalized medicine (PM) which determines treatment based on genetics. The question is how is the data gathered, stored, and transferred? Corporations, governments, insurance companies, and employers can misuse biotechnology data, despite a finding that there was a breach of informed consent, fiduciary duties, and ownership rights. The California Supreme Court refused to grant Moore relief in *Moore v Regents of the University of California.*[330] Biotechnology data was collected from Moore without his consent. The samples were used in researches that lead to new treatments that the University patented. No DPSIP impact study was done prior to granting intellectual property (IP) protections. Thus, the awarding of IP protections to the University without a privacy impact audit creates more problems because it limits the movement by developers to privacy by design. Moore's DNA was essentially stolen, the University benefited, and Moore had no recourse.

Global Positioning Systems (GPS) which used satellite systems to monitor radio beacons were another example. The most developed at the time of this thesis was the US system, which used forty satellites that circled the globe twice a day. Similar systems were under development in China, the EU, India, Russia, and Sweden. The entire continent of Africa was covered by these systems.[331]

GPS units were very small and helped people to navigate while driving or walking. The units identified latitude, longitude, and altitude for military and personal uses. Attached devises included cars, cellular telephones, and other electronics. When combined with other databases, the system could track individuals and movements without warrants or legal protections. Most users thought that the system was one way, but it was not. GPS also monitored the user. There were no legal privacy protections of the storage or use of the

---

330 793 P.2d 479 (Cal. 1990). (US)

331 GPS World, *Wayfinder Expands Coverage to Southeast Asia, Africa* (2008, January 23), http://lbs.gpsworld.com/gpslbs/LBS+News/Wayfinder-Expands-Coverage-to-Southeast-Asia-Afric/ArticleStandard/Article/detail/486451?contextCategoryId=44174&searchString=countries (last visited on 12 March 2012).

data collected by means of the GPS unites. Intellectual property protections were issued to those operating the GPS systems without a DPSIP impact study.

Another example was keystroke logging or keylogging, which involved hardware, software, or wireless mechanisms that recorded and transmitted computer users' key strokes. A complete record of a user's session was monitored. These keystroke logging approaches collected any type of subject data. A case on point, *United States v. Scarfo*,[332] found that the approach was not a warrant violation under the Fourth Amendment or an unlawful wire communication violation under federal law.

The field of medical informatics provided another example where governments ignored issues of data protection and security violation problems caused by emerging technologies. Medical informatics includes the technological collection, storage, and use of health and medical records. Advocates argued that computerizing health and medical records would save lives and money without doing extensive risk benefit studies. The movement argues for more predictive, personalized, and preemptive treatment. Data protection and security concerns are mentioned, but not fully addressed. Few protections are proposed or legally enforced. Even without full computerization, the evidence showed that employers, governments, and insurance companies misuse medical data. As far back as 2001, twenty-five percent of Fortune 500 companies admitted using DNA testing to eliminate potential employees who might have a possibility for a genetic disease.[333] Moreover, no computer system is totally safe or secure. The US Department of Defense secured a 300 billion dollar, Joint Strike Fighter computer project that was breached.[334] Less expensive health and medical systems are more

---

[332] 180 F. Supp. 2d 572, 576 (D.N.J. 2001). (US)

[333] Aaron P. Stevens, Arresting Crime: Expanding the Scope of DNA Databases in America, 79 *Texas Law Review* 4, 921 (2001).

[334] Siobhan Gorman, et al., *Computer Spies Breach Fighter-Jet Project*, Wall Street Journal (21 April 2009), http://online.wsj.com/article/SB124027491029837401.html (last visited on 21 April 2012).

vulnerable. Data security has not been adequately addressed for computerized health and medical records. Protection and security must be a matter of law.

Radio Frequency Information Devices (RFID), small chips that collect data, identify objects, and transmit information to a reader served as a final example. The chips track movement and location. The data can track purchases and purchasers. Passive RFIDs are not active until read. Active RFIDs transmit data all of the time. At first, RFIDs were limited in transmission areas but the transmission expanded. Some RFIDs could read through water and on metals with a 99.99 percent accuracy rate.[335]

RFIDs can track individual movement by monitoring products worn by the user or products in the user's possession. Some Canadian provinces advocate using RFIDs in driver licenses. The federal government in the US took no action to regulate RFIDs, but several states passed laws limiting RFID use. Intellectual property protections are legally awarded with no data protection, security, or privacy audits. Another self-regulatory set of guidelines suggested that Electronic Product Code (EPC) tags should be capable of being disabled and discarded, and that consumers should have access to the data EPC tags provide.[336] However, those guidelines did not have the force of law.

DPSIP legal issues have an intellectual property law justification. The major problem is that most intellectual property organizations and agencies exist to perpetuate the power and control of major corporations rather than to protect the privacy rights of individuals.

2.7.5 Personal Property Law Issues

---

335 Omni-Id, *Why RFID? The Reliability Problem* (2009), http://www.omni-id.com/technology/ (last visited on 21 April 2012).

336 Eocglobal, *EPCglobal Guidelines on EPC for Consumer Products* (2005), http://www.epcglobalinc.org/public/ppsc_guide/ (last visited on 10 April 2012).

The personal property law model considered privacy as property - like any other ownership right. The following authors advocate for this position.

Richard Murphy proclaimed, "Personal information is in fact, property."[337] Judith Thomson critically evaluated a number of privacy-based cases. She argued that the basis of the problem were a violation of property law and concluded that some cases were a violation of access to the person.[338]

Anne Branscomb argued that information was a commercial asset.[339] As such, private information was a property interest best protected by property law. She wrote that people had a legal right to withhold private information and prevent violations of their right to privacy. New rules were needed to provide checks and balances.[340] One essential issue was who owned the information and what was its value?

Eugene Volokh noted that those that violate DPSIP legal principles were free riders and thieves.[341] Under the property model, with the exception of a lawful warrant, third parties could not share personal information with law enforcement, share personal information without the person's consent, or use such information for direct marketing purposes.

Critics of the model falsely proclaimed that the model required the government to establish a completely new property right in information, which would be difficult to do.[342] Such a view ignored the ease of creating

---

337 Richard S. Murphy, Property Rights in Personal Information: An Economic Defense of Privacy, 84 *Georgetown Law Journal* 2381–2417 (July, 1996), at 2393.

338 Judith Jarvis Thomson, The Right to Privacy, 4 *Philosophy & Public Affairs* 4, 295 (1975).

339 Anne Wells Branscomb, *Property Rights in Information*, *in* Information Technologies And Social Transformation (Bruce R Guile Ed., National Academy Press 1985); Anne Wells Branscomb, *Who Owns Information? From Privacy to Public Access* (Basic Books 1994).

340 *Id.* 1994, at 185.

341 Eugene Volokh, Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People From Speaking About You, 52 *Stanford Law Review* 5, 1049 (2000), at 1074.

342 Andrew J. Mcclurg, A Thousand Words are Worth a Picture: A Privacy Tort Response to Consumer Data Profiling, 98 *Northwestern University Law Review* 1, 63 (2003).

intellectual property rights in words, information, and knowledge that already existed. Critics further argued the fact that individuals often give their personal information for a low transaction cost, so there is no property right in the information. Such a position ignored that the vast majority of people declared in surveys that their personal information was valuable and needed protection. Such a view also ignored that informed consent and a property interest in information privacy had not been the standard, at least in some of the countries in this study.

Richard Posner[343] argued that Warren and Brandeis were right in maintaining that information privacy was a property right but wrong in the assignment of the right. Rather than assigning the right to the owner of the information kept private, it belonged to the person who needed the information. Posner argued that data subjects should have no control.[344] Posner distorted the basic principles of information privacy. He asserted, without documentation or scientific evidence that privacy concerns were used to mislead others.[345] In the past, no other form of property ownership right was transferred to those who might need to use it. The only possible exception might be eminent domain, and even in such cases, the government must tender fair payment for the property confiscated.

Jerry Kang[346] showed that individuals should control their information. To do otherwise would place substantial research and collective action costs on the person. The collector and holder of the information were in a better position to identify and pay for the valuable resource. Richard Murphy agreed.[347]

---

[343] Richard A. Posner, The Economics of Privacy, 71 *The American Economic Review* 2, 405–409 (1981).

[344] Richard A. Posner, *An Economic Theory of Privacy*, in *Philosophical Dimensions of Privacy: An Anthology*, at 337 (Ferdinand Schoeman ed., Cambridge University Press 1984).

[345] Richard A. Posner, The Economics of Privacy, 71 *The American Economic Review* 2, 405–409 (1981), at 406.

[346] B. Jerry Kang, Information Privacy in Cyberspace Transactions, 50 *Stanford Law Review* 4, 1193 (1998).

[347] Richard S. Murphy, Property Rights in Personal Information: An Economic Defense of Privacy, 84 *Georgetown Law Journal* 2381–2417 (July, 1996).

Personal information was a form of property in which the individual held ownership rights. Privacy information was not a collective value but an individual value that placed ownership with the individual.[348] Kattrin Schwartz declared that use of individually owned data required a default opt-in format and obtaining an informed consent.[349]

Information privacy, is in fact, a form of property and subject to property laws.[350] Eugene Volokh[351] established that governments and businesses that collect and trade personal information were freeloaders who used other person's property without compensation or permission. He argued that the law must protect individual data and make individuals equals when dealing with governments and business organizations. Furthermore, the sale, surrender, or trade of personal information and data must be constrained, and users must follow strict legal standards. In Volokh's perspective, information privacy was an inalienable property right that placed restrictions on all of those who hold or use the information. Paul Schwartz also argued that DPSIP law should restrict the use and transfer of personal information.[352] The property right extended to compiled dossiers and discovered knowledge based on the individual's personal information. Schwartz reasoned tht personal property rights extend to facts, information, and knowledge.

In *Folsom v. Marsh*[353] Justice Story explored the issue of information and knowledge control, privacy rights as property, and granting intellectual property rights. The situations he described were current today.

---

348 Kattrin Schartz Byford, Privacy in Cyberspace: Constructing a Model of Privacy for the Electronic Communications Environment, 24 *Rutgers Computer & Technology Law Journal* 1, 1 (1998).

349 Paul M. Schwartz, Property, Privacy, and Personal Data, 117 *Harvard Law Review* 7, 2055 (2004).

350 Richard S. Murphy, Property Rights in Personal Information: An Economic Defense of Privacy, 84 *Georgetown Law Journal* 2381–2417 (July, 1996).

351 Eugene Volokh, Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People From Speaking About You, 52 *Stanford Law Review* 5, 1049 (2000).

352 Paul M. Schwartz, Property, Privacy, and Personal Data, 117 *Harvard Law Review* 7, 2055 (2004), at 2098.

353 *Folsom v. Marsh*, 2 Story 100, 111 (1841). (US) It was held:

Alan Westin argued that the right to control personal information was a property right and due process standards should give protection to such right against private and public violators.[354] Annie Branscomb argued in the same vein that information privacy data is a form of property, including intellectual property, and must have general property protections. The protections included the right to control "accessibility, commerciality, commonality, confidentiality, equity, integrity, interoperability, liability, privacy, publicity, reciprocity, responsibility, and secrecy."[355]

J.T. Johnson suggested that attorneys tend to think of information privacy as property while social scientists think of information privacy as control of information.[356] The reality was that the two models address the same issues. Academic discipline differences should not impede an integrated understanding of DPSIP legal issues. The oft-used deductive reasoning of the law and the inductive reasoning of the social sciences both contributed to understanding the issues and establishing sound laws and public policy. Data protection and information privacy was, at the same time, a claim, concept, condition, construct, interest, right, state, and topic. Sound contributions involved each approach.

A.R. Miller attempted to clarify the two distinctions. Miller argued that information privacy controls were a property right owned by the data subject -

---

> If a holder of a letter: attempts to publish such letter or letters on other occasions, not justifiable, a court of equity will prevent the publication by an injunction, as a breach of private confidence or contract, or of the rights of the author; and *a fortiori*, if he attempts to publish them for profit; for then it is not a mere breach of confidence or contract, but it is a violation of the exclusive copyright of the writer. . . The general property, and the general rights incident to property, belong to the writer, whether the letters are literary compositions, or familiar letters, or details of facts, or letters of business. The general property in the manuscripts remains in the writer and his representatives, as well as the general copyright. A fortiori, third persons, standing in no privity with either party, are not entitled to publish them, to subserve their own private purposes of interest, or curiosity, or passion (p. 111).

354 Alan Westin, *Privacy and Freedom*, at 324 (Atheneum 1967).

355 Anne Wells Branscomb, *Who Owns Information? From Privacy to Public Access*, at 181 (Basic Books 1994).

356 J. T Johnson, The Private I, You, They, 9 *Journal of Mass Media Ethics* 4, 223 (1994), at 226-227.

with all of the constitutional, legal, and theft protections recognized by the property law.[357]

Warren and Brandeis argued the information privacy data was comparable to intellectual property law. The authors thought that privacy was a higher individual property right. Privacy violations damaged the person and the community. They wrote that "the common-law protection enables him to control absolutely the act of publication, and in the exercise of his own discretion, to decide whether there shall be any publication at all.[358]

David Linowes assessed the impact of the Warren and Brandeis article. The work became an international legal and policy standard.[359] At the time, corporations did not have the legal rights of a person. Information was not as valuable as it was in the information economy. The legal fiction of corporate natural entity legal protections was not yet established. The Constitution protected people's rights, not the government or businesses. The people's right to a free press did not mean that corporate owned information or entertainment businesses could do anything that they wanted. Corporations cannot logically claim legal protections for trade secrets and proprietary information while claiming ownership of information privacy data.

2.7.6 Tort Law Issues

Having considered asset protection standards, contract law issues, information and knowledge control law issues, intellectual property law issues, and personal property law issues, the final two sections in this chapter will

---

357 Arthur R Miller, Personal Privacy in the Computer Age: The Challenge of a New Technology in an Information-Oriented Society, 67 *Michigan Law Review* 6, 1089 (1969), at 1224-1225.

358 Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, 4 *Harvard Law Review* 5, 193 (1890), at 197.

359 David F. Linowes, *Privacy in America: Is Your Private Life in the Public Eye?* (University of Illinois Press. 1989), at 12.

consider tort law issues, and privacy law conflicts. Tort law developed in different patterns in the countries studied. In the US, the law protected the privacy of people from appropriation of a person's likeness for gain and intrusions upon one's private affairs, appropriation, false light, public disclosure of private facts, and the right to seclusion, or solitude.[360] One could not disclose private facts about another that might violate these principles. The major problem for privacy violations under tort law was the determination of damages. Other countries in this study took a different approach.

Some saw the historic tort model of privacy as secrecy or third party control. The Daniel Solove[361] model described the issues as a grouping of views that suggested that the individual must take steps to keep private those things so desired. The general assumption was that the public would favor release of all information.

The model was suggested in *Katz v. United States* when the Court stated that constitutional protections did not apply when the person released information; only if one sought to protect the data, and it was protected.[362] Legal and medical privacy rules were an example of the model. The person controlled the information. Critics, like Stephen Henderson, maintained that the major problem with the model was that it treated private data "as an indivisible commodity."[363]

Edward Bloustein argued that, "privacy began its modern history as a tort."[364] Privacy tort law began with the publication of an article written by Warren and

---

360 American Law Institute, *Restatement of the Law, Second, Torts*, at § 652B-C (The American Law Institute 1977).

361 Daniel J. Solove, et al., *Privacy, Information, and Technology* (2nd ed., Aspen Publishers 2006).

362 *Katz v. United States*, 389 U.S. 347, 88 S.Ct. 507, 19 L.Ed.2d 576, (1967), at 351. (US)

363 Stephen E Henderson, Nothing New Under the Sun? A Technologically Rational Doctrine of Fourth Amendment Search, 56 *Mercer Law Review* 507, 524 (2005), at 546.

364 Edward J. Bloustein, Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser, 39 *New York University Law Review* 962, 985 (1964), at 963.

Brandeis. The work advocated protections against unwanted publication of personal information while protecting the "products and processes of the mind"[365] and protected one's "inviolate personality."[366] The authors argued that "political, social and economic changes entail recognition of new rights and the common law... grows to meet the demands of society."[367] Warren and Brandeis argued that privacy rights required "protection, without the interposition of the legislature"[368]

In *Melvin v. Reid*,[369] the California court protected the privacy of Melvin. A movie had been made of her life prior to the movie and used her real name. The court found that the advertisements and movie violated her privacy.

The American Law Institute's *First Restatement of Tort Law* defined the tort of interference with privacy in the following words: "A person who unreasonably and seriously interferes with another's interest in not having his affairs known to others or his likeness exhibited to the public is liable to the other."[370] The "interest appears only in a comparatively highly developed society."[371]

The American Law Institute's *Second Restatement of Tort Law* identified the major areas of privacy related to tort law. The first was intrusion upon seclusion.[372] The second was false light.[373] The third was public disclosure of private facts.[374] The fourth was appropriation.[375] Prosser provided problematic examples of each. Invasion of seclusion and private affairs must

---

365 Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, 4 *Harvard Law Review,* 5, 193 (1890), at 194.

366 *Id.* at 192.

367 *Id.* at 193.

368 *Id.* at 195.

369 *Melvin v. Reid*, 112 Cal. App. 285, (1931). (US)

370 American Law Institute, *Restatement of the Law, Torts*. Ch. 42, Sec. 867, at 398 (American Law Institute 1939).

371 *Id.* at 398-399.

372 American Law Institute, *Restatement of the Law, Second, Torts* (The American Law Institute 1977), at § 652B.

373 *Id.* at § 653E.

374 *Encyclopaedia Britannica Id.* at § 652D.

375 *Id.* at § 653C

be “highly offensive to a reasonable person.” False light must also meet the same measure. Public disclosure of private facts must meet the first test plus there must not be a matter of public concern. Appropriation allowed litigation when the use of one’s name or likeness resulted in a benefit to the defendant. Information privacy as a matter of information or knowledge control was a basis for privacy litigation.

Edward Bloustein criticized the reductionism of the Prosser argument. However, the point was that information privacy was not just an isolated individual issue. Blousten declared that most of the populace held to the right to determine "to what extent thoughts, sentiments, emotions shall be communicated to others."[376]

William Parent argued that information privacy violations could be classified into two different groups. The list included gratuitous and indiscriminate violations. The list included:

1. Those that served no legitimate purpose, being simply products of idle curiosity or malicious pranksters (gratuitous);
2. Those that were unnecessary in that less intrusive means of obtaining the needed information were available (gratuitous);
3. Those that were arbitrary and capricious (gratuitous);
4. Those that acquired information that was not relevant to the justifying purpose involved (indiscriminate);
5. Those that were carried out in such a way so persons with no business knowing the personal facts acquired were permitted cognitive access to them (indiscriminate).[377]

Parent also suggested some safeguards to prevent unlawful information privacy violations. The list included:

---

[376] Edward J. Bloustein, Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser, 39 *New York University Law Review,* 962 (1964), at 969.

[377] William A. Parent, A New Definition of Privacy for the Law, 2 *Law and Philosophy* 3, 305 (1983), at 310.

1. There must be a valid or legitimate need for invading the privacy.
2. There must be probable cause to believe that the information sought is relevant to the justifying need. There must be probable cause to believe that this information (and not some other, irrelevant information) was obtainable by the techniques recommended.
3. There must not be any alternative, less intrusive means available for obtaining the desired information.
4. An impartial judicial officer must issue a warrant particularly describing the place searched and the information sought.
5. There must be restrictions on cognitive access to the information during the times of its acquisition, disclosure, and storage so that only persons entitled to know the facts have them.[378]

Parent defined information privacy as undocumented information. The problem with this model was that once information became public under this definition, the individual had no further rights of information privacy.

Ferdinand Schoeman maintained that there were two important aspects to privacy. The first was "freedom from intrusions by others."[379] The concept protected people from intrusions by governments, businesses, those seeking social control, and others. The second was "freedom for developing a variety of important relationships of varying degrees of intimacy."[380] This second concept allowed for greater expression, through membership in different organizations. The problem was that the second concept tended to increase social pressure for more information. No one entity or power group should have access to all of

---

[378] *Id.* at 311.

[379] Ferdinand David Schoeman, *Privacy and Social Freedom*, at 21 (Cambridge University Press 2008).

[380] *Id.* at 156.

the personal information. Such a position protects people from extensive efforts of social control.

Teeter and LeDuc argued that tort law principles alone, was not enough to gain a full understanding of information privacy law. They argued that judges and legislators ignored the broad DPSIP legal issues.[381]

In *Pavesich v. New England Life Insurance Company*, the State of Georgia Supreme court unanimously ruled on a key privacy appropriation case. The court found that "no one had the right to use someone else's image or name in an advertisement without permission."[382]

William Prosser[383] suggested that three information privacy legal issues to be resolved. The current thesis maintained that a strong balancing test with a set bias toward maintaining information privacy standards should be the order of the day. The first issue was whether being in public negated information privacy rights. Just because a person made a bank deposit in a public bank did not negate the person's right to have financial records held private.

The second was whether information in public records would be private. Some public demands for wanting to know where ex-convicts live would argue for public record transparency. The reality was that the government released and protected data, essentially on a whim. If a news story unlawfully released information, the data was then in the public record. The issue was more complex because some companies could data-mine public records and add additional information that was more private and then sell it to anyone willing to pay. Public record data release should only occur when there is a strong societal need to know and then only to those that can accurately analyze the data. The US military had DNA on every soldier. The data was a public

---

381 Don L. Teeter & Dwight L. Le Duc, *Law of Mass Communications: Freedom and Control of Print and Broadcast Media*, at 250 (7th ed., Foundation Press 1992).

382 *Pavesich v. New England Life Insurance Company*, 122 Ga. 190; 50 S.E. 68; 1905 Ga. LEXIS 156, (1905), at 31. (US)

383 William Lloyd Prosser, Privacy, 48 *California Law Review* 3, 383 (1960).

record in that the public had paid for the information gathering, testing, and storage. Such public records should remain private. Reasonable suspicion and a warrant from a court of competent jurisdiction should be required when privacy rights involved public records.

In *Time v. Hill,*[384] the US Supreme Court ruled that plaintiffs could sue for invasion of privacy when a newspaper made "false reports of matters of public interest."[385] The case centered on a family that was taken hostage and some time later, the newspaper reported false information about what had happened.

The last concern was private information revealed after a long length of time. Some courts have determined that even death does not provide for a breach of confidentiality and privacy. The Warren Commission inquiry into the assassination of US President John F. Kennedy was sealed and even extended. The above noted actions should require a strong societal need to know, limited release, and where applicable, reasonable suspicion and a warrant from a court of competent jurisdiction should apply.

The approaches found in the countries in this study explore different DPSIP strategies. The current analysis provides an analysis of effective approaches, standards, and policies. The largest threat to DPSIP is the lack of consistent enforceable laws and systems that apply to corporations and governments. The comparative analysis documents problems in each of the countries studied. Each of the countries is considered a representative democracy, yet the laws in force do not fully represent the will of the people. The laws and courts often represent the interests of the governments and corporations.

---

[384] 385 US 374, 383, (1967). (US)
[385] *Id.* at 388.

2.7.7 Privacy Law Conflicts

Amitai Etzioni,[386] a sociologist, argued that communities must balance social responsibilities and individual rights. He maintained that limiting privacy rights curtailed governmental control and intrusion. Friends, neighbors, and organizational members could use approbation, censure, and recognition to insure pro-social behavior. Public health and safety trumped informational privacy. Privacy was only one of many rights that had no *a priori* priority over other rights. Social conditions ought to modify information privacy rights. Etzioni made the classic *assumption of belief error*.[387] The issue of data protection and information privacy was not just an individual issue but a societal issue.

Etzioni joined Robert Bellah[388] and Mary Ann Glendon[389] in claiming, without sound evidence, that informational privacy rights had blocked "needed" public policies, chilled common good public policies for fear of litigation, stopped devices and technology innovations, and successfully delayed public actions through the courts. The common good definition suffered from the utilitarian ethical criticism. Who defined the "greatest good for the greatest number" and how were minority rights protected?

Four factors determined if privacy and common good concerns were out of balance. Etzioni[390] suggested that a "well-balanced communitarian society" must use sociological tests.

---

386 Amitai Etzioni, *The Limits of Privacy* (Basic Books 1999).

387 A term coined by the current author in previous sociolegal publications to describe when one assumes that his or her beliefs are in fact factual and historically correct.

388 Robert N. Bellah, et al., *Habits of the Heart: Individualism and Commitment in American Life* (University of California Press 1985).

389 Mary Ann Glendon, *Right Talk: The Impoverishment of Political Discourse* (Free Press 1991).

390 Amitai Etzioni, *The Limits of Privacy*, at 12-13 (Basic Books 1999).

While arguing for public distribution of HIV testing, criminal record publication, national identification cards, medical record release, communication monitoring, and internment of sexual offenders and Aids patients, Etzioni explored another informational privacy danger. He argued that the greatest privacy threat was not just from the government but also from private companies that functioned as privacy merchants. No one was protected from bankers, corporate surveillance, insurance companies, and marketers. The "Big Bucks" of Little Brother were to be feared more than "Big Brother." Recent events in the countries in the study have showed that both are a major danger.

Justice William O. Douglas' dissenting statement in *Osborn* needs a friendly amendment. He wrote: "We are rapidly entering the age of no privacy, where everyone is open to surveillance at all times; where there are no secrets from the government (and data merchants)."[391] We are already there.

Justice Brandeis dissented from the majority who ruled in *Olmstead v. United States* that telephone wire taping without a warrant was not a violation of constitutional protections against illegal search and seizure because there was no search or seizure. Brandeis argued that with the development of the telephone, "subtler and more far-reaching means of invading privacy had become available to the Government."[392] The same holds true for current computer technologies.

---

1. Limits information privacy only if it faces a well-developed and macroscopic threat to the common good, not a merely hypothetical danger.
2. Responding to a tangible and macroscopic danger does not start with resorting to measures that might restrict privacy rights.
3. When privacy-curbing measures must be introduced, the approach must be as minimally intrusive as possible.
4. Measures that treat undesirable side effects of needed privacy-diminishing measures are preferred over those that ignore these effects.
5. When the above four measures are met, there should be increased penalties for privacy violations.

391 *Osborn v. United States*, 385 341, (1966). (US)

392 In Olmstead v. U.S., 277 U.S. 438, 478 S. Ct. 564. 66 ALR 376, 72 L.Ed. 944, (1928), at 438. (US) It was held that:

Having knowledge about an individual's personal information was to have power over that individual. Having knowledge about a near entire population's personal information was to control the population. The holder of the data could control the population's information and strongly influence the decisional privacy of the people.

Paul Schwartz clarified the connection between decisions and information. "Decisional and information privacy are not unrelated; the use, transfer, or processing of personal data by public and private sector organizations will affect the choices that we make."[393] The issues were so important that the US Supreme Court clarified the issues of information privacy in *Whalen v. Roe.*[394] Information privacy was protected by the Fourteenth Amendment. The decision referenced the *Griswold v. Connecticut*[395] case which held that "The First Amendment has a penumbra where privacy is protected from governmental intrusion."[396]

Charles Sykes showed that "By invoking fears of drug cartels, kidnappings, and international terrorism, the FBI has sought the power to be a fly on the wall in the new information age."[397] Jeffrey Rosen further explained that when "intimate information is removed from its original context and revealed to

---

> The evil incident to invasion of the privacy of the telephone is far greater than that involved in tampering with the mails. Whenever a telephone line is tapped, the privacy of the persons at both ends of the line is invaded and all conversations (277 U.S. 476) between them upon any subject, and, although proper, confidential, and privileged, may be overheard. Moreover, the tapping of one man's telephone line involves the tapping of the telephone of every other person he may call or who may call him. As a means of espionage, writs of assistance and general warrants are but puny instruments of tyranny and oppression when compared with wiretapping.

393 Paul M. Schwartz, Property, Privacy, and Personal Data, 117 *Harvard Law Review* 7, 2055 (2004), at 2058.

394 429 U.S. 589, (1977). (US)

395 38 1 U.S. 479, 85 S.Ct. 1678, 14 L.Ed.2d 510, (1965). (US)

396 *Id.* at 483.

397 Charles J. Sykes, *The End of Privacy: Personal Rights in the Surveillance Society*, at 156 (St. Martin's Press 1999).

strangers, we are vulnerable to being misjudged on the basis of our most embarrassing, and therefore most memorable, tastes and preferences."[398]

The National Commission on Terrorist Attacks provided a number of insights and suggestions. Increased surveillance can negatively affect civil rights. "This shift of power and authority to the government calls for an enhanced system of checks and balances to protect the precious liberties that are vital to our way of life."[399] The commission recommended that the President work to protect privacy rights and that the government monitor the protections. Neither recommendation was effectively followed.

Jeffrey Rosen concluded that dataveillance was like general rather than specific warrants. Privacy should be considered first because scanning innocent information to find a sign of guilt was a resource diversion that threatened equality, privacy, and ignored more effective terrorism protections.[400] Such behavior was a violation of the Fourth Amendment but was done during the Nixon era and by subsequent US presidential administrations. In fact, Podesta and Goyle[401] determined that the George W. Bush administration was more extensive in spreading privacy surveillance on domestic citizens than J. Edgar Hoover did during the Nixon years.

Chris Hoofnagle[402] documented that the government did not have to collect all of the information within the existing legal constraints. The government

---

398 Jeffrey Rosen, *The Unwanted Gaze: The Destruction of Privacy in America*, at 9. (Random House 2000).

399 National Commission On Terrorist Attacks Upon The United States, *Final Report of the National Commission on Terrorist Attacks upon the United States, the 9/11 Commission Report 394* (Authorized 1st ed.) (Government Printing Office 2004), at 394.

400 Jeffrey Rosen, *The Naked Crowd: Reclaiming Security and Freedom in an Anxious Age*, at 24 (Random House 2004).

401 John D. Podesta & Raj Goyle, Lost in Cyberspace? Finding American Liberties in a Dangerous Digital World, 23 *Yale Law and Policy Review* 2, 509 (2005).

402 Chris Jay Hoofnagle, Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement, 29 *North Carolina Journal of International Law and Commercial Regulation* 4, 595 (2004).

could and did buy data from data aggregators. Such data collection would be illegal for government to directly collect. The data was delivered in any format requested. The research described revealed over 1,500 documents related to companies soliciting government business with aggressive and tailored databases for law enforcement. The list of companies included ChoicePoint, Database Technologies Online, Dun & Bradstreet, Experian, and LexisNexis.

2.8 Summary of the Sociolegal Literature and Issues Reviewed

This Chapter examined the sociolegal justifications for DPSIP legal intervention. Data about and by DPSIP protagonists were addressed. Research, theory, legislation, and court decisions have shown the need for a sound legal approach. The approach drew on literature from the nations involved in the current study, namely AU, CA, SA, the UK, and the US.

Chapter Three changes the focus to historic international legal standards and guidelines. The data drew on legal documents, treaties, conventions, and cases. The data shows that SA and other nations could draw on the collective international perspective when addressing DPSIP legal issues.

CHAPTER THREE: DATA PROTECTION AND SECURITY LAW: INTERNATIONAL LEGAL STANDARDS

> *Instead of a model act or international privacy regulation, the solution will most likely involve a multifaceted approach that will include both international oversight checked by local governance and changes in social institutions. It cannot be a comprehensive initiative, nor can it be left totally to each municipality or state to decide. It will have to have a broad international framework within which local flexibility is allowed and encouraged.* Dan Bustillos[1]

3.0 Overview

As SA develops and other nations evaluate and update DPSIP laws and regulations, an understanding of historic and current international standards provides essential facts and insights. Much of the current flow of information is international. This chapter examines a number of ancient legal documents that address DPSIP-related issues. Modern international treaties[2] are analyzed. The various European Declarations, the Asia-Pacific Economic Cooperation (APEC) Privacy Charter, and relevant African privacy declarations are explored. Selected national and non-governmental organizations' privacy standards are studied. A critique of International DPSIP legal standards is provided. The international literature and issues are summarized and reviewed.

---

[1] Dan Bustillos, *Privacy and Consent Concerns in International Genetic Databanks*. (2005), at http://www.law.uh.edu/healthlaw/perspectives/August2005/(DB)GeneticDatabanks.pdf (last visited on 7 September 2012), at 3.

[2] Also termed accord; conventions, covenants, declarations, pact, or guidelines. See Bryan A. Garner, *Black's Law Dictionary* (Bryan A. Garner ed., West Group 17 ed. 1990), at 1507. Also termed agreement, mutual understanding, promise, protocol, and stipulation. See William C. Burton, *Legal Thesaurus* (Maxwell Macmillan 2nd ed. 1992), at 966.

3.1 Background

A number of historic codes of behavior and laws present insights into modern DPSIP issues. Some were formal legal codes. Others were international treaties that bound the signatories to accept the principles as a matter of law. A third set was an organizational or national declaration on the proper protection of private information. An understanding of those areas of consensus is an important background to comparing AU, CA, SA, UK, and US DPSIP standards. Principles and concepts that have particular relevance to DPSIP issues are highlighted in bold face font in the discussion below.

3.2 Ancient Codes

The *Code of Hammurabi* establishes a principle for privacy and data protection law responsibilities. Section 53 declared: "If any one be **too lazy to keep his dam in proper condition, and does not so keep it; if then the dam break** and all the fields be flooded, **then shall he in whose dam the break occurred be sold for money, and the money shall replace** the corn which **he has caused to be ruined**."[3] The Code presents a doctrine of responsibility that should apply to businesses and governments that collect and hold personal data because like agricultural land, personal data is an asset and commodity that has value that can be distributed. Such data is personal property that can be misused or stolen.

Section 125 of the *Code of Hammurabi* establishes the principle of liability for lost property, even personal property, entrusted to another.

> If **any one place his property with another for safe keeping**, and there, either through thieves or robbers, his property and the property of the other man be lost, **the owner of the house, through whose**

[3] Code of Hammurabi, *Code of Hammurabi*. (1780 BCE), at http://www.fordham.edu/halsall/ancient/hamcode.html (last visited on 24 September 2012), at 53. (emphasis added)

> **neglect the loss took place**, shall compensate the owner for all that was given to him in charge.[4]

Data subjects have a reasonable expectation that data controllers will protect their property.

The classic *Hippocratic Oath*, which has historically been taken by physicians, specifically refers to privacy and data protection concepts. "**What I may see or hear in the course of the treatment or even outside of the treatment in regard to the life of men**, which on no account one must spread abroad, **I will keep to myself, holding such things shameful to be spoken about.**"[5] While the oath was and is sworn by physicians, the principle of confidentiality applies to many business and governmental DPSIP activities. The concept is also the basis for trade secret laws.

The maxim of the *Code of Justinian*, established in the Roman Empire during the 6th century A.D. is to "live honestly, **to hurt no one, to give every one his due.**"[6] This code also addresses the issue of ownership of property. Part 1, Divisions of Things, declares: "But **things sold and delivered are not acquired by the buyer until he has paid the seller the price, or satisfied him in some way** or other, as by procuring some one to be security, or by giving a pledge."[7] The Justinian code shows that possession of another's data does not constitute ownership. Any transfer of ownership must be clear and involve compensation.

Part XIV, entitled Other Ways of Contracting an *Obligatio*, addresses the principle behind the obligation to protect any personal data collected. The

---

[4] *Id*. at § 125. (emphasis added)

[5] Hippocrates, *The Classical Hippocratic Oath*. (2005), at http://www.mnsu.edu/emuseum/prehistory/aegean/culture/greekmedicine.html (last visited on 20 August 2012). at 7. (emphasis added)

[6] Code of Justinian, *Codex Justinianus*. (529), at http://www.fordham.edu/halsall/basis/535institutes.html (last visited on 26 September 2012). (emphasis added)

[7] *Id*. at § 41. (emphasis added)

Code declares the following: "But he who has **received a thing lent** for his use, is indeed **bound to employ his utmost diligence in keeping and preserving it;** nor will it suffice that he **should take the same care of it, which he was accustomed to take of his own property**."[8]

Book IV, entitled Obligations Arising from *Delicta* (acts that fall short of some approved standard of conduct), addresses the holder's misuse of property and recognizes that the owner of property has the power to determine its use. The Section reads: "**It is theft, not only when anyone takes away a thing belonging to another, in order to appropriate it, but generally when anyone deals with the property of another contrary to the wishes of its owner**."[9] Personal data is often appropriated and misused without informed consent.

These ancient codes no longer have legal power except as persuasive authority. However, the principles noted in the codes do relate to some current DPSIP legal issues of ownership and data collectors' responsibilities.

3.3 Modern International Treaties

Additional persuasive authority and some binding legal authority can be found in modern international treaties and declarations that address civil and human rights related to DPSIP legal responses. Signatories are bound to comply with the documents, and the treaties set a general standard for businesses and governments.

---

[8] *Id.* at § 2. (emphasis added)

[9] *Id*. at § 6. (emphasis added)

3.3.1 The Universal Declaration of Human Rights

The *Universal Declaration of Human Rights*[10] declares a number of DPSIP related principles. The declaration is the cornerstone of all modern privacy protections. Article 12 of the declaration makes the following proclamation:

> No one shall be subjected to arbitrary interference with his **privacy, *family, home or correspondence,*** nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks.

Moreover, Article 12 makes two relevant proclamations:

1. ***"Everyone has the right to own property alone as well as in association with others."***
2. ***"No one shall be arbitrarily deprived of*** **his property."**

The Declaration is not a legally binding treaty but originally was a General Assembly resolution. Over time, however, the declaration reached the status of international customary legal standards binding on all member states. While the declaration clearly establishes privacy and related property rights as a human right, seeking redress is difficult if not impossible.

3.3.2 American Declaration of the Rights and Duties of Man

The Organization of American States (OAS) is one of a number of regional alliances the US helped to form after the Second World War. In 1948, the OAS passed the *American Declaration of the Rights and Duties of Man*. Article 5 declares that, "Every person has the **right to the protection of the law against abusive attacks upon** his honor, his reputation, and **his private**

---

[10] United Nations, *Universal Declaration of Human Rights* (1948), at http://www.hrweb.org/legal/udhr.html (last visited on 20 August 2012). (emphasis added)

and family life." Article 9 declares, "Every person has the right to the **inviolability of his home**." Article 10 declares, "Every person has the **right to the inviolability and transmission of his correspondence**."[11] The Declaration recognizes a privacy right, including the right to have boundaries and privacy in one's correspondence. The right to privacy in one's correspondence, family, and home life is echoed in a number of other declarations as noted below and is the basis for the right to data protection, data security, and information privacy.

Article 11 of the *American Convention on Human Rights* addresses the Right to Privacy. The article makes the following declarations:

1. Everyone has the right to have his honor respected and his dignity recognized.
2. No one may be the object of **arbitrary or abusive interference with his private life**, his family, his home, or his correspondence, or of unlawful attacks on his honor or reputation.
3. Everyone has the **right to the protection of the law against such interference or attacks**.[12]

The Convention permits cases only when there are state parties. If two states are involved, both must agree to the same jurisdiction. Despite its role in creating the organization, the US never ratified the agreement.

In May of 1948, the newly organized Organization of American States (OAS) established the declaration of rights and duties of man. In 1979, the OAS agreement created the Inter-American Court of Human Rights and the Inter-American Commission on Human Rights. The Inter-American Court of Human Rights ruled that the Declaration "defines the human rights referred to

---

[11] Organization of American States, *American Declaration of the Rights and Duties of Man*. (1948), at http://www.oas.org/juridico/english/ga-Res98/Eres1591.htm (last visited on 10 June 2012). (emphasis added)

[12] Organization of American States, *American Convention on Human Rights*. (1969), at http://www.hrcr.org/docs/American_Convention/oashr.html (last visited on 10 June 2012), at § 11. (emphasis added)

in the Charter…and is a source of international obligations related to the Charter of the Organization."[13] The Court determined that the declaration is a source on international obligation. However, the decisions of the Court are not legally binding.

3.3.3 European Convention of Human Rights and Fundamental Freedoms

The *European Convention of Human Rights and Fundamental Freedoms* also addresses the issue of privacy and data protection. Article 8, Section 1, Right to **respect for private** and family life declares, "Everyone has the **right to respect for his private and family life**, his home and **his correspondence**." Section 2 provided a number of exemptions, some of which need mentioning:

> There shall be **no interference by a public authority with the exercise of this right except such as is in accordance with the law** and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.[14]

The European Court of Human Rights enforces the convention. The Court can evaluate individual and inter-state disputes. The decisions are only binding on state parties. The Convention not only provides for a government obligation to respect the right to abstain from intervention but also a positive obligation to protect the rights.

---

[13] Inter-American Court of Human Rights, Advisory Opinion OC-10/89, I-A. Court H.R., Series A: Judgments and Opinions, No. 10, at 45 (1989).

[14] European Convention of Human Rights and Fundamental Freedoms, *European Convention of Human Rights and Fundamental Freedoms*. (1950), at http://conventions.coe.int/treaty/en/Treaties/Html/005.htm (last visited on 24 September 2012). (emphasis added)

3.3.4 International Covenant on Civil and Political Rights

Part Three, Article 17, Section 1 of the *International Covenant on Civil and Political Rights*[15] declares that, "No one shall be subjected to **arbitrary or unlawful interference with his privacy**, family, home or **correspondence**, nor to unlawful attacks on his honor and reputation." Section 2 states that, "**Everyone has the right to the protection of the law against such interference or attacks**." The major flaw of the covenant is that individuals have no clear legal mechanism to enforce privacy rights.

The US ratified the Covenant as a matter of international law. However, the Senate declared that Articles 1 to 26 of the Covenant are not self-executing; thus, the ratification "will not create a private cause of action [in] the US Courts."[16] Supreme Court Justice Sandra Day O'Connor rejected this view. She argues that the Supremacy Clause of the US Constitution gives legal force to treaties and thus full compliance for the Covenant.[17]

Australia also signed the Covenant, but it does not automatically become national law without enabling domestic legislation.[18] The Covenant does have indirect influence in statutory interpretations and common law development.[19]

The Covenant is binding on all member states to promote, protect, and respect the rights, but there is no individual right of action. The EU General Assembly declared that:

---

15 United Nations, *International Covenant on Civil and Political Rights, (ICCPR). Article 17*. (1966), at http://www2.ohchr.org/english/law/ccpr.htm (last visited on 20 August 2012). (emphasis added)

16 United States Senate, *Report on Ratification of the International Covenant on Civil and Political Rights* § Exec. Rep. No. 102-123, 15 (1992).

17 Sandra Day O'Connor, Federalism of Free Nations, 28 *New York University Journal of International Law and Politics* 1-2, 35 (1996). at 42.

18 *Dietrich v The Queen*, 177 CLR 292 at 305, (1992). (AU); *Minister for Immigration and Ethnic Affairs v Teoh*, 183 CLR 273 at 286-305 (1995). (AU)

19 *Ibid*. *Chu Kheng Lim v Minister for Immigration*, 176 CLR 1 at 38, (1992). (AU) Also see Kristen Walker, *Treaties and the Internationalisation of Australian Law in* Courts of Final Jurisdiction: The Mason Court in Australia (Cheryl Saunders ed. Federation Press 1966).

> **Effective measures have to be taken by States to ensure that information concerning a person's private life does not reach the hands of persons who are not authorized by law to receive, process and use it, and is never used for purposes incompatible** with the Covenant. In order to have the most effective protection of his private life, **every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes**. Every individual should also be **able to ascertain which public authorities or private individuals or bodies control or may control their files. If such files contain incorrect personal data or have been collected or processed contrary to the provisions of the law**, every individual should have the **right to request rectification or elimination**.[20]

This is perhaps the modern treaty that most directly addresses data subjects' rights to privacy and control of their personal information as part of a general principle of civil rights.

3.3.5 The Convention on the Rights of the Child

The UN *Convention on the Rights of the Child*, Article 16, states that:

> No child shall be subjected to **arbitrary or unlawful interference with his or her privacy,** family, home **or correspondence**, nor to unlawful attacks on his or her honor and reputation. The child has the right to the protection of the law against such interference or attacks.[21]

Thus, under the principles of the UN Convention, even children have privacy rights.

---

[20] United Nations, *Guidelines Concerning Computerized Personal Data Files. Adopted by the General Assembly on 14 December 1990.* (1990b), at http://ec.europa.eu/justice_home/fsj/privacy/instruments/un_en.htm (last visited on 3 January 2012), at 10. (emphasis added)

[21] United Nations, *Convention on the Rights of the Child. UN General Assembly Document A/RES/44/25*. (1989), at http://www.cirp.org/library/ethics/UN-convention/ (last visited on 20 August 2012). (emphasis added)

3.3.6 International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families

In 1990, the EU adopted a convention regarding migrant workers that addresses privacy issues. Part III, Human Rights of all Migrant Workers and Members of their Families, addresses the issues of migrant worker privacy and property.

> ***Article 14:*** No migrant worker or member of his or her family shall be subjected to **arbitrary or unlawful interference with his or her privacy**, family, home, **correspondence or other communications**, or to unlawful attacks on his or her honor and reputation. Each migrant worker and member of his or her family shall have the **right to the protection of the law against such interference or attacks**.
>
> ***Article 15:*** No migrant worker or member of his or her family shall be arbitrarily **deprived of property**, **whether owned individually or in association with others.** Where, under the legislation in force in the State of employment, the assets of a migrant worker or a member of his or her family are **expropriated in whole or in part**, the person concerned shall have the **right to fair and adequate compensation**.[22]

3.3.7 EU General Assembly Guidelines Concerning Computerized Personal Data Files

In addition to these broader statements affirming individuals' right to privacy, in 1990 the EU General Assembly adopted rules specifically for computerized

---

[22] United Nations, *International Convention on the Protection of the Rights of All Migrant Workers and Members of their Families*. (1990a), at http://www.un.org/documents/ga/res/45/a45r158.htm (last visited on 20 August 2012). (emphasis added)

personal data files.[23] However, the guidelines provide minimal DPSIP direction.

These EU General Assembly guidelines apply to international organizations and provide directions for national legislation. The essential principle is that information collected and stored in computerized data bases should be fair, lawful, and adhere to the UN Charter.

The principle of accuracy suggests that the persons holding the data should ensure that the data is accurate, relevant, and current. The principle of the purpose-specification requires that the purpose must be legitimate, that data be used for the specified purpose, and with the informed consent of the data subject. The data subject must consent to use and disclosure. Time limits on data holdings also apply.

The principle of interested-person access requires that the data holder pay any rectification costs. Those with proof of identity should have access without undue delay or expense. Any data communication involves informing the party. The rule applies to all persons. Compilation of discriminatory data is unlawful. The discriminatory list includes "information on racial or ethnic origin, color, sex life, political opinions, religious, philosophical and other beliefs as well as membership of an association or trade union." Exceptions, with operational standards, include "national security, public order, public health, or morality." Exceptions also include situations involving human rights and fundamental freedom.[24]

The principle of security requires that databases should be secure. The security threats include unauthorized access, destruction, fraudulent misuse, loss, manmade and natural dangers, and IT viruses. The principle of

---

[23] United Nations, *Guidelines Concerning Computerized Personal Data Files. Adopted by the General Assembly on 14 December 1990.* (1990b), at http://ec.europa.eu/justice_home/fsj/privacy/instruments/un_en.htm (last visited on 3 January 2012).

[24] *Id.* at 5, 6, 9.

supervision and sanctions requires the appointment of an independent and impartial privacy authority. Criminal and other penalties should apply. Transborder data flow requires safeguards to protect privacy issues. The guidelines apply to all private and public computerized files.

The guidelines apply only to electronic files but incorporate many of the older OECD guideline principles. The standard sets minimum guarantees on national legislations. One of the most important guarantees is that "**Information about persons should not be collected or processed in unfair or unlawful ways, nor should it be used for ends contrary to the purposes and principles of the Charter of the United Nations**."[25] The document establishes "principles of lawfulness and fairness, accuracy, purpose-specification, interested **person access**, non-discrimination, power to make exceptions, **security, supervision and sanctions, transborder data flows**, and field of application to all public and **private computerized** files."[26]

3.4 European Declarations

There are three significant European DPSIP declarations: the OECD *Guidelines on the Protection of Privacy and Transborder Flow of Personal Data*, the *Council of Europe Convention on Data Protection,* and the *EU Directives on Data Protection.*

3.4.1 OECD Guidelines

The Organization for Economic Co-operation and Development (OECD) was the first group to address information privacy through harmonizing member state laws. In November of 1950, the OECD opened the Protection of Fundamental Rights and Fundamental Freedoms Convention for signature.

---

[25] *Id*. at Principle 1. (emphasis added)

[26] *Id*. at Principles 1-10. (emphasis added)

In September of 1953, the Convention went into effect. The Preamble declares that the members reaffirm:

> [T]heir profound belief in those fundamental freedoms which are the foundation of justice and peace in the world and are best maintained on the one hand by an effective political democracy and on the other by a common understanding and observance of the human rights upon which they depend.[27]

Article 8 declares:

1. **Everyone has the right to respect for his private and family life, his home and his correspondence**.
2. There shall be **no interference by a public authority with the exercise of this right** except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.[28]

The guidelines clearly establish information privacy as a fundamental freedom; however, the exceptions create significant problems in legal accountability. Each exempt category is open to a wide range of operational, political, and self-serving interpretations and definitions. Historically, exception claims have been used for unreasonable violation of basic civil liberty and human rights. For example, since 1990, the UN Human Rights Committee found AU guilty of seventeen violations of basic human rights.[29]

---

[27] Council of Europe, *Convention for the Protection of Human Rights and Fundamental Freedoms*. (1950), at http://conventions.coe.int/treaty/en/Treaties/Html/005.htm (last visited on 20 August 2012), at 1.

[28] *Id.* at 2. (emphasis added)

[29] N.S.W. Council for Civil Liberties, *Does Australia Violate Human Rights?* (2009), at http://www.nswccl.org.au/issues/hr_violations.php (last visited on 1 January 2012).

Japanese and Ukrainian Canadians were subject to internment during the Second World War.[30] A clear example in Europe is the World War II concentration camps and holocaust.[31] Examples in the US include the World War II Japanese internment camps,[32] the 1950s McCarthyism,[33] and the Nixon and Bush–Cheney administrations.[34] Therese Marie Sacco documented some human rights violations in SA.[35]

The exception of the economic well-being of the country is also troublesome. Such decisions are based on corporate power or corporate and governmental policies. Tom Sharman documents how the UK government and UK-based corporations use an economic well-being argument to violate human rights.[36] The economic, political, and policy making power of large corporations is well documented. The oppressive power is domestic and international. The "economic well-being of the country" is often defined as what is in the best interest of the corporation.[37]

---

30 Frederic P. Miller, et al., *Japanese Canadian Internment: World War II, Empire of Japan, Pearl Harbor, Brian Mulroney, Japanese American internment, Ukrainian Canadian internment, run internment camps during World War II* (Alphascript Publishing. 2009).

31 Jacques Delarue, *The Gestapo: A History of Horror* (Mervyn Savill trans., Frontline Books. 2008); Richard Lawrence Miller, *Nazi Justice: Law of the Holocaust* (Praeger. 1995); Ingo Müller, *Hitler's Justice: The Courts of the Third Reich* (Deborah Lucas Schneider trans., Harvard University Press. 1991). Michael Stolleis, *The Law under the Swastika: Studies in Legal History in Nazi Germany* (Thomas Dunlap trans., The University of Chicago Press. 1998).

32 Alan Brinkly, *A Familiar Story: Lessons from Past Assaults on Freedom*, *in* The War on Our Freedoms: Civil Liberties in an Age of Terrorism (Richard C. Leone & Greg Anrig eds., Public Affairs 2003).

33 *Ibid*. and David Cole & James X. Dempsey, *Terrorism and the Constitution: Sacrificing Civil Liberties in the Name of National Security* (The New Press 2nd ed. 2002).

34 Jane Mayer, *The Dark Side: The Inside Story of How the War on Terror Turned into a War on American Ideals.* (Doubleday. 2008).

35 Therese Marie Sacco, Social Exclusion: Experiences of Some of Apartheid's Victims of Human Rights Violations Post The Truth And Reconciliation Commission, *6 IUC Journal of Social Work: Theory and Practice*, 2 (2003).

36 Tom Sharman, *How the UK Government is Enabling the Violation of Human Rights Overseas: ActionAid UK submission to the Universal Periodic Review of the UN Human Rights Council*. (2007), (last visited on 1 January 2012).

37 See Joel Bakan, *The Corporation: The Pathological Pursuit of Profit and Power* (Free Press. 2004); John C. Bogle, *The Battle for the Soul of Capitalism* (Yale University Press. 2005); Lee Drutman & Charlie Cray, *The People's Business: Controlling Corporations and Restoring Democracy* (Berrett-Koehler Publishers, Inc. 2004); Byron L. Dorgan, *Take this Job and Ship It: How Corporate Greed and Brain-Dead Politics are Selling out America* (Thomas Dunne Books / St. Martin Press. 2006).

The Honorable Justice Michael Kirby[38] of the AU Court and Chair of the OECD Expert Group reports that the OECD guidelines are largely obsolete. He argues for new rights, including a right to "not be indexed … to encrypt personal communications … [to] fair treatment in public key infrastructures ... human checking … human checking of adverse automated decisions … beyond the aspiration of the OECD openness principle."[39]

3.4.1.1 Guidelines on the Protection of Privacy and Transborder Flow of Personal Data

On September 23, 1980, the OECD published *The Guidelines on the Protection of Privacy and Transborder Flow of Personal Data*. The transborder guidelines are voluntary. Some basic principles subsequently became law. The US approved the guidelines calling them "benchmark norms for fair information practice."[40]

The OECD Transborder Guidelines apply to all personal data in both the private and public sector.[41] Any exceptions should be at a minimum and known to the public.[42] The guidelines established basic principles, including:

> Paragraph 7. There should be **limits to the collection of personal data** and any such data should be obtained by lawful and fair means and, where appropriate, **with the knowledge or consent of the data**

Greg Farrell, *Corporate Crooks: How Rogue Executives Ripped Off Americans .... and Congress Helped Them Do It!* (Prometheus Books. 2006); and Wade Rowland, *Greed, Inc: Why Corporations Rule Our World* (Arcade Publishing. 2006).

38 Kirby was awarded the 2010 International Privacy Champion prize from the Electronic Privacy Information Center (EPIC). Liz Tay, *Kirby Crowned International Privacy Champion*, SC Magazine for IT Security Professionals. (2010), at http://www.securecomputing.net.au/News/166776,kirby-crowned-international-privacy-champion.aspx (last visited on 9 February 2012).

39 The Hon Justice Michael D Kirby, Privacy in Cyberspace, 21 *University of New South Wales Law Journal,* 2, 323 (1998), at 330.

40 Joel R. Reidenberg, Restoring Americans' Privacy in Electronic Commerce, 14 *Berkeley Technology Law Journal*, 771 (Spring 1999), at 771.

41 OECD, *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*. (1980), at http://www.olis.oecd.org/horizontal/oecdacts.nsf/linkto/C(80)58 (last visited on 22 January 2012), at 2.

42 *Id*. at 4.

> **subject**. 8. Personal data should be **relevant to the purposes for which they are to be used,** and, to the extent necessary for those purposes, should be **accurate, complete and kept up-to-date**. 9. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose. 10. **Personal data should not be disclosed, made available or otherwise used for purposes other than those specified** in accordance with Paragraph 9 except: a) with the **consent of the data subject; or b) by the authority of law**. 11. Personal data should be **protected by reasonable security safeguards** against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data. 12. There should be a **general policy of openness about developments, practices and policies** with respect to personal data. 13. An individual should have the right: a) to **obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;** b) to have communicated to him, data relating to him; i) within a reasonable time; ii) at a charge, if any, that is not excessive; iii) in a reasonable manner; and iv) in a form that is readily intelligible to him; c) to be given reasons if a request made under sub-paragraphs a) and b) is denied, and to be able to challenge such denial; and d) to challenge data relating to him and, if the challenge is successful, **to have the data erased, rectified, completed or amended.**[43]

The OECD requires that collection of personal information should be lawful, fair, and generally performed with the knowledge or consent of the subject. The data must be accurate, complete, necessary, relevant, and kept updated. The data must not be disclosed, made available, or used for any other purpose than that for which it is collected, unless the subject consents or by authority of law. The data must have reasonable security safeguards. The

---

[43] *Id*. at 7–13. (emphasis added)

safeguards should provide protection against all destruction, loss, modification, risks, unauthorized access, use, or disclosure. Personal data controllers should provide a means and policy of openness related to developments, practices, and policies. The transparency rule requires that the identity and usual residence of the controller, existence and nature of the personal data, as well as main purposes and use be readily available.[44]

The guidelines grant individuals rights. The subject must be able to access, confirm, and obtain whether or not the subject's data is held. The data controller's response must be given within a reasonable time and must be in an intelligible form. If the controller refuses, the subject must be able to challenge the denial and challenge the use of the subject's data. If the challenge is accepted, the subject could require that the data be amended, completed, erased, or rectified. The data controller is accountable for complying with the guidelines.[45]

The OECD guidelines consider the transborder flow of personal information. Member states are required to take all appropriate and reasonable steps to make sure that transborder personal data flows are secure and uninterrupted. A state can refuse transfer if the re-export would circumvent its domestic privacy laws or when the other state does not substantially observe the guidelines. Restrictions can apply for certain personal data categories covered by domestic legislation when the other state does not provide equivalent protection. A state should not attempt to circumvent transborder data flows by enacting laws, policies, and practices in the name of protection information privacy and individual liberties.[46]

---

44 *Ibid*.
45 *Ibid*.
46 *Ibid*.

3.4.1.2 Guidelines for Consumer Protection in the Context of Electronic Commerce

The OECD maintains that international consultation and cooperation is needed to effectively deal with different national laws to balance business and consumer concerns and build consumer confidence. Consumer laws, policies, and lawful practices must be maintained. Laws must be focused on preventing and punishing fraudulent, misleading, and unfair commercial conduct.[47]

The general principles maintain that organizations should have transparent and effective consumer protection and fair business, advertising, and marketing practices. Online data should provide accurate information about the business, about the goods or services, information about the transaction, and a secure confirmation and payment process. Dispute resolution and redress processes should adhere to the applicable law and jurisdiction including alternative dispute resolution (ADR) and redress. Privacy standards should provide appropriate and effective consumer protections. Businesses, consumer groups, and governments should also focus on privacy awareness and education. Governments should actively work to protect the standards.[48]

3.4.2 Council of Europe Convention on Data Protection

The first data protection and information privacy laws in Europe were passed by Germany in 1970 and then in 1973 by Sweden. Since the passage of these acts, the issues of privacy expanded to the entire continent. The European data protection position was influenced by privacy violation in World War II by the Nazis, fascists, and the result of Communist actions after the

---

[47] Organization for Economic Co-Operation and Development, *Guidelines for Consumer Protection in the Context of Electronic Commerce*. (2002), at http://www.oecd.org/dataoecd/18/13/34023235.pdf (last visited on 6 January 2012).

[48] Organization for Economic Co-Operation and Development, *Guidelines for Consumer Protection in the Context of Electronic Commerce*. (2002), at http://www.oecd.org/dataoecd/18/13/34023235.pdf (last visited on 6 January 2012).

war. Distrust of governmental personal data bases expanded to corporate data bases.[49]

The next European declaration to consider is the *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, which was adopted by the Council of Europe[50] in 1981 and is a multilateral treaty. The majority of member states (but not all) has signed the document. The document is the first international document that protects personal data against collection and processing abuses. The Council makes the connection between human rights and data protection and information privacy clear. The preamble of the convention, which the member states agreed on, addresses basic DPSIP principles.[51]

Chapter 2, Article 5 set standards for maintaining data quality. The article reads:

> Personal data undergoing automatic processing shall be:
>
> a. obtained and processed fairly and lawfully;
>
> b. stored for specified and legitimate purposes and not used in a way incompatible with those purposes;

---

[49] See Marsha Cope Huie, et al., The Right of Privacy in Personal Data: The EU Prods the U.S. and Controversy Continues, 9 *Tulsa Journal of International and Comparative Law,* 391, 441 (Spring 2002); Steven R. Salbu, *The European Union Data Privacy Directive and Internal Relations,* 9 *Vanderbilt Journal of Transnational Law*, 655, 668 (March 2002).

[50] Council of Europe, *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data: Strasbourg, 28.I.1981*. (1981), at http://conventions.coe.int/Treaty/EN/Treaties/Html/108.htm (last visited on 15 January 2012).

[51] *Id.* at 1. Considering that the aim of the Council of Europe is to achieve greater unity between its members, based in particular on respect for the rule of law, as well as human rights and fundamental freedoms; Considering that it is desirable to extend the safeguards for everyone's rights and fundamental freedoms, and in particular the right to the respect for privacy, taking account of the increasing flow across frontiers of personal data undergoing automatic processing; Reaffirming at the same time their commitment to freedom of information regardless of frontiers; Recognizing that it is necessary to reconcile the fundamental values of the respect for privacy and the free flow of information between peoples.

c. adequate, relevant and not excessive in relation to the purposes for which they are stored;
d. accurate and, where necessary, kept up to date;
e. preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.[52]

Article 6 addresses the problems of special categories. Such data can not be automatically processed unless national laws provide additional protections. The categories include data involving beliefs, criminal convictions, health, political opinions, racial origin, religious beliefs, and sexual lifestyle.[53]

The Explanatory Report of the Council of Europe advances sound DPSIP principles. Sound laws, regulations, and administrative guidelines are needed. Such legal standards aid in voluntary compliance and even technical product innovation. The declaration rejects the folly of the US self-regulation policy. The Report declares that "voluntary measures are not by themselves sufficient to ensure full compliance with the convention."[54]

Article 10 stresses the importance of effective sanction and remedies for protection violations. Data users' duties must be fulfilled. Data subjects' rights must be protected. The sanctions and remedies are based on the act, a *prima facie* case, strict liability, and no proven damages. The remedies may include administrative, civil, and/or criminal sanctions and interventions.

In August of 2001, an *Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Regarding Supervisory Authorities and Transborder Data Flows* was

---

[52] *Id*. at Chapter 2, Article 5.
[53] *Id.* at Chapter 2, Article 6.
[54] *Id.* at 39.

approved.[55] The major changes establish national supervisory bodies and standards for transborder data flows to non-contracting states. Article One establishes that, at a minimum:

> 1. **Each Party shall provide for one or more authorities to be responsible for ensuring compliance with the measures in its domestic law** …
>
> 2. a. To this end, the said authorities shall have, in particular, **powers of investigation and intervention**, as well as the **power to engage in legal proceedings or bring to the attention of the competent judicial authorities violations of provisions of domestic law giving effect to the principles** …b. Each **supervisory authority shall hear claims lodged by any person** concerning the protection of his/her rights and fundamental freedoms with regard to the processing of personal data within its competence.
>
> 3. The supervisory authorities shall exercise their **functions in complete independence.**[56]

Article Two declares that "Each party shall provide for the transfer of personal data to a recipient that is subject to the jurisdiction of a State or organization that is not Party to the Convention only if that State or organization ensures an adequate level of protection for the intended data transfer."[57] The Article gives credence to the view that DPSIP is an international concern.

The Committee of Ministers of the Council of Europe has the power to make highly influential but not legally binding recommendations to the member

---

55 Council of Europe, *Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows*. (2001), at http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=181&CM=1&DF=11/5/2008&CL=ENG (last visited on 4 March 2012).

56 *Id.* at 1. (emphasis added)

57 *Id.* at Article 2.

states. The following table shows recommendations that identify specific data protection and information privacy concerns.

Table 3.0 Resolutions

Issue	Resolution	Title
Databanks in the private sector	Resolution Res (73)22	On the protection of privacy of individuals vis-à-vis electronic databanks in the private sector
Databanks in the public sector	Resolution Res (74)29	On the protection of individuals vis-à-vis electronic data banks in the public sector
Direct marketing	Recommendation Rec (85)20	On the protection of personal data used for the purposes of direct marketing
Employment purposes	Recommendation Rec (89)2	On the protection of personal data used for employment purposes
Insurance purposes	Recommendation Rec (2002)9	On the protection of personal data collected and processed for insurance purposes
Medical data	Recommendation Rec (97)5	On the protection of medical data
Medical databanks	Recommendation Rec (81)	On regulations for automated medical data banks
Payment and other related operations	Recommendation Rec(90)19	On the protection of personal data used for payment and other related operations
Personal data held by public bodies	Recommendation Rec (91)10	On the communication to third parties of personal data held by public bodies
Police sector	Recommendation Rec (87)15	On regulating the use of personal data in the police sector
Privacy on the Internet	Recommendation Rec (99)5	On the protection of privacy on the Internet
Public authorities	Recommendation Rec (81)19	On the access to information held by public authorities
Scientific research and statistics	Recommendation Rec (83)10	On the protection of personal data used for scientific research and statistics
Social security purposes	Recommendation Rec (86)1	On the protection of personal data used for social security purposes
Statistical purposes	Recommendation Rec (97)18	Concerning the protection of personal data collected and processed for statistical purposes
Telecommunication services, with	Recommendation Rec (95)4	On the protection of personal data in the area of telecommunication

telephone services		services, with particular reference to telephone services

58

The Committee of Ministers of the Council of Europe identifies a number of DPSIP concerns. The concerns include issues with databanks in the private and public sector. Specialized concerns also include employment purposes, insurance purposes, medical data, medical databanks, payment and other related operations, personal data held by public bodies, police sectors, privacy on the Internet, and public authorities. Additional issues include scientific research and statistics, social security purposes, statistical purposes, as well as telecommunication and telephone services.[59]

In November of 2004, the European Council became more interested in sharing personal data for security reasons. The Hague Program allows law enforcement officers from any area in the EU to have direct access to a massive data base of personal and biometric information. The Council, perhaps naively, declared that six principles must be followed.[60] The list includes:

> (1) the exchange may only take place in order that legal tasks may be performed,
>
> (2) the **integrity of the data** to be exchanged must be **guaranteed**,
>
> (3) the need to protect sources of information and to **secure the confidentiality of the data at all stages** of the exchange, and subsequently,
>
> (4) common standards for access to the data and common technical **standards must be applied**,
>
> (5) **supervision of respect for data protection**, and appropriate control prior to and after the exchange must be ensured, (6) individuals

---

58 Committee of Ministers, *XVIII. Protection of Personal Data: Resolutions and Recommendations Adopted by the Committee of Ministers*. (2008), at http://www.coe.int/t/e/legal_affairs/about_us/treaties_and_recommendations/listall.asp#P389_25201 (last visited on 22 August 2012).

59 *Ibid*.

60 European Council, *The Hague Programme: Strengthening Freedom, Security and Justice in the European Union*, *Official Journal of the European Union*, C 53(1), pp 1-14. (2005), at http://eurocrim.jura.uni-tuebingen.de/cms/en/doc/557.pdf (last visited on 10 September 2012).

must be **protected from abuse of data** and have the **right to seek correction of incorrect data**.[61]

3.4.3 European Union Directives on Data Protection

The third and final additional relevant declarations from Europe considered here are the *EU Directives on Data Protection.* From 1968 through 1970, The Council of Europe's Parliamentary Assembly studied the issue of data protection and information privacy with technology devices. The Committee found that then current declarations were inadequate to deal with technological intrusions into privacy from public and private sources. The Committee recommended a number of privacy principles that included:

1. The information stored **should be accurate and should be kept up to date**. In general, information relating to the intimate private life of persons or information which might lead to unfair discrimination should not be recorded or, if recorded, should not be disseminated.
2. The information **should be appropriate and relevant** with regard to the purpose for which it has been stored.
3. The information **should not be obtained by fraudulent or unfair means.**
4. Rules should be laid down to **specify the periods beyond which certain categories of information should no longer be kept or used.**
5. Without appropriate authorization, information **should not be used for purposes other than those for which it has been stored, nor communicated to third parties.**
6. As a general rule, the **person concerned should have the right to know the information stored about him, the purpose for which it has been recorded, and particulars of each release of this information.**

---

61 *Id.* at 8. (emphasis added)

7. Every care should be taken to **correct inaccurate information** and to erase obsolete information or information obtained in an unlawful way.
8. Precautions should be taken against any abuse or misuse of information. **Electronic data banks should be equipped with security systems**.
9. Access to the information stored **should be confined to persons who have a valid reason to know it.**
10. **Statistical data should be released only in aggregate form** and in such a way **that it is impossible to link the information to a particular person**.[62]

The Committee provides some general definitions for the resolution. The "term 'personal information' means information relating to individuals (physical persons), and the term 'electronic data bank' means any electronic data processing system which is used to handle personal information and to disseminate such information."[63]

In 1974, the Council of Europe addressed similar concerns in a second resolution related to public agencies. Article 6 of the Council of Europe Convention provides for special categories for shared data. The Article declares,

> Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions.[64]

---

[62] Council of Europe, *Resolution (73) 22 on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector*. (1973), at http://www.coe.int/t/e/legal_affairs/legal_co%2Doperation/data_protection/documents/international_legal_instruments/Resolution(73)22_EN.pdf (last visited on 20 January 2012). (emphasis added)

[63] *Id.* at 10.

[64] Council of Europe, *Resolution (74) 29 on the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector*. (1974), at

Article two defined personal information or data as "any information relating to an identified or identifiable individual ('data subject')."[65]

Starting on October 24, 1995, the EU passed a number of *Data Protection Directives* (95/46/EC).[66] The Directives are a consensus of what individual countries must incorporate into national legislation. The EU is interested in harmonizing national laws to aid in a single-market approach. The focus is based on a historic distrust of governmental and even corporate data handling based on the history with the fascists during the Second World War and post-war Communists.[67]

The Directive provides a blueprint or framework for data protection through national laws. The omnibus nature of the Directive is in sharp contrast to the sectoral, near *laissez-faire,* nature of privacy legislation in the US that only addressed discrete data categories. The Directive addresses all data collection, processing, and storage including transfers to non-EU nations.[68]

---

http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Data_protection/Documents/International_legal_instruments/Resolution%2874%29 29.asp - TopOfPagehttp://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Data_protection/Documents/International_legal_instruments/Resolution%2874%29 29.asp - TopOfPage (last visited on 22 January 2012).

65 *Ibid*.

66 European Union Directives, *The 95/46/EC Directive*. (1995), at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML (last visited on 4 January 2012).

67 See Marsha Cope Huie, et al., *The Right of Privacy in Personal Data: The EU Prods the U.S. and Controversy Continues*, 9 Tulsa Journal of International and Comparative Law, 391, 441 (Spring 2002); Steven R. Salbu, *The European Union Data Privacy Directive and Internal Relations*, 35 Vanderbilt Journal of Transnational Law, 655 (March 2002).

68 On 25 January 2012, The European Commission proposed considerable changes in the directive. The proposal was to establish an EU law rather than a directive. Given that at the time of this writing, the change is only a proposal; the complete details will not be address. The essence of the changes will be integrated in Chapter 9 of this work. For information on the proposal see: European Commission, *General Data Protection Regulation*. (2012), at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf (last visited on 25 January 2012) and European Commission, *General Data Protection Regulation: Impact Assessment*. (2012), at http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_en.pdf (last visited on 25 January 2012).

Chapter 1 Article 2 provides key legal definitions. Personal Data is "any information relating to an identified or identifiable natural person ('data subject'); … identified, directly or indirectly, …[linked to] an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."[69] Processing of personal data addresses

> any operation or set of operations … performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.[70]

The data controller is the "natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data."[71] The data subject's consent applies to "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed."[72]

Under the Directive, data quality must be maintained. The data must be characterized by the following:

> **processed fairly and lawfully;**
>
> **collected for specified, explicit and legitimate purposes** and not further processed in a way incompatible with those purposes.
>
> **adequate, relevant and not excessive** in relation to the purposes for which they are collected and/or further processed;
>
> **accurate** and, where necessary, **kept up to date**; every reasonable step must be taken to ensure that data which are inaccurate or

---

69 European Union Directives, *The 95/46/EC Directive*. (1995), Ch. I, Art. 2(a).
70 *Id.* at 2(b).
71 *Id.* at 2(d).
72 *Id.* at 2(h).

> incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;
>
> kept in a form which permits **identification of data subjects for no longer than is necessary** for the purposes for which the data were collected or for which they are further processed.[73]

Data processing can take place only when "(a) the data subject has unambiguously given his consent."[74] The only exceptions include when the processing was necessary:

> for the **performance of a contract** to which the data subject is party
>
> for **compliance with a legal obligation** to which the controller is subject;
>
> to **protect the vital interests** of the data subject;
>
> for a task carried out in the public interest or in the **exercise of official authority**
>
> for the purposes of the legitimate interests pursued by the controller or by the third party … except where such interests are overridden by the **interests for fundamental rights and freedoms of the data subject which require protection**.[75]

The 1997 Directive 97/66/EC applies the principles to the telecommunications industry. However, it was repealed in 2002 with the Directive 2002/58/EC, which extended the principles to all electronic communications.[76] On March

---

[73] *Id.* at Ch. II, Art. 6(1)(a)-(e). (emphasis added)

[74] *Id.* at Ch. II, Art. 7(a).

[75] *Id.* at Ch. II, Art. 7(b)-(f). (emphasis added)

[76] European Union Directives, *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications)*. (2002), at http://eur-

15, 2006, the EU passed Directive 2006/24/EC titled *The Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communication Services or of Public Communications Networks*.[77] Graham Greenleaf declares that the 1995 directive was the "most important international development in data protection in the last decade."[78]

The 1995 EU Directive uses similar language with the *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*. The Directive declares the following:

> Whereas data-processing systems are designed to serve man; whereas they must, whatever the nationality or residence of natural persons, **respect their fundamental rights and freedoms, notably the right to privacy,** and contribute to economic and social progress, trade expansion and the well-being of individuals.[79]

Article 8 requires explicit consent for the collection of certain types of data. The list includes special categories like ethnicity, medical data, political affiliation, race, religious beliefs, sexual orientation, and union membership.[80]

The directive establishes security principles that include organizational and technical protections. The purpose is to protect against alteration,

---

lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML (last visited on 4 January 2012).

[77] European Union Directives, *Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC*. (2006), at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF (last visited on 4 September 2012).

[78] Graham Greenleaf, *The European Privacy Directive - Completed*, 2 Privacy Law & Policy Reporter 5, 81 (1995), at http://www.austlii.edu.au/au/journals/PLPR/1995/52.html (last visited on 3 March 2012), at 81.

[79] European Union Directives, *The 95/46/EC Directive*. (1995), at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML (last visited on 4 January 2012), at 2.

[80] *Id.* at Art 8.

destruction, loss, unauthorized access, and unauthorized disclosure.[81] Decisions based on the database can not be subject to automated processing.[82]

The EU and its members established the most comprehensive data protection and information privacy law in the world. In addition to establishing legal standards, the addition of offices of data controllers provided for independent implementation.

However, the devil is always in the details. The EU 95/46/EC Directive exempts the "processing of data by a natural person in the course of purely personal or household activities."[83] This exception makes sense. The one exception that does not have adequate checks and balances is the exception that the Directive does not apply for "operations concerning public security, defense, or state security."[84]

Article 8 defines sensitive data, which can not be processed. Section 1 declares that "Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life." However, the Directive standard exceptions apply.[85]

The Directive prohibits secret processing of personal data by governments or businesses. A person/data subject has the legal right to know what information was collected and what was being done with the data.[86] The notice includes why the data is collected, who collects it, and who has access.[87] The Directive requires that data subjects have access, "without

---

81 *Id.* at Art. 17(1).
82 *Id.* at Art. 15(1).
83 *Id.* at Art. 3.2.
84 *Id.* at Art. 3.1.
85 *Id.* at Art 8.
86 Directive at Ch. II, Arts. 10, 11; Arts 12, 14.
87 *Id.* at Ch. II, Arts. 10-12, 14.

constraint at reasonable intervals and without excessive delay or expense."[88] A data subject can request error corrections free of charge.[89] The legal problem is how one discovers that personal data is secretly being processed.

The Directive also requires that all member states harmonize data protection and information privacy law within three years. The approach is based on the view that information privacy is a fundamental human right that requires legal standards to ensure and monitor data processing, data quality, data security, international data transfer rules, and the rights of data subjects. The purpose was to protect information privacy and harmonize the nations in the EU, for the free exchange of information in internal markets. The Directive expands on the data protection standards of the 1981 Convention. This Directive includes data that is not automatically processed. Article 3(1) states that it covers "the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form a part of a filing system."[90]

The directive establishes new privacy law rights. Article 6 addresses data quality. All data processing must meet a quality standard:

> (a) **processed fairly and lawfully**;
> (b) **collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.** Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;
> (c) **adequate, relevant and not excessive in relation to the purposes** for which they are collected and/or further processed;

---

88 *Id.* at Art. 12(a).
89 *Id.* at Art. 14(b).
90 *Id.* at § 3(1). (emphasis added)

> (d) accurate and, where necessary, **kept up to date**; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;
>
> (e) **kept in a form which permits identification of data subjects for no longer than is necessary for the purposes** for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.[91]

Article 7 establishes standards for legitimate data processing. The law requires the following:

> (a) the **data subject has unambiguously given his consent**; or
>
> (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or
>
> (c) processing is necessary for compliance with a legal obligation to which the controller is subject; or
>
> (d) **processing is necessary in order to protect the vital interests of the data subject**; or
>
> (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or
>
> (f) **processing is necessary for the purposes of the legitimate interests pursued by the controller** or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1(1).[92]

---

[91] *Id.* at § 6. (emphasis added)

[92] *Id.* at §7. (emphasis added)

Article 8 establishes the rights of data subjects. The Directive declares that, "Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life."[93]

Article 12 declares that every data subject have a right of access.

> Member States shall guarantee **every data subject the right to obtain from the controller:** (a) **without constraint at reasonable intervals and without excessive delay or expense**: - confirmation as to whether or not data relating to him are **being processed** and information at least as to the purposes of the processing, the **categories of data** concerned, and the **recipients or categories** of recipients to whom the data are disclosed, - communication to him **in an intelligible form** of the data undergoing processing and of any available information as to their source, - knowledge of the **logic involved in any automatic processing of data** concerning him at least in the case of the automated decisions referred to in Article 15 (1);
>
> (b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;
>
> (c) **notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance** with (b), unless this proves impossible or involves a disproportionate effort.[94]

Article 12 also declared the right of subjects to object:

---

[93] *Id.* at Article 8.

[94] *Id.* at Article 12. (emphasis added)

> **Member States shall grant the data subject the right**: (a) at least in the cases referred to in Article 7 (e) and (f), **to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him**, save where otherwise provided by national legislation. Where there is a justified objection the processing instigated by the controller may no longer involve those data;
>
> (b) to object, on request and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing, or to **be informed before personal data are disclosed for the first time to third parties** or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses. **Member States shall take the necessary measures to ensure that data subjects are aware of the existence of the right** referred to in the first subparagraph of (b).[95]

Article 17 sets a standard for data security. The directive required the appointment of Data Controllers to make sure that the data remains confidential and secure. The Directive required the following:

> 1. Member States shall provide that **the controller must implement appropriate technical and organizational measures to protect personal data** against accidental or unlawful destruction or accidental **loss, alteration, unauthorized disclosure or access**, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Having regard to the state of the art and the cost of their implementation, such measures shall ensure **a level of security appropriate to the risks** represented by the processing and the nature of the data to be protected.
>
> 2. The Member States shall provide that the controller must, where processing is carried out on his behalf, choose a **processor providing**

---

[95] *Id.* at 12. (emphasis added)

> **sufficient guarantees** in respect of the **technical security measures** and organizational measures governing the processing to be carried out, and **must ensure compliance** with those measures.
> 3. The carrying out of processing by way of a processor must be **governed by a contract or legal act** binding the processor to the controller and stipulating in particular that: - the processor shall act only on instructions from the controller, - the obligations set out in paragraph 1, as defined by the law of the Member State in which the processor is established, shall also be incumbent on the processor.
> 4. For the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to the measures referred to in paragraph 1 shall be in writing or in another equivalent form.[96]

Article 25 recognized that the European Directive is more advanced than any standard in the world. The issue of data transfer outside of the European Union is set by the following standard:

> 1. The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, **the third country in question ensures an adequate level of protection.**
>
> 2. The **adequacy of the level of protection afforded by a third country shall be assessed** in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in

---

96 *Id.* at 17. (emphasis added)

question and the professional rules and security measures which are complied with in that country.

3. **The Member States and the Commission shall inform each other of cases where they consider that a third country does not ensure an adequate level of protection** within the meaning of paragraph 2.

4. Where the Commission finds, under the procedure provided for in Article 31 (2), that a third country does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, Member States shall **take the measures necessary to prevent any transfer of data of the same type to the third country in question**.

5. At the appropriate time, the Commission shall enter into negotiations with a view to remedying the situation resulting from the finding made pursuant to paragraph 4.

6. The Commission may find, in accordance with the procedure referred to in Article 31 (2), that **a third country ensures an adequate level of protection** within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the **protection of the private lives and basic freedoms and rights of individuals**.[97]

Under the directive, data subjects have a right to know of data held, how to access it, and how to object to uses. Data controllers are accountable for confidentiality and security of the data. Subjects have a legal right to judicial remedies, including compensation, damages, and sanctions. The directive addresses the problems of transnational data flow to countries that do not have adequate protections. The directive further declares that supervisory agencies must be able to hear complaints, be independent, initiate legal

---

[97] *Id.* at Article 25. (emphasis added)

proceedings, intervene in data processing activities, investigate, and monitor data protection and information privacy legal issues.

The EU added to the data protection standards with a directive concerning the processing of personal data and of privacy in the electronic communications sector.[98] The Electronic Communication Directive Article 1(1) declares that members are "**required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy,** with respect to the processing of personal data in the electronic communication sector."[99] Article 4(1) requires that electronic providers "must take appropriate technical and organizational **measures to safeguard security of its services … [and] ensure a level of security appropriate to the risk presented.**"[100] Article 5(1) mandates that members must do the following:

> ensure the **confidentiality of communications** and the related traffic data by means of a public communications network and publicly available electronic communications services, … **prohibit listening, tapping, storag**e or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, **without the consent of the users concerned**, except when legally authorized to do so.[101]

Providers are required to **erase confidential information no longer needed**.[102] An exception includes billing data until paid or the period for a legal challenge expires.

---

98 European Union Directives, *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications)*. (2002), at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML (last visited on 4 January 2012).

99 *Id.* at Article 1(1).

100 *Id.* at Article 4(1). (emphasis added)

101 *Id.* at Article 5(1). (emphasis added)

102 *Id.* at Article 6(1). (emphasis added)

3.4.3.1 Third Country Rules

The European Directives apply only to members of the EU, so rules are necessary to address the issues in other or third countries. The members also exist in a wider economic, legal, and political system. Data controllers could outsource data processing to other countries or companies. Other countries, including most notably the US, consistently violated the spirit and letter of the European law. Non-EU nations did not have a Data Protection Authority (DPA-EU).

A major focus of the European Directive is the transfer of data to other countries. Within the union, transfers are determined by this directive and national laws. A key issue is the transfer of data to the rest of the world. Transfers can be accomplished based on the adequacy of the third countries' DPSIP standards. Transfers require that the data subject has freely given unambiguous consent or the transfer must be necessary rather than simply convenient.[103] The country transfer test includes the "nature of the data, the purpose and duration of the proposed …operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in those countries."[104] The Council determined that data could be easily transferred to CA because the country was determined to be adequate.[105] AU and SA have not been determined to be adequate.

Upon passage of the European Directive, some unintended consequences appeared. For instance, members could outsource data processing to a country that did not have strict laws and regulation. The EU was unable to get

---

[103] Directive at Ch. IV, Art. 26(1).

[104] Directive at Ch. IV, Art. 25(2).

[105] Council of the European Union, *Agreement between the European Community and the Government of Canada on the processing of API/PNR data (2006/230/EC)*. (2005), at http://ec.europa.eu/justice_home/fsj/privacy/docs/adequacy/pnr/canada_ec_230_2006_en.pdf (last visited on 26 December 2012). Chapter 5 explores the issue in more depth.

other countries to pass omnibus DPSIP programs. The US was a major obstacle. The third country rules were loosened. The EU essentially switched from a strict country to country standard to include a company-by-company approach based on established contract clauses.

The International Chamber of Commerce advocated for the interests of multi-jurisdictional, multinational conglomerates. Thus, the Binding Corporate Rules (BCR) was established. BCR apply to internal and external corporate data transfers and outsourcing partners. The rules are legally binding for data transfers using a single set of rules. The rules are more flexible, less costly, less time consuming, and allegedly more proactive than dealing with national laws.[106] The European Commission Data Protection Working Party established a set of guidelines that cover the legal standards for BCR. The rules must address the "binding nature, effectiveness, cooperation duty, description of processing and data flows, mechanisms for reporting and recording changes, and data protection safeguards."[107]

The Commission of the European Communities passed a number of binding legislative decisions related to standard contractual clauses concerning the transfer of personal data to third countries. The clauses are known as binding standard clauses or binding model contractual clauses.[108] The approved

---

106 International Chamber of Commerce, *ICC Report on Binding Corporate Rules for International Transfers of Personal Data*. (2004), at http://www.iccwbo.org/uploadedFiles/ICC/policy/e-business/pages/FINAL_ICC_BCRs_report_rev.pdf (last visited on 26 December 2012).

107 Article 29 Data Protection Working Party, *Working Document Setting Up a Table with the Elements and Principles to be Found in Binding Corporate Rules (1271-00-00/08/EN-WP 153)*. (2008), at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp153_en.pdf (last visited on 26 December 2012).

108 See *Commission Decision* (2001/497/EC), *Commission Decision* (2002/16/EC, *Commission Decision* (2004/5271/EC) at http://ec.europa.eu/justice_home/fsj/privacy/modelcontracts/index_en.htm (last visited on 26 December 2012). See also Article 29 Data Protection Working Party, Opinion 3/2009 on the Draft Commission Decision on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC. (2009), at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp161_en.pdf (last visited on 26 December 2012).

contract clauses allow transfer of data that insures sufficient safeguards to third countries. The pre-approved adhesion contracts apply to data exporters and data importers. The clauses address automated decision making, confidentiality, data quality, direct marketing restrictions, dispute resolution, onward transfer restrictions, proportionality, purpose limitations, rectification, rights of access, security, sensitive data special rules, and transparency. The need for audits, inspections, and reasonable inquiries are addressed.

A data subject or data protection authority can litigate for injuries related to a breach of contract. Depending on the clause, the actions can be directed toward the data importer or exporter; the importer and exporter are liable jointly and severally unless an indemnification agreement,[109] due diligence, or proportional liability are in place.[110]

The US was considered a third country in respect of the Directive. Thus, EU data subject information could not be transferred to the US. The US objected. A compliance problem existed based on the economic power of US multinational corporations, ethnocentric attitudes, Neo-Conservative political power sources, and Corporate Republic value differences. The US government refused to comply with the EU transfer decision, threatened an economic war, and sought a compromise. The US Department of Commerce led the attack. A country-specific *safe harbor* compromise was developed. The US promised to develop a voluntary, self-certification approach as a data transfer alternative. The agreement applied only to personal information related strictly to European data subjects.

Corporations that seek safe harbor protection must seek registration with either the FTC or Department of Transportation depending on the industry sector. The firm must notify the Department of Commerce of its self-certification. The company pays a $200 USD application fee plus a $150 yearly fee, and completes a simple data form. A public privacy policy

---

[109] *Commission Decision (2001/497/EC),* at *26.*
[110] *Commission Decision* (2004/5271/EC, at 115.

statement is also required. Most participants develop an in-house policy only. Some joined with or were members of a self-regulating industry group.

A safe harbor participant must agree to follow seven basic principles. The list includes clear and conspicuous note, an opt-out option except for sensitive information, rules for onward transfer, reasonable security efforts, as well as providing data integrity, reasonable access, and a dispute resolution process.[111] However, relatively few applicable US corporations abide by these principles.

3.4.3.2 Analysis

The EU 1995 Directive sets an international standard for data protection. With technological developments, serious threats to DPSIP evolved. The Directive attempted to confront such issues, but systemic limitations presented obstacles.[112] However, with time some key elements changed. The UK became one of most surveillance-ridden nations in the world. Moreover, the EU appeared to be following the pattern.

The EU 1995 Directive attempts to balance a number of privacy-related issues. The task was made difficult due to national differences. Germany used a constitutional justification while the UK focused on a regulatory approach. Key terms like the "legitimate interests of a society" were rather vague; therefore, a number of exemptions were added to abate opposition. Most member states attributed a low priority to DPSIP concerns.[113] The drafters did not want to limit the power of some countries to shape the

---

111 European Commission, *How Will the "Safe Harbor" Arrangement for Personal Data Transfers to the US Work?* (2009), at http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/adequacy-faq1_en.htm (last visited on 26 December 2012). See also Caslon Analytics, *Privacy Guide*. (2004), at http://www.caslon.com.au/privacyguide14.htm (last visited on 26 December 2012). See Chapter 6 of the current work for more analysis.

112 Patrick J. Murray, The Adequacy Standard Under Directive 95/46/EC: Does U.S. Data Protection Meet This Standard? 21 *Fordham International Law Journal*, 932, 971 (1998).

113 Ulrich U. Wuermeling, Harmonisation of European Union Privacy Law, 14 *John Marshall Journal of Computer & Information Law*, 411, 414 (1996).

national law.[114] The effect was that member nations could limit the effectiveness of the DPSIP legal standard.[115]

Because the EU 1995 Directive did not apply to activities "outside the scope of Community law," such as proclaimed national security concerns,[116] the spirit of the directive could be easily avoided. No operational definitions are provided. Member states are allowed to re-write the law. Few controls are instituted to review the police use of personal data.[117] Governments prize efficient police operations, and the mentality tends to ignore the data subject's "right to know." Spiros Simitis argued that clear access rules should "never be totally excluded, but rather can at most be partially restricted or temporarily suspended in a series of unequivocally defined and exhaustively listed cases."[118] Member States can technically comply with the Directive while ignoring the principles involved.

A data subject's access to the data is also limited when it involves scientific research.[119] No qualifications are needed for the organization conducting the research nor any audited purpose or quality control restrictions. Any business can establish a research department to avoid Directive restrictions.[120] Member states could define key terms like "sole research use" or "adequate safeguards." The exemptions are vague and fail to define measures, decisions, or adequate legal safeguards related to the principle.[121]

---

[114] Spiros Simitis, From the Market to the Polis: The EU Directive on the Protection of Personal Data, 80 *Iowa Law Review,* 445 (1995). He argued that information privacy was no longer just an individual concern and could be used for behaviour control.

[115] *Id.* at 451.

[116] Directive at *3(2), 13*.

[117] Jacqueline Klosek, The Development of International Police Cooperation Within the EU and Between the EU and Third Party States: A Discussion of the Legal Bases of Such Cooperation and the Problems and Promises Resulting Thereof, 14 *American University International Law Review* 3, 599-656 (1999).

[118] Spiros Simitis, From the Market to the Polis: The EU Directive on the Protection of Personal Data, 80 *Iowa Law Review* 3, 445 (1995). at 460.

[119] Directive Art 13(2).

[120] Simitis at 457.

[121] *Id.* at 459.

The distinctive feature of the European approach to DPSIP is the comprehensive nature of the legislation. Each country must establish an independent privacy protection agency with an identified data protection/ information privacy commissioner and office that has responsibility for compliance with laws or regulations related to data protection and information privacy. Each organization that collects or deals with personal data must have a similar officer and office.

DPSIP principles embody the principle of human rights. The documents are clear about information privacy in general. However, there are three major problems. The first is that business and governmental concerns, security, and Neo-Conservative perspectives always trump human rights. The second is that none of the general human rights declarations specifically addresses information privacy concerns. The third is that the human rights perspective ignores the related legal issues of property, ownership, intellectual property, consumer protection, and legal protections.

In early 2012, the EU Commission proposed a strategic change related to DPSIP standards. The historic directive would be changed to a regulation. The regulation would apply to all EU States, impact all non-EU nations dealing with EU parties, and eliminate the historic patchwork directive. The proposal included a shift to an opt-in rather than opt-out agreement, a right of data portability, a right to be forgotten, new breach notification standards, privacy by design standards,[122] and increased enforcement powers. Under the proposed change, protecting personal information became a fundamental right and the free flow of information became a common good.[123]

---

[122] This standard is evaluated in Chapter 5 of this work. The CA government developed the concept.

[123] Given that the EU processing of Directives and Regulations has historically taken years to the point of passage, a critical assessment of the current proposal is outside the time limited assessment of this study. However selected features of the EU proposal are integrated in Chapter 10 gold standard proposal. The proposed regulation can be found at: European Commission, *General Data Protection Regulation*. (2012), at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf (last visited on 25 January 2012).

3.4.4 Charter of Fundamental Rights of the European Union

In 2007, the Lisbon conference prepared the *Charter of Fundamental Rights*. The Charter, which became effective on 1 December 2009, identified key privacy issues. The list of such issues includes the principle that "Everyone has the right to respect for his or her private and family life, home and communications."[124] The work also addresses issues related to the protection of personal data. Specifically, the Charter declares the following:

1. Everyone has the **right to the protection of personal data** concerning him or her.
2. Such data must be **processed fairly for specified purposes** and on the basis of the **consent of the person concerned** or some other legitimate basis laid down by law. Everyone has the **right of access to data** which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be **subject to control by an independent authority**.[125]

Viviane Reding, a Luxembourg politician who served as a European Commissioner responsible for Information Society and Media, summarizes the current thinking of the Commission on DPSIP issues. She declares that "Without information security, protection of privacy and personal data is not possible... A key principle of EU data protection law is that those who process personal data have to take the necessary security measures to counter the risks to this data."[126] She further declares that, "Those who profit from the

---

[124] European Parliament Council - Commission on Risk Assessment and Risk Management, *Charter of Fundamental Rights of the European Union (2007/C 303/01)*. (2007), Title II, Art. 7. at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2007:303:0001:0016:EN:PDF (last visited on 21 December 2012).

[125] *Id.* at Art. 8. (emphasis added)

[126] Viviane Reding, *Securing Personal Data and Fighting Data Breaches*. (2009, October 23), at http://ec.europa.eu/commission_barroso/reding/docs/speeches/2009/brussels-

information revolution must respond to the public policy responsibilities that come with it."[127]

The Charter of Fundamental Rights Commission also addresses issues related to developing technologies like RFID tags. The standards require that "RFID enabled products must be automatically deactivated at the point of sale."[128] However, the consumer does have an opt-in option. Businesses and governmental agencies are required to provide clear, simple, and purposeful statements. RFID users need to provide product information to potential consumers. DPSIP users are required to conduct impact assessments prior to smart chip use. The Privacy impact assessment should also be mandated to be reviewed by "national data protection authorities."[129]

The EU Information Commissioner's Office contracted with Rand Europe to perform a review of the Data Protection Directive. The analysis found that the directive was a model of good DPSIP practices that harmonized sound principles. The model allows for some internal marketing for the data. The Directives permits some flexibility and is technology neutral. A major strength of the Directive is that it increased awareness of DPSIP issues. The Directive became an international standard.

A range of DPSIP weaknesses have been found. The issues of personal data and risks are unclear. Transparency and notification standards are, in practice, inconsistent and ineffective. Transfer rules are found to be outmoded and cumbersome. The functional powers, accountability standards, and enforcement abilities of the various Data Protection Authorities is inconsistent. Key definitions of processing entities are simplistic and

---

20091023.pdf (last visited on 23 December 2012), at 2. As of December 2009, she was the EU Commissioner for Justice and Fundamental Rights.

127 *Id*. at 2-3.

128 Paul Melle, *EC Sets Out Privacy Requirements for Smart RFID Tags*, Computer World. (2009, May 13), at http://computerworld.co.nz/news.nsf/scrt/5EA85E21103475EBCC2575B400729F86 (last visited on 23 December 2012), at 1.

129 *Ibid*.

static.[130] The study did find evidence of "information based harm, inequality, injustice, and restriction of moral autonomy."[131] DPSIP violations cause harm to society. The personal damage includes potential and actual economic, personal, physical, psychological, and social harm.[132] The letter of the DPSIP laws must be clear, but the enforcers and authorities must also be accountable and responsible.

These international treaties and declarations established a basis for DPSIP law. Some of the documents related to the law as a personal property and intellectual property right whereas other documents relate the legal basis as a human and civil right. No matter the basis, an international treaty and declaration existed for DPSIP laws. Broad declarations were important but lacked operational specificity.

3.5 Asia-Pacific Economic Cooperation Privacy Charter

The Asia-Pacific Economic Cooperation (APEC) organization was formed at the urging of Australian Prime Minister Bob Hawke.[133] Three of the member countries—AU, CA, and the US—were subjects of this study. The organization focuses on regional economic integration. The focus includes trade and investment liberalization, business facilitation, and economic and technical cooperation.[134]

The group's 2004 privacy charter uses some key terms and principles;

---

[130] Hans Graux, Neil Robinson, Maarten Botterman, & Lorenzo Valeri, *Review of the European Data Protection Directive* (Rand Europe. 2009).

[131] *Id.* at 2-3.

[132] *Id.* at 48.

[133] The membership through 2010 included Australia, Brunei Darussalam, Canada, Chile, China, China and Chinese Taipei, Hong Kong, Indonesia, Japan, Korea, Malaysia, Mexico, New Zealand, Papua New Guinea, Peru, Philippines, Russia, Singapore, Thailand, United States, and Viet Nam.

[134] APEC, *Asian-Pacific Cooperation*. (2009), at http://www.apec.org/apec/about_apec.html (last visited on 10 October 2012). See also http://www.worldlii.org/int/other/PrivLRes/2003/1.html (last visited on 17 December 2012).

however, the details reveal several errors and miscalculations. The standards are allegedly based on the OECD privacy principles. However, they are much weaker than the OECD standards. APEC also ignores some basic EU Data Protection Directive standards. The standards do not require any national legislative or regulatory mechanisms. No data protection export requirements exist. With the exception of CA, the privacy charter was devised by countries that did not want to meet the EU directive. The APEC framework is based on the principle of self regulation.

The framework of APEC focuses on establishing ethical e-commerce practices that balance business needs and commercial interests with some consumer protections. The APEC focuses on reasonable consumer expectations that businesses should recognize. The practices apply only to natural persons, not legal persons.

The framework suggests a number of privacy principles. The first is to prevent harm, meaning to prevent the misuse of information. A notice principle included notice of the data collection, purpose of the collection, disclosure principles, and controller identification notice before or at the time of collection. No notice is required for alleged publically available information. The information collection process should be fair, lawful under national standards, and relevant to the stated purpose. The principle allows for appropriate consent or notice, but does not require both.[135] The use of the information must be limited to the stated purpose or to other purposes that are compatible or related purposes determined by the collector. APEC provides exceptions that include individual consent, requested products or services, or legal authority. The APEC framework includes weak principles for instruments, proclamations, and pronouncements.[136]

---

[135] How can one consent if there is no notice? How can notice eliminate the need for informed consent by the data subject?

[136] Asia-Pacific Economic Cooperation, *APEC Privacy Framework*. (2004, November 17-18), at http://www.nacpec.org/docs/APEC_Privacy_Framework.pdf (last visited on 21 December 2012), at 8-11.

The APEC framework also includes language that, only when a business determines it is appropriate, the individual should be provided a level of choices related to the collection, disclosure, and use of the personal information. When the organization determines that the issue is appropriate, the choice should be accessible, affordable, clear, easily understood, and prominent. Only when required for the stated purpose of the collection, the controller makes sure that the data is accurate, complete, and kept up to date. Security safeguards should be proportional to the likelihood, sensitivity, and severity of the threatened harm as determined by the data controller. When appropriate, safeguards should protect from data loss, disclosure, misuses, modification, risks, unauthorized access, unauthorized destruction, or use. When appropriate, periodic reassessments and reviews should be conducted.[137]

The APEC framework also state that individuals should have access and the ability to request corrections of the data file. Upon proving identity, corrections could be made to challenge the accuracy of the data when appropriate to have the data amended, completed, deleted, or rectified. The request must be within a reasonable manner and time, generally understandable, and not excessive. The access can be denied when the burden or expense is disproportionate to the risk. Protection of confidential commercial information, legal information, and protecting others' privacy or security issues can also result in a denial of access.[138]

The information controller should[139] be held accountable to following the APEC framework. When transferring data domestically or internationally, the controller should[140] obtain individual consent, do due diligence, or take

---

[137] *Id.* at 12-14.
[138] *Id.* at 15-18.
[139] Should means "ought to," but not necessarily will.
[140] *Ibid.*

reasonable steps to ensure protection.[141] The controller has full power over which standard would apply.

The implementation of the framework was rather open. Members were allowed to use administrative, industry self-regulatory, legislative approaches, or a combination of approaches. The approach, which was meant to be flexible, might include central authorities, designated industry bodies, multi-agency enforcement, or a combination of these elements. Each country can decide which elements of the approach to use.[142]

3.5.1 Analysis

The APEC framework declares that people recognize the importance of privacy and that it is a basic human right. However, enforcement requires justification and proportionality. The standards for consent are insufficient. Accountability is required but the responsibility is on the person rather than the data collector. Openness is suggested, but the regulatory responsibility is on the individual. The data owner must advocate for non- discrimination issues.

Google was concerned about the impact of the EU DPSIP standards. The corporation's privacy counsel started a movement to abandon the strict EU and CA standards and even some US state laws in favor of the APEC business-friendly system.[143] Not surprisingly, the company wanted to change DPSIP law standards in favor of full industry self-regulation. Historic research shows that the APEC approach went through several versions that were increasingly less stringent. Graham Greenleaf[144] argues that part of the reduction of standards was due to increased participation in the process by

---

141 *Id.* at 19.

142 *Id.* at 20.

143 Eric Auchard, *Google Says World Could Use Asian Privacy Approach*, Reuters. (2008, September 14), http://mobile.reuters.com/mobile/m/FullArticle/CTECH/ntechnologyNews_uUSN1340110220070914 (last visited on 14 September 2012).

144 Graham Greenleaf, *APEC Privacy Principles: More Lite with Every Version*. (2003), at http://www2.austlii.edu.au/~graham/publications/2003/APECv5_article.html (last visited on 1 August 2012).

the US. The APEC privacy standards are "inadequate to produce a high quality result."[145]

Eric Schmidt, Google's Chief Executive Officer, illogically and unreasonably argues that only those who have done something wrong should be concerned about privacy issues. He publically declared that, "If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place."[146] Yet, he personally banned a news agency's access to Google public meetings when it published information about him that could be found only on a Google site.[147]

Not surprisingly, Google ranks as the worst Internet company in terms of privacy protection.[148] The Google advocacy and the APEC standards are clear attempts at Neo-Conservative market governance. Both suggest that business and corporate powers should control all information privacy activities.

The Australian Privacy Foundation is highly critical of the APEC privacy standards and principles. The list of criticisms includes the following facts:

> [APEC] categories of 'national exceptions' are open-ended. There are ineffective controls on the scope of any particular 'national exception'. Notice is not clearly required to be given to individuals from whom information is collected. Collection is not limited to the minimum information necessary for a stated purpose. Secondary uses are allowed for 'compatible' purposes, a very weak test. The elevation of 'choice' (or consent) to a separate principle facilitates the commodification of privacy. 'Commercial proprietary' reasons should

---

145 Graham Greenleaf, *APEC Privacy Principles: More Lite with Every Version*. (2003), at http://www2.austlii.edu.au/~graham/publications/2003/APECv5_article.html (last visited on 1 August 2012), at 8.

146 Iain Thomson, *Google Boss Dismisses Privacy Concerns*. (2009), at http://www.securecomputing.net.au/News/162419,google-boss-dismisses-privacy-concerns.aspx (last visited on 10 December 2012), at 3.

147 *Ibid.*

148 BBC News, *Google Ranked 'Worst' on Privacy*. (2007, June 11), at http://news.bbc.co.uk/2/hi/technology/6740075.stm (last visited on 11 June 2012).

> not be an exception to access and correction. 'Maximizing Benefits' should not become a principle. The OECD Principles of Purpose Specification, Openness and Data Export Limitation are missing and their content should be reinstated in the APEC Principles. At least an additional Deletion Principle should be added for a minimum set.[149]

APEC is a trade and investment organization and has membership enforcement options only. Chris Pounder expresses further concerns. The framework problem list includes the following facts about the policy and system. It:

> (1) is unlikely to provide an adequate level of protection as required by the European Data Protection Directive;
>
> (2) is likely to result in inconsistent implementation by APEC member states and a confused hotchpotch of national data protection laws, regulations or rules;
>
> (3) is likely to be policed by a very weak regulatory regime;
>
> (4) is likely to allow member states to adopt divergent policies on important privacy aspects with the result that the Framework is unlikely to provide a sound, long-term, basis for the international trade in personal data; and
>
> (5) contains principles and procedures which could be implemented in a way that results in an unacceptable or minimal level of protection for personal data.[150]

The basic document addresses nine principles that include preventing harm; notice; collection limitations; uses of personal information; choice; integrity of personal information; security safeguards; access and correction; and

---

149 Australian Office of The Federal Privacy Commission, *Community Attitudes towards Privacy 2004* (Author. 2004), at 4.

150 Chris Pounder, *Why the APEC Privacy Framework is Unlikely to Protect Privacy*. (2007), at http://www.out-law.com/page-8550 (last visited on 1 August 2012), at 5.

accountability. While the topics are similar to other established standards, the actual details include more business-friendly definitions and avoidance options.

The APEC standard of preventing harm is intended to prevent information misuse. The standard places the burden of proof on the consumer. In contrast, other standards such as the Canadian system address issues of unauthorized collection, disclosure, and use as per se violations with no proof of harm required. The APEC standard fails to define remediation and proportionality in any operational terms.

The principle of notice sets specific time periods that include before or at the time of collection standards. No informed consent requirements are established. The principle does not address automatic collection as in the use of cookies.

Collection limitations are restricted to notice or consent at the time of collection. No limitations are placed on the amount of information collected or the potential uses.

The business or government use of personal information standard is more extensive than the OECD standard, which requires consent or legal authority. The APEC framework includes authority of law, consent, or when the individual requests products or services. The company determines when the individual request is necessary.

Choice is required only when the exercise of the choice is appropriate. The question of who determined choice—the business or individual—is unclear.

The APEC adopted a standard concern for the integrity of personal information found in standard DPSIP documents. The problem is that the integrity issue is only important when a necessity of purpose exists to use the data. Moreover, the data controllers make such decisions.

Data security is a business and policy given.[151] The APEC framework theoretically limits the use or transfer of personal data standards that are reasonable and proportionality balanced by a vague standard of likelihood and severity. However, no operational standards are established.

The APEC principle of access and correction establishes the concept as a central aspect but not an absolute right. Individuals can be denied direct access to the information. No requirement is established to insure that individuals should have any awareness of the extent of the information or to whom it may have been disclosed.

Accountability standards are diminished. Data controllers are held to be accountable for the use and disclosure of personal information. Informed consent is suggested. However, only due diligence or reasonable steps are needed to protect the controllers.

The approach places no restriction on data retention limits. Moreover, no limits are placed on collection, consent, disclosure, or use of personal information.[152]

3.6 African Privacy Declarations

While the Constitution of the Republic of South Africa[153] provides clear privacy rights, African continent international declarations on DPSIP legal issues are limited. However, one can argue that Article Eleven of the *African Charter on Human and People's Rights* infers a DPSIP legal right. The

---

151 Not subject to debate, assumed to be true.

152 See A.C.L.U. of Northern California, *Google's Privacy Policy: What Would be the Real Impact of APEC?* (2007), at http://www.aclunc.org/issues/technology/blog/asset_upload_file251_6206.pdf (last visited on 3 November 2012).

153 *Constitution of the Republic of South Africa,* 1996, at http://www.info.gov.za/documents/constitution/1996/index.htm (last visited on 19 June 2012).

African Union's *Declaration of Principles on Freedom of Expression in Africa* specifically uses the term "privacy."

Article eleven of the African Charter on Human and People's Rights declares the following:

> **Every individual shall have the right to assemble freely with others**. The exercise of **this right shall be subject only to necessary restrictions provided for by law,** in particular those enacted in the interest of national security, the safety, health, **ethics and rights and freedoms of others.**[154]

The right to assembly infers that there is a right not to assemble or share. Ethics, rights, and freedom of others further infers a right to ethics, rights, and freedoms that protects oneself. Human rights issues are difficult to establish against powerful business and governmental powers. The Charter was agreed to prior to more specific DPSIP international declarations.

Article twelve of the African Union's *Declaration of Principles on Freedom of Expression in Africa* does express a perspective on privacy. The section addresses freedom of expression and protecting reputations. Sub-section Two declares that "Privacy laws shall not inhibit the dissemination of information of public interest."[155] The Declaration focuses on defamation issues[156] more than information privacy issues. The first implementation issue is who should determine the public interests and at what cost. The second issue is that "privacy laws shall not inhibit the dissemination of information"[157] may be considered a universal negative. The argument could

---

154 African Commission on Human and Peoples' Rights, *African Charter on Human and Peoples' Rights* (Author. 1981). (emphasis added)

155 African Commission on Human and Peoples' Rights, *Declaration of Principles on Freedom of Expression in Africa*. (2002), at http://www.achpr.org/english/declarations/declaration_freedom_exp_en.html (last visited on 21 January 2012).

156 Article 19, *Implementing Freedom of Expression: A Checklist for the Implementation of the Declaration of Principles on Freedom of Expression in Africa* (Author. 2006).

157 *Ibid.*

be made that no privacy law shall inhibit, including established DPSIP legal principles.

3.7 National and Non-Governmental Organization Standards

A number of governmental and non-governmental organizations have established information privacy standards. The standards, while not legislative, provide a means to measure a standard of care expectation. The standards have influenced DPSIP debates and policy making. The standards are organized chronologically rather than by nation state.

One of the first major administrative rulings was the US guidelines established in 1973 by the Advisory Committee on Automated Data Systems of the US Department of Health, Education, and Welfare (now Health and Human Services). The *Code of Fair Information Practices* established five principles, which include the following:

1. There must be **no personal data record-keeping systems whose very existence is secret.**
2. There must be a **way for a person to find out what information about the person is in a record and how it is used**.
3. There must be a way for a **person to prevent information** about the person that was obtained **for one purpose from being used or made available for other purposes without the person's consent**.
4. There must be a way for **a person to correct or amend a record** of identifiable information about the person.
5. **Any organization** creating, maintaining, using, or disseminating records of identifiable personal data **must assure the reliability of**

> **the data for their intended use and must take precautions to prevent misuses of the data.**[158]

In 1977, the US Privacy Protection Study Commission, established under the Privacy Act of 1974,[159] established voluntary privacy standards. The standards restrict the "Disclosures of Personal Employment Data" while providing for "individual access" and "informing the individual" of data collection efforts and informed consent. Special rules were established regarding protecting "medical records," "use of investigative firms," and "Arrest, Conviction, and Security Records."[160]

The report also established standards for periodic and systematic reviews. Such review should include the following:

1. Number and types of records an employer maintains on individual employees, former employees, and applicants;
2. Items of information contained in each type of employment record it maintains;
3. Uses made of the items of information in each type of record;
4. Uses made of such records within the employing organization;
5. Disclosures made of such records to parties outside the employing organization;
6. Extent to which individual employees, former employees, and applicants are both aware and systematically informed of the uses and disclosures that are made of information in the records kept about them.[161]

---

158 Health & Human Services, *Code of Fair Information Practices* (1973), at http://aspe.hhs.gov/datacncl/1973privacy/Summary.htm (last visited on 30 July 2012), at 6. (emphasis added)

159 Privacy Act of 1974. 5 U.S.C. § 552(a)(4) (1974) (U.S.).

160 Privacy Protection Study Commission, *Personal Privacy in an Information Society*. (1977), at http://www.epic.org/privacy/ppsc1977report/ (last visited on 29 July 2012), 11.

161 *Ibid*.

In 1996, the CA Standard Association established a model privacy code. The standards include the following principles:

1. An organization is responsible for personal information under its control.
2. The purposes for collecting personal information shall be identified at or before the time the information is collected.
3. An organization should obtain consent of the individual for the use or disclosure of his or her personal information.
4. The collection of personal information shall be limited to the purposes identified by the organization.
5. Personal information shall not be used or disclosed for purposes other than those the organization states. If the organization wants to use personal information for other purposes not identified at or before the time the information is collected, it should obtain the consent of the individual.
6. An organization collecting personal information should keep the information accurate, complete, and up-to-date.
7. An organization collecting personal information should keep the information safe.
8. An organization shall provide information about its policies and practices with regard to its management of personal information it collects.
9. An organization should inform the individual whose personal information is collected about the existence, use, and disclosure of his or her personal information. The organization should give the individual access to one's own personal information. An individual shall be able to request amendment if the collected information is inaccurate or incomplete.
10. An organization collecting personal information should designate an individual or individuals to be accountable for the organization's

compliance and to address complaints.[162]

In its 1990 model privacy code, the CA Banking Association declared that "Canada's chartered banks have always been, and will continue to be, concerned with maintaining accuracy, confidentiality, security and privacy of customer information."[163] In 1996, the Code was modified. The standards include the following:

1. An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.
2. The purposes for which personal information is collected shall be identified at or before the time the information is collected.
3. The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.
4. The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.
5. Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.
6. Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

---

[162] Canadian Standards Association, *Model Code for the Protection of Personal Information*. (1996), at http://www.csa.ca/standards/privacy/code/Default.asp?language=English (last visited on 15 June 2012), Principles 1-10.

[163] Colin J. Bennett, *The Protection of Personal Financial Information: An Evaluation of the Privacy Codes of the Canadian Bankers Association and the Canadian Standards Association*. (1997), at http://web.uvic.ca/polisci/bennett/research/cba.htm (last visited on 31 December 2012), at 4.

7. Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.
8. An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.
9. Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.
10. An individual shall be able to address a challenge concerning the above principles to the designated individual or individuals accountable for the organization's compliance.[164]

The newer Code is more clear and user friendly. However, the standard does include business-friendly opt-out provisions which are subject to misuse. This new language is more prescriptive and relevant. While each member bank must adopt the principles, each bank has the option to establish its own key operational definitions.[165]

In its 1998 *Privacy Report,* the US FTC established four privacy principles. The Principles are listed below:

1. Notice – data collectors must disclose their information practices before collecting personal information from consumers.
2. Choice – consumers must be given options with respect to whether and how personal information collected from them may be used for purposes beyond those for which the information was provided.
3. Access – consumers should be able to view and contest the accuracy and completeness of data collected about them.

---

[164] *Id.* at 4.
[165] *Ibid.*

4. Security – data collectors must take reasonable steps to assure that information collected from consumers is accurate and secure from unauthorized use.[166]

The US FTC established several key Privacy Fair Practices. The standards require the following:

1. Companies should give a notice to their Web site visitors about their information practices and policies.[167]
2. Consumers should have a choice to limit use or disclosure of their personal information.[168]
3. Consumers should be allowed to access and correct their personal identifiable information.[169]
4. The information collectors should secure the collected information and maintain the integrity of the information.[170]
5. An enforcement mechanism should be established to ensure the compliance with the privacy principles and provide redress to harmed individuals.[171]

In 1998, the US National Telecommunications and Information Administration of the Department of Commerce responded with notice of public hearings. The Department of Commerce proposed elements for protecting information privacy that included consumer awareness, published privacy policies, notification of changes, consumer education, choice, data security, data integrity, consumer access, and accountability.[172] The proposed follow-up

---

166 Federal Trade Commission, *Privacy Online: A Report to Congress*. (1998c), at http://www.ftc.gov/reports/privacy3/toc.shtm (last visited on 10 May 2012), § 3.A.

167 *Id.* at 7-8.

168 *Id.* at 8-9.

169 *Id.* at 9.

170 *Id.* at 10.

171 *Id.* at 10-11.

172 National Telecommunications And Information Administration - Department Of Commerce, *Elements of Effective Self Regulation for the Protection of Privacy and Questions Related to Online Privacy*. (1998, June 5), at http://www.ntia.doc.gov/ntiahome/privacy/6_5_98fedreg.htm (last visited on 1 June 2012), § 1.

compliance standards and data collection standard is questionable. The Department of Commerce established fair practices include:

1. Information collectors should notify their data subjects about their privacy policies and consumer education.
2. Information collectors should offer data subjects opportunities to dictate the use of their personal information.
3. Information collectors should ensure data security.
4. Information collectors can keep only information that is relevant for the purpose of the collection, and that information should be accurate, complete, and current.
5. Data subjects should be allowed to access and correct their personal identifiable information.
6. Information collectors are responsible for any consequences resulting in failing to comply with its privacy policy.[173]

Both the FTC and the National Telecommunications and Information Administration of the Department of Commerce took a somewhat different stand regarding privacy regulations. While both fall in with the party line, each declared that legal enforcement mechanisms must be established and followed. The Clinton administration responded with a faint threat of legal enforcement if self-regulation efforts failed.

In 1999, the Electronic Financial Services Council responded to the challenge. The Council recognized that, "Though lacking the power to require their members to abide by these principles, the associations recommended their adoption."[174] The Council represents the American Bankers Association, the Consumer Bankers Association, Bankers Roundtable, and Independent Bankers Association of America. The Council standards include the following:

---

[173] *Id.* at 731.

[174] Electronic Financial Services Council, *On-line Financial Privacy: Current Legal Framework and Recent Developments*. (1999), at http://www.efscouncil.org/frames/Library/Privacy/EFSCPrivacyIssues.html (last visited on 19 August 2012), § 4.

> Recognition of a customers' expectation of privacy; commitment to the use, collection and retention of customer information only if the institution believes the customer will benefit; maintenance of accurate customer information; limits to employee access to such information; protection of information via established security procedures; restrictions on the disclosure of account information; maintenance of customer privacy in business relationships with third parties; and disclosure of an institutions' privacy policies to the consumer.[175]

The 2000 US FTC Report to Congress found that after years of studies, "online privacy continues to present an enormous public policy challenge … self regulatory initiatives …demonstrate that industry efforts alone have not been sufficient."[176] The FTC recommended additional online consumer protection legislation.

The On-line Privacy Alliance (2003) is a not-for-profit organization of over 80 global companies that agreed to protect information privacy. While the membership is relatively small, the organization adopted some reasonable standards. For membership and certification, a member of the organization must prove that it has instituted a program that includes "(1) Adoption and Implementation of a Privacy Policy; (2) Notice and Disclosure; (3) Choice and Consent (opt-out); (4) Data Security; and (5) Data Quality and Access."[177]

The Australian Direct Marketing Association (ADMA) established a voluntary industry code related to DPSIP issues. The code only relates to Business to Consumer (B2C) activities and integrates some standards in the Privacy Act

---

175 *Ibid*.

176 Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace: A Report to Congress*. (2000), at http://www.ftc.gov/reports/privacy2000/privacy2000.pdf (last visited on 26 July 2012), ii.

177 On-Line Privacy Alliance, *Guidelines for Online Privacy Policies*. (2003), at http://www.privacyalliance.org/resources/ppguidelines.shtml (last visited on 2 August 2012), 1.

of 1988 NPPs and OECD standards. The current privacy protection statement is as follows:

> An integral part of the Code is the National Privacy Principles (NPPs). The NPPs give consumers some control over their personal information by limiting the amount of information that companies can collect about individuals. In addition marketers are required to **inform consumers** who are collecting the information, how the company can be contacted and the **intended usage** of the personal information, including whether it will be disclosed to third parties. Consumers must be given the opportunity [to] **opt-out of future direct marketing approaches and block transfer** of their contact details to any other marketer.[178]

A review of national and interest group DPSIP concerns establish that there are valid concerns and show an interest in establishing standards. Such an approach is laudable; however, the strategy is insufficient to remedy the range of DPSIP problems. National Codes apply only to the nation of origin and do not always have the force of law. Non-governmental codes are industry specific and are voluntary. Most are established to thwart governmental regulation in pro-business governments. Industry and non-governmental codes generally have little to no consumer input and little agreement on the basic principles that need to be addressed. The macro issues are usually ignored and the black letter aspects of the principles are misunderstood or ignored. Such codes have considerable compliance, enforcement mechanisms, monitoring, and sanction powers. Non-governmental codes have no serious redress or remedies. Penalties and sanctions are a matter of ineffectual customs and membership. Peer pressure can be applied but there

---

[178] Australian Direct Marketing Association *The ADMA Direct Marketing Code of Practice*. (2007), at http://www.adma.com.au/asp/index.asp?pgid=1985&cid=10887&id=2196 (last visited on 6 January 2012) at 1. (emphasis added)

is no independent or neutral arbiter. The codes are self serving and do not provide concerns for potential victims or due process.[179]

3.8 International Legal Standards and Guidelines Critique

Modern international treaties relate to DPSIP legal issues and reveal a multinational concern and member consensus. The guidelines provide a legal justification for best practices in law and business; however, the treaties tend to be aspirations and even prescriptive rather than descriptive. The documents certainly declare that the principles are appropriate, ethical, fair, just, and legitimate. Compliance, on a rational personal level, should not be a major issue.[180] Some governments and major corporations are not always rational and behave with a distorted view of self-interest. The major strength and the major weakness of the treaties is that they are based on consensus. The consensus principles have little to no universal enforcement powers. Redress under the treaties is often impossible. The terms of the treaties must be legally operational under national codes and rigorously enforced. The same issues apply to the discussed national and non-governmental organization standards.

The European Directives have established some sound DPSIP legal standards. The Directives certainly need to be technology neutral and periodically updated. The Directives have framed the debate and have been enacted as law in several countries. The privacy laws in AU, CA, the UK, and recent legislation in SA have grown out of the EU Directive approach. Even the recalcitrant US policy has also been modified and improved to some extent.

The APEC Privacy Charter stands in sharp contrast to the EU approach. The standards are more lenient and more pro-business. Some US governmental

---

[179] Graham Greenleaf & Nigel Waters, *Direct Marketing Code of Practice Hits ACCC Snag*. (1998), at http://www.austlii.edu.au/au/journals/PLPR/1998/61.html (last visited on 31 December 2012).

[180] Tom R. Tyler, *Why People Obey the Law* (Princeton University Press. 2006).

officials and some major international corporations favor and are adding pressure to have the Charter become the international standard.

The major strength of the EU approach to DPSIP is that the legal standards are broad in the sense that the standards apply to all economy sectors, all personal data types, and all entities that are involved in data processing. The approach is in contrast to the US, which uses a sectoral approach—putting out privacy brush fires or rearranging the chairs on the deck of the Titanic. The US and the UK pass or reverse standards based on the issue of the moment. Specific data types or entities are allegedly regulated with mixed results.

The EU data protection efforts provide legal force to a number of guidelines. The focus is on harmonizing member states' obtaining and processing personal information. The strategic goal is on convergence.[181] Some advocates ague that the intent was on processing rather than protecting personal information.

One of the first measures of the effectiveness of a law and administrative system is to see if it works. Compliance is always an issue but one would expect governmental agencies to follow the data protection and information privacy law. In the 2008 fiscal year, the UK Ministry of Justice admitted that it had lost the personal data of 45,000 people in nine separate situations, but only six had been announced. The Ministry also announced that there might be other undisclosed cases. The Home Office also reported that it had lost the records of 3,000 seasonal agricultural workers because of the loss of unencrypted compact disks. The HM Revenue and Customs office lost the data of 25 million families in the UK during the same period.[182] The good

---

[181] Colin J. Bennett, *Convergence Revisited: Toward a Global Policy for the Protection of Personal Data?* in *Technology and Privacy: The New Landscape* (Philip Agre & Marc Robinson eds., 1998).

[182] Leo King, *U.K. Justice Agency Lost 45,000 Personal Records in Past Fiscal Year*. (2008, August 18), at http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxono

news was that the system worked to the point that agencies had an obligation to report.

A critical factor in any DPSIP legislation or regulation process involves exceptions. The 1995 EU Directive is a good example. The directive clearly states a set of reasons for not following the directive. Article 13[183] set the exceptions. The exception list included the following:

> (a) national security; (b) defence; (c) public security; (d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions; (e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters; (f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e); (g) the protection of the data subject or of the rights and freedoms of others.[184]

The major problem with such a list of data protection and information privacy law exceptions is clearly documented in Chapter Two and Section 3.4.1 of this thesis. The issue is who watches the exceptions. *Is the fox monitoring the chicken coop*?[185]

Article 25 allows countries to avoid EU Directive requirements. The country could legally avoid the review by sending the data to be processed to a third country.[186]

---

myName=storage_security&articleId=9112864&taxonomyId=153&intsrc=kc_top (last visited on 18 August 2012). at 1.

183 An interesting number for superstitious people in some parts of the world.

184 European Union Directives, *The 95/46/EC Directive*. (1995), at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML (last visited on 4 January 2012), at 6.

185 Foxes sneak into chicken coops and eat the chickens.

186 Graham Pearce & Nicholas Platten, Orchestrating Transatlantic Approaches to Personal Data Protection: A European Perspective, 22 *Fordham International Law Journal*, 5, 2024 (1999).

On 13 December 2004, the European Council passed legislation that requires biometric identification on all passports and travel documents. Technically, the change maintains document authenticity and identifies the holder. Electronically readable fingerprints and a picture *in interoperable formats* are used.[187] All of the resultant data is placed in a massive database of personal information and all travel data.

The action violates fundamental principles of the 95/46/EC Directive and the August 1, 2003, Article 29 Working Party document on biometric data protection. "The Working Party is of the view that most biometric data imply the processing of personal data. It is therefore necessary to fully respect the data protection principles provided for in Directive 95/46/EC taking into account the particular nature of biometrics."[188]

On 15 March 2006, the EU passed Directive 2006/24/EC, which mandates retention of all European communications data. Service providers must collect and give governmental access to the data. The data includes e-mails, faxes, Internet usage, mobile phone calls, party addresses, party names, phone calls, registered users, and subscribers.[189] Article 6 requires member states to pass legislation that mandates that service providers keep the data for at least six months and no longer than two years. The Justice and Home and Justice Councils were not consulted.[190]

---

187 Council of Europe, *Council of Europe's Convention on the Automated Processing of Personal Data* (2004), at http://www2.echo.lu/legal/en/dataprot/counceur/conv.html (last visited on 29 May 2012).

188 Working Party, *Working Document on Biometrics. Article 29 - Data Protection Working Party, 12168/02/EN WP 80*. (2003, August 1), at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp80_en.pdf (last visited on 1 September 2012), at 11.

189 European Union Directives, *Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC*. (2006), at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF (last visited on 4 September 2012), at Article 5, 57.

190 *Id.* at 58.

Behaviorally, the focus of the UK and the EU regarding DPSIP in the US and CA has and is shifting. Rather than continuing legal policies to protect a legal right to control personally identifiable information, the focus is on protection. Protection is being operationally defined as protecting corporate data base proprietors from loss and theft. Part of the problem is political; however, some of the problem is the Nazi-derived "Big Lie" of national security and the fact that the cost of not complying with the 1995 Data Protection Directive is set low.

The issue is compounded by the fact that litigation relief is limited by individual and class action constraints and unconscionable damage requirements. The legal regulators tended to be resistant and noncompliant. Neo-Conservatives in business and government have reframed the issue. Informed consent has been replaced with excessively long, unreadable, and small print opt-out clauses. Over the past ten years, the concept of checks and balances has been abandoned in the UK, EU, and the US with missionary zeal. The George W. Bush administration undermined data protection and information privacy law using Machiavellian techniques and strategies.[191]

On 25 July 2007, the European Data Protection Supervisor (EDPS)[192] concluded that the Data Protection Directive does not need to be amended at this time. However, member states must be more insistent on its implementation. The EDPS opinion declares that no new legal principles are needed and that the wide scope of the law should not change. Class action litigation should be allowed. Law enforcement access must be controlled and justified. Regulations should be easily updated when new technology provides a threat – Radio Frequency Identification (RFID), for example.

---

191 For examples, see § 2.4 of this work.

192 European Data Protection Supervisor, *Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council on the Follow-Up of the Work Programme for Better Implementation of the Data Protection Directive*, Official Journal of the European Union, 27.10.2007, C 255/1 - 14. (2007, July 25), at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2007:255:0001:0012:EN:PDF (last visited on 22 September 2012).

The International Chamber of Commerce[193] held a conference with forty representatives including data protection authorities, EU institutions, governmental authorities, international companies, and law firms. The focus was on the distinction between data controllers and processors. While no firm recommendations were made, the distinction between the two was considered artificial. Some suggested that it be eliminated.

The UK's Information Commissioner's Office issued a number of changes that might be made to the EU Directive-based system. While the Commissioner had aggressive investigation rights, firms could opt-out. Routine audits, similar to those in Ireland, ought to be accomplished. Data Sharing Reviews showed that the UK commission did not have the power to do the tasks effectively. Having a regulatory system that requires the data controllers to consent to be monitored defeats the purpose of the regulation. Investigations should be the same for public and private data controllers. The Commissioner's office should have "simple power to enter premises to conduct an inspection, with appropriate notice requirements and accountability mechanisms to ensure the power is used responsibly."[194] Operational funding should be fee based on the number of "personal data process."[195] The fee would increase if a controller "knowingly or recklessly" provides faulty data or has a data protection violation.

The EU and the UK could profit from one US protective approach. A number of states have enacted strong data breach notification laws. The laws provide DPSIP law protections. The laws also provide a motivation for increased data

---

193 International Chamber Of Commerce, *ICC Task Force on Privacy and the Protection of Personal Data: Summary of the Workshop on the Distinction between Data Controllers and Data Processors*. (2007, October 25), at http://www.iccwbo.org/policy/ebitt/id17704/index.html (last visited on 15 September 2012).

194 Information Commissioner's Office, *The Information Commissioner's Inspection Powers and Funding Arrangements under the Data Protection Act 1998: Response of the Information Commissioner to the Ministry of Justice's Consultation Paper of 16 July 2008*. (2008, August 22), at http://www.ico.gov.uk/upload/documents/library/corporate/notices/response_of_ic_to_moj_consultation_paper.pdf (last visited on 12 September 2012), at 16.

195 *Id.* at 20.

security. The responsibility is placed on the data controller. Some EU experts are suggesting such legislation, but the responsibility would be on the customer – user.[196]

Despite some recent changes, the Data Protection regimen of the EU is classic, and more and more countries outside the Union are adopting similar principles. The task is to make sure that the same mistakes are not made.

The EU data protection and information approach keeps the issues alive. Peter Hustinx, the EU Data Protection Supervisor, addressed some uncomfortable truths. He reports that all companies that collect and use personal data should adhere to the established directives. The pronouncement includes IP addresses because personal data can be extracted. The data can be used for a range of purposes including political profiling and behavioral advertising.[197]

Some member states are passive about implementing the EU Data Protection Directives in practice. Rather than following the spirit and letter of the law, minimal funding and powers are established. The EU has essentially allowed the US to violate basic directive standards. Examples include the transfer of passenger data on flights to the US and allowing personal financial data transferred by the Society for Worldwide Interbank Financial Telecommunication (SWIFT) and the *Safe Harbor* program.

The Directives themselves contain a number of exemptions and exceptions. For example, no controlling principles apply to police or governmental terrorist agencies. History shows that governments and police agencies need checks and balances at least as much as corporations. The EU Directives and APEC Privacy Charter do not address such constraints.

---

196 Miya Knights, *Security Professionals Debate the Recommendations of Independent Research to Introduce Tough European Data Breach and Security Regulations*. (2008, October 9), at http://www.itpro.co.uk/606960/security-pros-call-for-data-breach-regulations (last visited on 11 October 2012).

197 Pinsent Masons, *Hustinx: Nameless Data Can Still Be Personal*, Out-law.com. (2008, June 11), at http://www.out-law.com/page-9563 (last visited on 12 June 2012).

With the exception of the EU Directives, historic and current international agreements have no power to constrain business organizations or large multinational corporations. No effective checks and balances exist to restrain powerful, wealthy, and well-structured organizations from ignoring DPSIP legal standards. Self interest is used to violate privacy principles. Widespread DPSIP standards are directly and indirectly violated in a systematic manner. International law principles must be supplemented by national regulation approaches.

The EU proposal to move to a Data Protection Regulation approach was not without it opponents. Not surprisingly the UK led a group of opponents that included Belgium, Denmark, Hungary, Slovenia, and Sweden. The supporting countries included Bulgaria, France, Germany, Greece, Ireland, Italy, Luxembourg, Netherlands, and Spain.[198]

Speaking at the Data Protection Congress, European Commission Director General for Justice Francoise Le Bail noted, "We need a regulation that is flexible enough to be applied to technological advances that we may have no notion of right now." Article 29 Working Party Chair Jacob Kohnstamm said while there is "always room for improvement," the regulation's applicability across member states is "a big step forward."[199]

3.9 Summary of International Literature and Issues Reviewed

Ancient codes have established long-standing legal principles related to boundaries, confidentiality, personal property, legal responsibility, and redress for personal wrongs. Modern international treaties have codified information privacy rights and obligations. The EU declarations have provided clear privacy and data transfer standards for EU nations and mechanisms for

---

198 Hawtalk, *UK Government Opposed to the Commission's Data Protection Regulation*. (2012), at http://amberhawk.typepad.com/amberhawk/other-information-law/ (last visited on 12 November 2012)

199 *Ibid*.

dealing with third country data standards. The APEC Privacy Charter has provided an anti-DPSIP standard that is a pro-business and self-regulation alternative to the EU approach. Some national and non-governmental standards address DPSIP legal concerns with mixed success.

In the studied countries, the experience shows that compliance with DPSIP legal standards is not consistent. Not all police officers and departments even follow the law. Governmental agencies and business organizations do not always follow the law. The legal standards often make it impossible for individuals and even groups to control or monitor personal data. Institutional checks and balances are limited. The reality is that organizations tend to want to know everything; therefore, limitations are often by-passed. Even the EU Data Protection Supervisor does not have authority over all of the massive databases. Not all countries are complying with the implementation timetables; moreover, many are opposing the system.

A number of historic and recent international legal principles support the rationale and terms related to DPSIP legal principles. However, international agreements are not binding on each signatory. Member states do not always keep promises or implement standards in a consistent, effective, responsible, or vigilant manner. The SA approach to DPSIP laws and regulations does not need to re-invent the wheel. Instead, the SA approach needs to learn from the successes and failures of internationally based DPSIP laws and policies. Benchmarking others' efforts provides a means for the SA to take a step forward in its own legislations and policy and lead the next development of standards for itself and the world.

Chapter Four begins a country analysis of DPSIP legal and policy issues. The AU attempt to meet international standards has some strengths and weaknesses. SA can learn from both.

CHAPTER FOUR: DATA PROTECTION AND SECURITY LAW: AUSTRALIAN LEGAL STANDARDS

> *To the extent that the individual has no control over, and perhaps no knowledge about, the mass of identifiable data which may be accumulated concerning him or her, and to the extent that national law-makers, despite their best endeavours, enjoy only limited power effectively to protect the individual in the global web, privacy as a human right, is steadily undermined.* The Hon Justice Michael Kirby[1]

4.0 Overview

AU is a member of the Commonwealth of Nations and shares a common law tradition with CA, the UK, and the US. AU has passed DPSIP laws in response to the EU Directive. Due to some enacted provisions, AU has not been judged as EU adequate.[2] Despite some less than adequate provisions of the DPSIP approach, AU has enacted some privacy statute provisions that are far more data protective than the standards found in the other countries evaluated in this study.

The AU chapter begins with presenting background on the country. The analysis continues with an examination of the relevant AU Commonwealth Constitutional declarations. AU federal legislation and Commonwealth case

---

[1] The Hon Justice Michael D. Kirby, Privacy in Cyberspace, 21 *University of New South Wales Law Journal* 2, 323-332 (1998), at 323.

[2] European Commission, *Submission to the House of Representatives Committee on Legal and Constitutional Affairs Concerning its Inquiry into the Privacy Amendment (Private Sector) Bill 2000. MARKT/E1//FB/fb D(2000).* (2000), at http://www.aph.gov.au/house/committee/laca/Privacybill/sub113.pdf (last visited on 30 December 2012).

law is examined. The research then focuses on AU State Constitutional declarations, State legislation, and case law. An analysis of the AU implementation system is reviewed. AU sociolegal concerns are presented. A critique of the AU approach is then offered. A summary of the AU literature and issues, using the thesis comparative model of the current legal support is then reviewed and presented.

4.1 Background

Justice Michael D. Kirby summaries the AU view of DPSIP issues. He argues that historically, information privacy has been protected by costs, inconvenience, impermanency, and indexing problems. The privacy concerns of the 1980s have increased due to technical developments that have increased the accessibility, power, storage capacity, and speed of processing. Justice Kirby argues that the right to confidentiality of communications, honor, privacy, and reputation must be protected.[3]

Justice Kirby further proposes a reasonable plan of action. He argues that every jurisdiction must review and debate current DPSIP laws and regulations to avoid a patchwork of ineffective legal efforts. Businesses, governments, and organizations must establish open and transparent privacy standards. National governments need to defend privacy rights, stand firm against commercial resistance, and participate in an international strategy debate.[4]

Justice Kirby argues for enhanced privacy rights, including a right not to be indexed. He advocates for the following rights: grant individuals access to their data, effectively encrypt personal communications, ensure fair treatment, implement human checking of adverse decisions, protect personal information privacy, and understand automated decisions.[5]

---

[3] *Ibid*.
[4] *Ibid*.
[5] *Ibid*.

Paul Keating, former AU Prime Minister, called for major DPSIP changes. He added support for breach legislation, increased powers for the AU Privacy Commissioner, and fines. He argued that privacy is under attack and that the media is failing to respond.[6]

AU is a multi-cultural Commonwealth nation.[7] The majority of the population remains Anglo-Saxon. The culture, customs, language, legal tradition, and manners are similar to CA, the UK, and the US.

AU has a democratically elected government that uses the British Parliamentary system and is a federation similar to the US. The government includes a US format of an executive branch,[8] legislative branch,[9] and judiciary.[10] The legal system is based on the UK and US common law tradition. The structure includes the central government, six state governments, and two Territories.[11] The States and Territories are generally self-governing. Since the passage of the *Australia Act of 1986*,[12] all AU governmental levels have been legally independent of the UK. The government functions on the principle of separation of powers. The Constitution of Australia was approved in 1900 by Queen Victoria.[13] The Constitution does not have a US-style Bill of Rights; rather, the constitution

---

[6] Adam Carey, *Fine Breaches of Privacy: Keating* The Sydney Morning Herald. (2010), at http://www.watoday.com.au/national/fine-breaches-of-privacy-keating-20100804-11fny.html (last visited on 5 August 2012).

[7] Australian Government, *Australian Government*. (2010), at http://australia.gov.au/ (last visited on 5 August 2012). Site contains reference data for this section.

[8] Government of Australia, *Prime Minister of Australia*. (2010), at http://www.pm.gov.au/ (last visited on 5 August 2012).

[9] Government of Australia, *Parliament of Australia*. (2010), at http://www.aph.gov.au/ (last visited on 5 August 2012).The legislative branch includes a House of Representatives and a Senate.

[10] Government of Australia, *High Court of Australia*. (2010), at http://www.hcourt.gov.au/ (last visited on 5 August 2012). See http://www.hcourt.gov.au/legal_04.html for links to all courts

[11] The States include New South Wales, Victoria, Queensland, Tasmania, South Australia, and Western Australia. The Territories include the Australian Capital Territory (the national seat of government - Canberra) and the Northern Territory. Only Queensland has a uni-cameral parliament.

[12] Includes the Parliament of Australia Act (No. 142 of 1985) and the Parliament Act of the United Kingdom c.2 1986) see http://www.statutelaw.gov.uk/content.aspx?activeTextDocId=1330183

[13] *Commonwealth of Australia Constitution Act 1900 (Imp), 63 & 64 Victoria, c 12 (Imp.)* (1900). (AU)

authors thought that the Parliamentary system would sufficiently protect any such issues addressed by the US Bill of Rights.

In 2004, the Australian Capital Territory passed the first *Human Rights Act*. Section twelve of the Act declares that "Everyone has the right, (a) not to have his or her privacy, family, home or correspondence interfered with unlawfully or arbitrarily; and (b) not to have his or her reputation unlawfully attacked."[14] In 2006, the State of Victoria passed the *Charter of Human Rights and Responsibilities Act* which is a Human Rights law. Section thirteen, Privacy and Reputation, incorporates the language of the Australian Capital Territory Act.[15] The Australian Human Rights Commission was established by the federal Parliament as an independent statutory organization that reports to the Attorney-General. The Commission addresses human rights and related discrimination issues.[16]

In 2009, at the request of the AU States, The Commonwealth government passed The National Credit Protection Act. The Act was a federal recognition that some personal information needs to be protected and regulated.[17] The Act replaced the state Uniform Consumer Credit Codes and it licenses credit information services organizations, provides violation sanctions, increases enforcement powers, and expands consumer protections.

---

[14] Australian Capital Territory, *Human Rights Act 2004*. (2004, amended 2010), at http://www.legislation.act.gov.au/a/2004-5/current/pdf/2004-5.pdf (last visited on 27 July 2012). (AU)

[15] State of Victoria, *Charter of Human Rights and Responsibilities Act 2006*. (2006, amended 2010), at http://www.austlii.edu.au/au/legis/vic/consol_act/cohrara2006433/ (last visited on 27 July 2012). (AU)

[16] Australian Human Rights Commission, *About the Commission*. (2010), at http://www.hreoc.gov.au/about/index.html (last visited on 27 July 2012).

[17] Australian Government, *National Consumer Credit Protection Act*. (2009), at http://www.treasury.gov.au/consumercredit/content/legislation.asp (last visited on 26 July 2012). (AU) The actual code is at http://www.comlaw.gov.au/ComLaw/Legislation/Act1.nsf/0/151D9CCDD6F2FAC1CA25768E001B64CC?OpenDocument

4.2 Australian Commonwealth Constitutional Declarations

The AU Constitution does not enumerate a clear privacy right. The document does grant the Commonwealth powers to address DPSIP legal issues. The parliament has the "power to make laws for the peace, order, and good government."[18] DPSIP-related sections include trade and commerce, telecommunications, intellectual property, external affairs, and property acquisition.[19]

4.3 The Australian Commonwealth Legislation

The *Australian Privacy Act of 1988*[20] was the government's compliance response to Article 17 of the 1966 *International Covenant on Civil and Political Rights*.[21] The legislators used concepts noted in international standards as a guide.[22] The Act failed to create a general right of privacy in AU law but does protect personal information held by the Commonwealth, and it requires the appointment of a Privacy Commissioner. Commercial information, other than credit information, was excluded until the Act was amended.

The *Privacy Act of 1998* was the first AU data privacy regulation. The Act establishes eleven Information Privacy Principles (IPPs) but only applies to

---

[18] Parliament of Australia, *Commonwealth of Australia Constitution Act as amended*. (2003), at http://www.aph.gov.au/senate/general/constitution/par5cha1.htm (last visited on 7 January 2012). Chpt. 1, part V, § 51. (AU)

[19] *Ibid*.

[20] *Privacy Act of 1988 (Cwlth)* amend. Act No. 119 of 1988, Act No. 102 of 2009 (1988). (AU)

[21] United Nations, *International Covenant on Civil and Political Rights, (ICCPR). Article 17*. (1966), at http://www2.ohchr.org/english/law/ccpr.htm (last visited on 20 August 2012). See Chapter 3 § 3.3.4 for additional information.

[22] See OECD, *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*. (1980), at http://www.olis.oecd.org/horizontal/oecdacts.nsf/linkto/C(80)58 (last visited on 22 January 2012); United Nations, *Guidelines Concerning Computerized Personal Data Files. Adopted by the General Assembly on 14 December 1990.* (1990b), at http://ec.europa.eu/justice_home/fsj/privacy/instruments/un_en.htm (last visited on 3 January 2012); Council of Europe, *Resolution (73) 22 on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector*. (1973), at http://www.coe.int/t/e/legal_affairs/legal_co%2Doperation/data_protection/documents/international_legal_instruments/Resolution (73)22_EN.pdf (last visited on 20 January 2012).

governmental offices as they relate to natural persons. The IPPs address three general areas of concern. The first area relates to the government's collection, disclosure, storage, and use of personal information. The second allows people access to governmental information about themselves. The third area is a right for people to request changes in the information. The principles include the following:

IPP 1: Manner and purpose of collection—The information must be necessary for the agency's work, as well as collected fairly and lawfully.

IPP 2: Collecting information directly from individuals—An agency must take steps to tell individuals why they are collecting personal information, what laws give them authority to collect it, and to whom they usually disclose it.

IPP 3: Collecting information generally—An agency must take steps to ensure the personal information it collects is relevant, up-to-date, complete, and not collected in an unreasonably intrusive way.

IPP 4: Storage and security—Personal information must be stored securely to prevent its loss or misuse.

IPP 5: Information relating to records kept by record-keeper—Nature and purpose of the records, class of people, period of time kept, and access.

IPP 6: Access to records containing personal information—Except when limited by law or authorized by the courts.

IPP 7: Alteration of records containing personal information—Records should be accurate, not misleading, and held for the stated purpose. Data can be amended or corrected if wrong.

IPP 8: Use only accurate, up-to-date, and complete information.

IPP 9: Use information for a relevant purpose.

IPP 10: Basic rules about using and disclosing—Consent must be informed and free but may be implied or express.

> IPP 11: Disclosure—An agency may disclose personal information to someone else but only in special circumstances, such as with the individual's consent or for some health and safety or law enforcement reasons.[23]

Over the next few years, the AU Commonwealth passed a number of sectoral acts. The *Data-Matching Program (Assistance and Tax) Act 1990* established an office in the Office of the Privacy Commission to monitor the government's data-matching program.[24] The Commission was given power to investigate, evaluate, and supervise Privacy Act compliance. The Commission can also issue reports on damages and losses related to breaches of privacy principles.

The *Credit Reporting Code of Conduct of 1991* extended DPSIP concerns to the private sector. The Act established legal requirements for credit reports, reporting credit worthiness, and legitimate processing activities. Credit reporting agencies are bound to adhere to the privacy principles.[25] The principles relate to collection, use, disclosure, data quality, data security, openness, access, correction, identifiers, anonymity, transborder data flows, and sensitive information.[26] Restricted criminal offenses can be charged for false, misleading, or unauthorized access.

AU credit reports are limited to data related to credit worthiness. Data on affiliations or beliefs related to political, religious, or social information are not allowed. Collecting and reporting data on ethnic or national origin and race classifications are prohibited. Data on sexual preferences or practices are restricted. Criminal or medical history is not recorded or shared. Physical handicaps are not allowed to be noted. The law also prohibits the processing

---

[23] Australian Office of the Federal Privacy Commission, *Information Privacy Principles*. (2009), at http://www.privacy.gov.au/materials/types/law/view/6892 (last visited on 27 December 2012).
[24] *Id.* at http://www.privacy.gov.au/aboutprivacy/history
[25] See the modifications in the *Amendment Acts of 2000* noted in this section.
[26] *Id.* at http://www.privacy.gov.au/materials/types/infosheets/view/6583

of information on character, lifestyle, or reputation.[27] The AU approach is far more protective than the standards in CA and the US.

Section 135AA of the *National Health Act of 1991* and amendments established that the Privacy Commissioner had oversight of health information guidelines for data collected by the government through its Medicare and Pharmaceutical Benefits schemes. Agencies were required to inform the Commissioner of data collection activities; persons can file a grievance with the Commission for alleged breaches. The guidelines establish that Medicare and Pharmaceutical benefit data can not be stored together. The Act provides for occasions when data from the programs can be linked or re-linked.

The Commonwealth *1997 Telecommunication Act* gives the Privacy Commissioner power over disclosure of customer data held by telecommunication carriers and service providers. Interception of telecommunication system communications is prohibited. The Commissioner must be consulted on all codes and standards related to privacy. The Act allows the establishment of industry privacy codes and standards that can not derogate from the 1988 Privacy Act.[28]

Under the guidelines, public interest can trump individual privacy concerns in certain situations. The situations include "criminal matters, public health or safety, consumer affairs/protection, matters of politics, government and public administration, matters relating to the conduct of organizations, such as corporations, businesses and trade unions, which impact on the public, and seriously anti-social conduct which causes harm to others."[29]

---

[27] Australian Government Office of the Privacy Commissioner, *Credit Reporting Fact Sheet 7: Credit Reporting Databases (May 1996)*. (2009), at http://www.privacy.gov.au/materials/types/factsheets/view/6494 (last visited on 16 February 2012).

[28] *Id.* at Sec. 116A at http://www.austlii.edu.au/au/legis/cth/consol_act/ta1997214/s116a.html

[29] Australian Communications and Media Authority, *Privacy Guidelines for Broadcasters* (Australian Communications and Media Authority. 2005) at 3.

Section eighteen of the *Spam Act of 2003* addressed information privacy concerns. The Act required an opt-in requirement for direct marketing and all commercial electronic messages. However, the 1988 Privacy Act only required an opt-out approach.[30]

The *Market and Social Research Privacy Code* of 2003 and 2007 clarified industry-specific privacy standards. The purpose of the code was to protect information privacy data subjects as well as enable accurate and quality data processing standards for commercial, governmental, and not-for-profit organizations. The code extended standards to operations not previously covered by the 1988 Privacy Act. Under the code, research organizations can collect information only for the stated purpose, data subjects can refuse to participate, and the organizations' actions must be fair, legal, and reasonable. Informed consent is required. "A research organization must not use, disclose or transfer identified information (including information received from another organisation) for any purpose other than a research purpose."[31] The data must be accurate, complete, and up-to-date. Data security standards are required to protect the data from loss, misuse, unauthorized access, disclosure, modification, and transfer.[32] The organization's standards must be transparent and interested parties must be granted access. When information is retained, provisions are required for access, destruction, deletion, and de-identification. The Privacy Commissioner has the power to approve the Code.

The *Privacy Amendment (Private Sector) Act of 2000* extended DPSIP standards to private businesses. The Act reaffirmed the 11 privacy principles of the 1988 Privacy Act and establishes ten National Privacy Principles (NPPs) for the commercial sector. The Act addressed anonymity, disclosure, management of personal data, offshore transmissions, and use. The purpose

---

[30] Office of the Privacy Commissioner, *SPAM Act 2003 Review* (Office of the Privacy Commissioner. 2006). For an analysis of the issue, see Chapter 2, Section 2.7.2

[31] Commonwealth of Australia Law, *Market and Social Research Privacy Code*. (2003), at http://www.comlaw.gov.au/comlaw/legislation/legislativeinstrument1.nsf/framelodgmentattachments/0671CDE24C557D58CA257309000A399E at 2.1. (last visited on 29 December 2012).

[32] *Id*. at 4.3.

is to establish a single comprehensive approach for collecting, correcting, disclosing, holding, and transferring personal information that met international DPSIP concerns. The *Privacy Amendment (Private Sector) Act of 2000* attempted to balance privacy issues, human rights, social interests, and business objectives.[33] Neo-Conservative special interests prevailed with the business community advocating for a significant small-business exemption from the Act.[34] The exemption was adopted and covered ninety-four percent of all AU businesses.[35]

The *Privacy Amendment (Private Sector) Act of 2000* provided a definition of sensitive information that warranted data protections. The list included "information or an opinion about an individual's racial or ethnic origin; or political opinions; or membership of a political association; or religious beliefs or affiliations; or philosophical beliefs; or membership of a professional or trade association; or membership of a trade union; or sexual preferences or practices; or criminal record; that is also personal information; or health information about an individual."[36]

Schedule 3 of the Act established ten NPPs. The Principles included the following:

NPP 1. Collection—data collection must have a purpose, be legal, fair, not unreasonably intrusive, and provide notice to the data subject.

NPP 2. Use and disclosure—organizations can only use or disclose personal data for a stated purpose, must obtain consent, the data must not be sensitive, must be lawful, reasonable, and provide written notice. The organization must meet a standard of responsibility.

---

[33] Commonwealth of Australia, *Privacy Amendment (Private Sector) Act 2000. Act - C2004A00748*. (2000), at http://www.comlaw.gov.au/ComLaw/Legislation/Act1.nsf/0/3E8F716C0779E822CA256F72000B40F8?OpenDocument at § 3. (last visited on 29 December 2012).

[34] This self-interest advocacy resulted in AU not being compliant with the EU data protection directive.

[35] Graham Greenleaf, Reps Committee Protects the 'Privacy- Free Zone", 7 *Privacy Law and Policy Reporter 1*, 1 (2000).

[36] *Id.* at § 27 (6.1).

NPP 3. Data quality—organizations must take reasonable steps to insure that the data is accurate, complete, and up-to-date.

NPP4. Data security—organizations must provide reasonable protection from unauthorized access, modification, or disclosure, and destroy or de-identify when no longer needed or used.

NPP 5. Openness—organizations must provide transparency related to information held, collected, used, or disclosed.

NPP 6. Access and correction—individual access to personal data is required except when the data is commercially sensitive, and individuals are entitled to reasons for any denials.

NPP 7. Identifiers—organizations must not use agency or governmental identification codes or disclose the same. Tax numbering systems were exempt.

NPP 8. Anonymity—wherever it is legal and practicable, persons can refuse to identify themselves when transacting business with the organization.

NPP 9. Transborder data flows—Organizations may not transfer data to other countries unless they believe the recipient follows privacy principles, the individual consents to transfer; the transfer is contractually necessary, benefits the person, the notice or consent is impracticable or assumes the person would consent if given the option, and the transfer is reasonable.

NPP 10. Sensitive information—organizations can not collect data unless a competent person consents; the data is required by law, prevents an imminent threat to life or health, and unless the organization is non-profit, and the data includes certain relevant health information. A non-profit organization includes organizations that address only racial, ethnic, political, religious, philosophical, professional, trade, or trade union aims.[37]

[37] Commonwealth of Australia, *Privacy Amendment (Private Sector) Act 2000. Act - C2004A00748*. (2000), at http://www.comlaw.gov.au/ComLaw/Legislation/Act1.nsf/0/3E8F716C0779E822CA256F72000B40F8?OpenDocument (last visited on 29 December 2012). (AU)

The *Privacy Amendment (Private Sector) Act of 2000* also established a *co-regulatory process* where businesses can institute different codes of practice at will. The Act itself and its broad and unregulated exemptions do not meet the EU standards for adequate protections.[38] The issues are related to the employee and small business exemptions, generally available exemptions, lack of data export standards, no correction rights of persons in other countries, business-oriented data sharing with no options, transparency restrictions, and industry enforcement issues.[39]

The Act exempted all small businesses. A small business is defined as one that has less than an annual turnover of $3 million AU dollars. The only exceptions to the exemption are those that provide health services or information, collect or disclose information from or to a third party, have a service contract with the Commonwealth, or are regulated by other legislation. Governmental archives, including libraries, media organizations, and political parties are also exempt.[40]

The Act provided for obtaining consent of the data subject to collect and use personal information. However, a major exemption to the law applied to direct marketing activities and marketing organizations. Marketing companies can essentially collect and use personal information as they want.

Complaints can be handled in two different ways. When no approved private code appears with a resolution clause, the Privacy Commissioner can hear the complaint and charge a service fee.[41] The Commission can conciliate or make determinations regarding damages, loss, or redress. The Federal Court can re-hear the complaint on the merits. When a privacy code does exist, the

---

[38] European Commission, *Submission to the House of Representatives Committee on Legal and Constitutional Affairs Concerning its Inquiry into the Privacy Amendment (Private Sector) Bill 2000. MARKT/E1//FB/fb D(2000)*. (2000), at http://www.aph.gov.au/house/committee/laca/Privacybill/sub113.pdf (last visited on 30 December 2012).

[39] *Ibid*.

[40] *Id.* at 6C, 6D-6EA, 7B(4) AD 7C.

[41] The approach provides some income to support operational costs but raises some issues related to governmental commitment to the issue. Self-funding raises issues around the rule of law and the independence of the Privacy Commission.

resolution is conducted by the body identified in the privacy code. If the defendant does not comply, the Federal Court can hear the case *de novo*. The privacy code can be developed by a specific industry sector, industry body, or be developed by an individual or organization that seeks an activity or information code.

The Privacy Commission has the power to conduct privacy audits.[42] The Commissioner can "conduct audits of records of personal information maintained by agencies for the purpose of ascertaining whether the records are maintained according to the Information Privacy Principles."[43] The power includes entry into premises with permission or a court-ordered warrant.[44]

The Privacy Amendment Act of 2004 amended the 1988 Privacy Act. The 2004 Act extended privacy protections to non-AU citizens.[45]

Under AU law, when the Privacy Act does not apply, alternative legal principles can be used to protect information privacy. The alternative principles include violations of computer crime legislation, confidentiality, contract law, conversion, corporation law, and defamation. Appropriate actions can also be brought under intellectual property law when behavior violates protected areas of the trade practices act, telecommunication statutes, and even trespass laws.

On 19 October 2011, a change was made to the administrative function of privacy and freedom of information policies. The Governor-General approved an amendment transferring the functions from the office of the Prime Minister and cabinet to the Attorney-Generals department. The function is now known

---

[42] After the questionable act.

[43] *Privacy Act of 1988 (Cwlth)* amend. Act No. 119 of 1988, Act No. 102 of 2009 (1988). (AU) at § 27(1)(h).

[44] The Commission does not have independent authority to act.

[45] Commonwealth of Australia, *Privacy Amendment Act of 2004*. (2004), at http://www.austlii.edu.au/au/legis/cth/consol_act/paa2004188/sch1.html (last visited on 29 December 2012). The Act was necessary for AU to comply with §25 of the EU Directive. (AU)

as the Information Law and Policy Branch.[46] Perhaps such a change may reduce some political influences.

4.4 Australian Commonwealth Case Law

Before examining the national common or case law on DPSIP legal issues, it is important to examine the power and reality constraints on the highest court in the jurisdiction. AU courts have traditionally followed the British common law tradition. A discussion without a common benchmark would be meaningless. A legal declaration without exploring and understanding the de facto influences is myopic. The US Supreme Count was selected as the benchmark for this study because, in theory, it represents the international standard in the rule of law, balance of powers, and political independence analysis. Granted, there is evidence that the benchmark Court has been inconsistent.

Table 4.0 Comparison of Australian and United States Supreme Court

Factor	High Court of Australia[47]	US Supreme Court[48]
Established	1903	1789
Power of decisions	Applies to all courts and jurisdictions in the country	Applies to all courts and jurisdictions in the country
Membership	One Chief Justice and six justices.	One Chief Justice and eight associate justices (currently)
Appointee Background	Leading appellate courts judges or lawyer.	Leading appellate courts judges, politicians, and law professors.
Term of Office	Retire at the age of seventy	Life or until retires.

[46] Australian Government Department of the Prime Minister and Cabinet, *Administrative Arrangements*, Australian Government (2012 October), at http://www.dpmc.gov.au/privacy/causeofaction/ (last visited on 20 October 2012).

[47] World Wide Legal Information Association, *Legal Resources*. (2010), at http://www.wwlia.org/LegalResources.aspx (last visited on 4 July 2012). See also High Court Of Australia, *About the Court*. (2010), at http://www.hcourt.gov.au/about.html (last visited on 5 July 2012).

[48] Kermit L Hall, *The Oxford Companion to the Supreme Court of the United States* (Oxford University Press 2nd. ed. 2005). See also Supreme Court of the United States, *About the Supreme Court*. (2010), at http://www.supremecourt.gov/ (last visited on 5 July 2012).

Jurisdiction	Original and appellate	Original and appellate
Role	Error-correction	Error-correction
Operations	Hears oral arguments but relies heavily on arguments presented in written briefs	Hears oral arguments but relies heavily on arguments presented in written briefs
Decisions	Varies based on the number of justices hearing a case. The majority decision prevails. A full court is two or more justices. A full bench is all members.	Opinion of the majority, written by one justice, and concurring and dissenting opinions of other justices.
Judicial Review	Recent	Historic since Marshall.
Appointment	Governor-General of Australia with advice.	President nominates, Senate confirms.
Representation	Consultation with political factors.	Recently more political
Opinions	Reference cases - Can render advisory opinions	No advisory opinions
Case Assignment	Court has discretion on selected cases.	Court determines what cases it will hear based on writ of certiorari. Since 1925, has discretionary docket control.

The AU federal courts have addressed DPSIP issues in a limited manner. In *Victoria Park Racing & Recreation Grounds Co Ltd v Taylor,*[49] the AU High Court ruled that, in a public area, it is legal to photograph a person with or without the person's knowledge or permission. AU has no common law tort of invasion of privacy. The court did suggest that contract law and tort negligence standards could be used to protect information privacy rights.

[49] *Victoria Park Racing & Recreation Grounds Co Ltd v Taylor*, HCA 45; (1937) 58 CLR 479, (26 August 1937). at 496. (AU) Reaffirmed in *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd*, (2001) HCA 63; 208 CLR 199; 185 ALR 1; 76 ALJR 1, (15 November 2001). (AU)

In *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd.*,[50] Justice Callinan argues that an invasion of privacy tort should be considered in AU; however, the effort should respect the role differences between the court and legislature.[51] While the Court did not reverse *Victoria Park*, no member suggested that the finding eliminated a possible privacy tort. Chief Justice Gleeson was concerned about definitional issues and a possible tension between privacy and free speech.[52] Justices Gummow and Hayne agreed that the Victoria Park decision did not eliminate a privacy cause of action.[53] Justice Kirby argued that because one of the parties was a corporation it was not reasonable to rule on a privacy issue.[54] Privacy relates to human individuals only.[55] Justices Gaudron, Gummow, and Hayne concurred.[56] The AU courts have the opportunity to create a tort cause of action or can re-define the breach of confidence principles.[57]

4.5 Australian State Constitutional Declarations

The Constitutions of the States of AU follow the general Federation principle of providing an operational manual while trusting the parliament to protect civil liberties, human rights, and DPSIP legal concerns. The Constitutions of New South Wales,[58] Queensland,[59] South Australia,[60] Tasmania,[61] Victoria,[62] and

---

[50] *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd*, (2001) HCA 63; 208 CLR 199; 185 ALR 1; 76 ALJR 1, (15 November 2001). (AU)
[51] *Ibid*.
[52] *Id.* at 325-326.
[53] *Id.* at 248-249.
[54] The argument addresses the schizoid position of the US granting corporation status as a person deserving special treatment over natural persons. Yet, corporations have more protections than natural persons politically and legally (i.e., trade secrets and intellectual property protections).
[55] *Id.* at 279.
[56] *Id.* at 256-258.
[57] See *Lange v Australian Broadcasting Corporation*, 189 CLR 520., (1997). (AU)
[58] New South Wales, *Constitution Act 1902, Act 32 of 1902*. (1902), at http://www.austlii.edu.au/au/legis/nsw/consol_act/ca1902188/ (last visited on 16 February 2012). (AU)
[59] Queensland, *Constitution of Queensland 2001, Act No. 80 of 2001*. (2001), at http://www.legislation.qld.gov.au/LEGISLTN/ACTS/2001/01AC080.pdf (last visited on 16 February 2012). (AU)

Western Australia[63] do not have a Bill of Rights or any guiding standards that independently support DPSIP legal intervention.

4.6 Australian State Legislation

The States of AU have adopted different strategies related to DPSIP legal approaches. Some states have adopted the international approach to data protection whereas others have developed a more limited approach. The approach of each state and territory is explored.

4.6.1 New South Wales (NSW)

The New South Wales (NSW) *Privacy Committee Act of 1975* was enacted prior to the establishment of the OECD and EU Directive guidelines. The Act established a process for complaints resulting in investigations in both the private and public sectors. The committee does not have enforcement or regulatory powers. Members function as ombudsmen and serve on a part-time basis. The Act was subsequently repealed and replaced with legislation providing stronger protection.[64] These Acts will b discussed below.

---

[60] South Australia, *Constitution Act 1934*. (1934), at http://www.legislation.sa.gov.au/LZ/C/A/CONSTITUTION%20ACT%201934/CURRENT/1934.2151.UN.PDF (last visited on 16 February 2012). (AU)

[61] Tasmania, *Constitution Act 1934, Act 94 of 1934; Royal Assent 14 January 1935*. (1934), at http://www.austlii.edu.au/au/legis/tas/consol_act/ca1934188/ (last visited on 16 February 2012). (AU)

[62] Victoria, *Constitution Act 1975, No. 8750 of 1975. Version incorporating amendments as at 1 January 2010*. (1975), at http://www.legislation.vic.gov.au/Domino/Web_Notes/LDMS/PubLawToday.nsf/a12f6f60fbd56800ca256de500201e54/4C214C9ECF03BDFFCA257695000AFCAC/$FILE/75-8750a194.pdf (last visited on 16 February 2012). (AU)

[63] Western Australia, *Constitution Act 1889* (1889), at http://www.austlii.edu.au/au/legis/wa/consol_act/ca1889188/ (last visited on 16 February 2012). (AU)

[64] New South Wales, *Privacy Committee Act of 1975*. (1975), at http://www.worldlii.org/int/other/PrivLRes/1995/3/51_2_1.html (last visited on 7 January 2012). See § 4.6.1.1 of this chapter. (AU)

4.6.1.1 NSW Privacy and Personal Data Protection Act 1998

The *NSW Privacy and Personal Data Protection Act 1998*[65] replaced the *Privacy Committee Act of 1975* and established public sector regulations for personal information and legally binding documents. Personal information is defined as information or an opinion about a person whose identity is apparent or can be reasonably ascertained including body samples, fingerprints, genetic information, or retina prints of those who are alive or have been dead for less than thirty years. Information that is in a publicly available publication, is excluded.[66]

Under the Act, public agencies can collect personal data only when the purpose is lawful and the data is "reasonably necessary for that purpose."[67] Before or after the data collection the person must be informed about the following:

> (a) the information that is being collected,
> (b) the purposes for which the information is being collected,
> (c) the intended recipients of the information,
> (d) whether the supply of the information by the individual is required by law or is voluntary, and any consequences for the individual if the information (or any part of it) is not provided,
> (e) the existence of any right of access to, and correction of, the information,
> (f) the name and address of the agency that is collecting the information and the agency that is to hold the information.[68]

The data may not be kept for longer than necessary for the purpose, must be disposed of securely, and be protected from improper access, disclosure,

---

[65] New South Wales, *Privacy and Personal Data Protection Act 1998* (1998), at http://www.austlii.edu.au/au/legis/nsw/consol_act/papipa1998464/ (last visited on 7 January 2012). (AU)
[66] *Id.* at Part 1, 3(4).
[67] *Id*. at Part 2, Division 1, 8(1).
[68] *Id.* at Part 2, Division 1,10(a-f).

misuse, modification, and use. Unauthorized use or disclosure is unlawful.[69] Exemptions are allowed for law enforcement, investigative agencies and authorized or specialized boards or commissions.

The *NSW Privacy and Personal Data Protection Act 1998* creates an appointed Privacy Commissioner and staff. The Commission functions, with the right of a Tribunal appeal, to perform the following duties:

(a) promote the adoption of, and monitor compliance with, the information protection principles,
(b) prepare and publish guidelines relating to the protection of personal information and other privacy matters, and to promote the adoption of such guidelines,
(c) initiate and recommend the making of privacy codes of practice,
(d) provide assistance to public sector agencies in adopting and complying with the information protection principles and privacy codes of practice,
(e) provide assistance to public sector agencies in preparing and implementing privacy management plans in accordance with section 33,
(f) conduct research as well as collect and collate information about any matter relating to the protection of personal information and the privacy of individuals,
(g) provide advice on matters relating to the protection of personal information and the privacy of individuals,
(h) make public statements about any matter relating to the privacy of individuals generally,
(i) conduct education programs and disseminate information for the purpose of promoting the protection of the privacy of individuals,
(j) prepare and publish reports and recommendations about any matter (including developments in technology) that concerns the need for (or the desirability of) legislative, administrative, or other action in the

[69] *Id*. at Part 2, Division 1, 12(a-d).

interest of the privacy of individuals,

(k) receive, investigate, and conciliate complaints about privacy-related matters (including conduct to which Part 5 applies),

(l) conduct such inquiries and make such investigations into privacy-related matters as the Privacy Commissioner thinks appropriate.[70]

4.6.1.2 NSW Criminal Records Act of 1991

The NSW Criminal Records Act of 1991[71] establishes some privacy protections regarding spent convictions (i.e. convictions that can be effectively ignored after a specified amount of time under a country's law).[72] A person with a spent conviction "is not required to disclose to any other person for any purpose information concerning the spent conviction, and a question concerning the person's criminal history is taken to refer only to any convictions of the person which are not spent."[73] A "person's character or fitness is not to be interpreted as permitting or requiring account to be taken of spent convictions."[74]

The *Criminal Records Act of 1991* makes it illegal for a person without lawful authority to disclose any information related to spent convictions. Anyone who dishonestly or fraudulently attempts to obtain or obtains information on a spent conviction is guilty of an offense.[75]

---

[70] *Id.* at Part 2, Division 2, 36(2)(a-l). The Commissioner is not totally independent from an economic or political perspective.

[71] New South Wales, *Criminal Records Act of 1991 (NSW)*. (1991), at http://www.austlii.edu.au/au/legis/nsw/consol_act/cra1991167/ (last visited on 7 January 2012). (AU)

[72] *Id.* at Part 2(7)(a-d) A spent conviction does not include a prison sentence of more than 6 months, sexual offenses, convictions against the bodies corporate or those prescribed by regulation. The culture and history of AU respects its convict history but also recognizes civil liberty, civil rights, and human rights issues.

[73] New South Wales, *Criminal Records Act of 1991 (NSW)*. (1991), at http://www.austlii.edu.au/au/legis/nsw/consol_act/cra1991167/ (last visited on 7 January 2012). at Div. 1, 12 (a-b). (AU)

[74] *Id.* at (cii).

[75] *Id.* at at Div. 1, 13-14. From a behavioral science and therapeutic jurisprudence perspective such a position is warranted.

4.6.1.3 NSW Health Records and Information Privacy Act of 2002

The *Health Records and Information Privacy Act of 2002* establishes privacy standards for NSW health information. The focus includes the state and local government, health care providers, private persons, and organizations in NSW. The Act establishes 15 health privacy principles (HPPs).[76]

The HPPs require that data collection must be lawful and directly related to its purposes. The data must be accurate, relevant, not excessive, and up-to-date. The data must be collected directly unless it is impracticable or unreasonable. Informed consent principles apply. Data storage must be secure, and data must be appropriately disposed of and may not be kept longer than necessary. The data processing must be transparent, accessible, correct, and accurate. Use of the data must be limited to the purpose for which it was collected or directly related to that purpose. Disclosure is limited to the purpose of the collection. Identification numbers can only be used when reasonably necessary for the particular function. Health services data can be provided anonymously when lawful and practicable. The *Health Records and Information Privacy Act of 2002* restricts the transfer of data outside of NSW. Any linkage or transfer of data to other organizations must include expressed consent.[77] The Act does not apply to small businesses excepted by the federal Privacy Act.

4.6.2 Northern Territory (NT)

The *Information Act of 2002* (NT) integrates archive and record management practices, the freedom of information, and privacy principles. The Act creates the post of the Information Commissioner but only applies to public agencies. This Act defines and establishes special standards for processing sensitive

[76] New South Wales, *Health Records and Information Privacy Act of 2002 (NSW).* (2002), at http://www.informationcommissioner.nsw.gov.au/lawlink/privacynsw/ll_pnsw.nsf/pages/PNSW_03_hripact (last visited on 1 January 2012). (AU)

[77] *Ibid.*

personal information. Sensitive personal information is defined as data concerning:

> racial or ethnic origin; political opinions; membership of a political association; religious beliefs or affiliations; philosophical beliefs; membership of a professional or trade association; membership of a trade union; sexual preferences or practices; a criminal record; or health information.[78]

The Act does not create or give rise to a "cause or action or create a legally enforceable right" and does not create "a criminal liability or make a person liable to be prosecuted."[79] In essence, this Act is little more than a resolution or statement of best practices.

When a conflict exists between established information privacy principles and the Act, the Act will prevail. The actual schedule of the information privacy principles are the same as the ten NPPs of the Commonwealth Acts described previously.

The *Criminal Record (Spent Conviction) Act of 1992* (NT)[80] is very similar to the *NSW Criminal Records Act*. One difference is the criminal record definition. This Act defines the exception as "a sexual offence; an offence by a body corporate; or a prescribed offence."[81] The Act provides the same privacy protections as the *NSW Criminal Records Act* noted above.

---

[78] Northern Territory of Australia, *Information Act 2002 amend 2009 (NT)*. (2002), at http://www.austlii.edu.au/au/legis/nt/consol_act/ia144.txt (last visited on 8 January 2012). at 8. (AU)

[79] *Id.* at 11.

[80] Northern Territory of Australia, *Criminal Records spent Convictions) Act 1992 (NT)*. (1992), at http://www.austlii.edu.au/au/legis/nt/consol_act/crca368/ (last visited on 8 January 2012). (AU)

[81] *Id*. at 6.

In 2007, NT passed the *Surveillance Devices Act*,[82] which prohibits the communication and publication of private activities and conversations based on direct or indirect use of unlawful devices. The Act even applies to police officers who function without a valid warrant.

4.6.3 Queensland (Qld)

In 1971, the State of Queensland passed its first privacy law—the *Invasion of Privacy Act*, which addresses issues related to credit reporting agencies and listening devices that can simultaneously listen, monitor, overhear, or record intended private conversations. This act prohibits the communication or publishing of any data from a listening device. The information is inadmissible in any civil or criminal proceeding. Advertising such devices is also illegal. The *Invasion of Privacy Act* further makes it an offense to enter a dwelling house unlawfully.[83] Qld has recognized an invasion of privacy tort, at least on a District level.[84]

The *Information Privacy Act of 2009* (Qld) applies to personal information handled by Qld governmental agencies and the majority of statutory government-owned corporations. The Act incorporates the eleven IPPs and the NPPs of the federal AU Privacy Act. The intention of this Qld act is to provide "safeguards for the handling of personal information in the public sector environment, and to allow access to and amendment of personal information."[85]

---

[82] *Surveillance Devices Act of 2007 (NT AU)*. (2007), at http://www.austlii.edu.au/au/legis/nt/consol_act/sda2007210/ (last visited on 12 February 2012). (AU)

[83] Queensland, *Invasion of Privacy Act 1971 (Qld)*. (2002), at http://www.legislation.qld.gov.au/LEGISLTN/CURRENT/I/InvasOfPrivA71.pdf (last visited on 9 January 2012). (AU)

[84] *Id.*

[85] Queensland, *Information Privacy Act of 2009 (Qld)*. (2009), at http://www.austlii.edu.au/au/legis/qld/consol_act/ipa2009231.txt/cgi-bin/download.cgi/download/au/legis/qld/consol_act/ipa2009231.txt (last visited on 9 January 2012). (AU)

The Qld *Information Privacy Act of 2009* allows for the appointment of a privacy commissioner who is under the direction of an appointed information commissioner. The term of office is at least five years and no more than ten years.[86] An individual may file a complaint; the resolution involves a mediation process. The Qld Civil and Administrative Tribunal has the power to hear any privacy-related cases.[87]

Qld has a spent conviction law similar to NSW and the NT.[88] The exception is that the Qld act includes records that relate to sexual crimes. The law provides privacy protections through non-disclosure sections.[89]

4.6.4 South Australia (SA-AU)

The State of South Australia (SA-AU) made a policy decision against any state-level privacy legislation. Instead, it chose to use administrative policy standards by Cabinet Administrative Instruction.[90] The instructions apply only to state agencies with local government exclusions. The Department of Health adopted the Federal NPPs for health information in a Code of Fair Information Practices.[91] SA-AU has also adopted a Code of Fair Information Practices.

The IPPs adopted the Federal IPPs pattern, which establish a six-person Privacy Committee of South Australia. The Committee functions in an advisory role to the Minister, makes recommendations to the Government, provides information to the public, and refers complaints to the authorities.[92]

---

[86] The approach raises issues of true independence and protections from Neo-Conservative political influences.
[87] *Id.* at §§ 141, 146.
[88] *Criminal Law (Rehabilitation of Offenders) Act 1986 (Qld)* (1986). (AU)
[89] *Id.* at §§ 5, 6.
[90] First issued July 1989; re-issued on 30 July 1992.
[91] Government of South Australia, *Information Privacy Principles (IPPs) Instruction, and Premier and Cabinet Circular 12, as amended by Cabinet 18 May 2009 (SA-AU)*. (1989), at http://www.premcab.sa.gov.au/pdf/circulars/pc12_privacy.pdf (last visited on 9 January 2012).
[92] *Id*. at § 2(1).

The *Listening Devices Act of 1972* evolved into the *Listening and Surveillance Devices Act 1972* as a result of repeated amendments.[93] The Act makes it illegal for a person to intentionally use a listening device to listen, monitor, overhear, or record a private conversation. The conversation parties must indicate expressed or implied consent to avoid a violation.[94]

4.6.5 Tasmania (Tas)

The Tasmania (Tas) Ombudsman has the operational authority of the 2004 *Personal Information and Protection Act*. The Act applies only to the state and local public sector, the University of Tasmania, as well as statutory office holders and bodies. The focus of this act is to regulate the government's collection, disclosure, maintenance, and use of personal information.[95]

The *Personal Information and Protection Act*[96] defines a person as a living person or one who has been dead for less than twenty-five years. The act is in contrast to the less than thirty-year standard in the NSW legislation. Basic personal information is limited to date of birth, gender, name, postal address, and residential address.[97] The *Personal Information and Protection Act* allows the personal information custodian to exempt information that is related to the courts and tribunals, public information, law enforcement information, employee information, and unsolicited information.[98] The ombudsman has the power to process individual complaints and make appropriate referrals.[99] The Act adopts the Federal IPPs' standards.

---

[93] Amendments were made in 1974, 1989, and 2001.

[94] *Listening and Surveillance Devices Act (AU)*. (1972), at http://www.austlii.edu.au/au/legis/sa/consol_act/lasda1972326/index.html (last visited on 12 February 2012).

[95] Tasmania Ombudsman, *Personal Information Protection*. (2009), at http://www.ombudsman.tas.gov.au/personal_information_protection (last visited on 9 January 2012).

[96] Tasmanian Legislation, *Personal Information Protection Act 2004 (Tas)*. (2004), at http://www.thelaw.tas.gov.au/tocview/index.w3p;cond=;doc_id=46%2B%2B2004%2BAT%40EN%2B20100110130000;histon=;prompt=;rec=;term= (last visited on 9 January 2012).

[97] *Id*. at part 1 § 3.

[98] *Id.* at Division 2 (7-11).

[99] *Id.* at Part 4.

The *Listening Devices Act of 1991*[100] prohibits a person from using, causing to use, or permitting the use of a listening device to listen or record a private conversation. This act applies if a person is or is not a party to the conversation.

4.6.6 Victoria (Vic)

Victoria has three major DPSIP legislative acts. The legislation includes the Information Privacy Act, Health Records Act, and the Surveillance Devices Act.

The *Information Privacy Act of 2000* creates a privacy commissioner known as Privacy Victoria.[101] The commissioner reports to the Attorney General who then reports to parliament.[102] The Act establishes ten privacy rights similar to the Commonwealth legislation. The Act applies to Vic state organizations, local councils, and statutory organizations; however, it does not apply to non-governmental organizations except when a business contracts with the state. In such a case, a contractual obligation may apply. Violations of the Act can result in a range of responses including an apology, change of a procedure, correction of information, deletion of personal information, or a maximum fine of $100,000 (AU dollars).[103]

Under the *Information Privacy Act of 2000*, personal information includes data and information in a database that is apparent or can be ascertained.[104] The

---

[100] *Listening Devices Act of 1991 (Tas AU)*. (1997), at http://www.austlii.edu.au/au/legis/tas/consol_act/lda1991181/ (last visited on 11 February 2012). (AU)

[101] Privacy Victoria, *The Information Privacy Act Gives Victorians Privacy Rights.* (2009), at http://www.privacy.vic.gov.au/privacy/web.nsf/content/about+privacy+victoria (last visited on 20 January 2012). (AU)

[102] This approach keeps DPSIP issues as political concepts rather than principles subject to the concept of the rule of law.

[103] *Information Privacy Act of 2000 (Vic-AU)* amend. No. 98 of 2000 (2000). (AU)

[104] *Id.* at Part 1, § 3. Reads "personal information means information or an opinion (including information or an opinion forming part of a database), that is recorded in any form and whether true or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion, but does not include information of a kind to which the Health Records Act 2001 applies;"

objectives of the Act are to balance free information processing with privacy protections, establish and provide education on responsible practices, and provide "responsible and transparent" public sector handling.[105] This act does not establish civil or criminal causes of action but does provide for administrative fines.

Section eleven of the *Information Privacy Act of 2000* allows for publically available information. The exempt sources include a "generally available publication," data for exhibition, reference, or study in an art gallery, library, or museum; or certain public records. This Act establishes ten IPPs based on the Commonwealth legislation. The principles include collection, use and disclosure, data quality, data security, openness access and correction, unique identifiers, anonymity, transborder data flows, and sensitive information.[106] Violations of the Act are processed through a conciliation approach by the Privacy Commissioner and may be originated by a person. If the conciliation does not resolve the conflict, a Tribunal may adjudicate the case.

In 2006, Vic passed the *Charter of Human Rights and Responsibilities Act,* which applies to courts and tribunals, parliament, and public authorities.[107] This legislation establishes that "a person has the right— (a) not to have his or her privacy, family, home or correspondence unlawfully or arbitrarily interfered with; and (b) not to have his or her reputation unlawfully attacked."[108] Under section twenty-eight, every Member of Parliament must submit a statement of compatibility with this Act for every proposed piece of legislation. The entire Parliament must consider these rights when passing any legislation.[109] The Act is also binding on the Attorney General, the courts, and public

---

[105] *Id.* at § 5.
[106] *Id.* at Schedule1—The Information Privacy Principles.
[107] *Charter of Human Rights and Responsibilities Act 2006 (Vic)* amend. No. 43 of 2006 (2006). (AU)
[108] *Id.* at Part 2, §13.
[109] This innovative approach is a principle that SA and the other countries noted in this study should consider. The provision attaches legislative accountability for DPSIP laws and policies.

authorities.[110] Part four creates the Victorian Equal Opportunity and Human Rights Commission, which has the power to intervene in areas addressed in the Act.

The Vic *Health Records Act of 2001*[111] applies to private and public health care providers and insurance corporations. The Act addresses the collection and use of private health information and requires protection of personal health information. The health privacy principles[112] enacted apply to aged care, disability, genetics, health issues, human tissue specimens, mental health, palliative care, and disabling conditions. The principles apply to holders of the data. There is no small business exemption.

The *Surveillance Devices Act of 1999*[113] regulates the installation, maintenance, and use of surveillance devices, restricts the release of private conversations, requires warrants or authorization for installation or use, and sets standards of data collection or use of information obtained. The Act does not apply to optical surveillance devices. According to the Act, a private activity does not apply to behavior outside a building or that might be observed by another. A private conversation requires that the parties reasonably expect privacy and not to be over heard.[114] Under the Act, a court-approved warrant is required.

4.6.7 Western Australia (WA)

The State of Western Australia (WA) has adopted the SA–AU strategic approach to DPSIP legal issues. No privacy regime has been adopted. The

---

[110] *Id.* at §§ 35-36, 38.
[111] *Health Records Act (HRA) 2001 (Vic)* amend. No. 2 of 2001 (2001). (AU)
[112] *Id.* at Schedule 1—The Health Privacy Principles, 93-116. The principles include The principals include Collection, Use and Disclosure, Data Quality, Data Security and Data Retention, Openness, Access and Correction Identifiers, Anonymity, Transborder Data Flows, Transfer or closure of the practice of a health service provider, and making information available to another health service provider.
[113] *Surveillance Devices Act 1999 (Vic)* amend. Act No. 21/1999 (1999). (AU)
[114] *Id.* at Section 3.

State has passed a *Freedom of Information Act of 1992*,[115] which addresses some information privacy and confidentiality provisions. Under the Act, the Supreme Court is required to preserve the confidentiality of any documents.[116] A person who "knowingly deceives or misleads" to access personal information regarding another or "information about the business, professional, commercial or financial affairs of another person" commits a crime under the statute.[117]

Under the WA *Spent Conviction Act of 1988*[118] criminal information must be secured and protected. The privacy protections in the statute provide a distinction between a lesser and a more serious conviction record. Lesser convictions are handled by the police service whereas serious convictions require district court approval.[119] As noted, a spent conviction is a conviction that has been spent (or removed from a person's public viewable police record).[120]

In 1998, WA passed a *Surveillance Devices Act*,[121] which prohibits the use of listening, optical surveillance, or tracking devices without a warrant. Information obtained by the use of such devices can not be communicated or published. A person can not record a private activity without consent or share such information known directly or indirectly.

---

[115] Western Australia, *Freedom of Information Act 1992 (WA)*. (1992), at http://www.slp.wa.gov.au/legislation/agency.nsf/foi_main_mrtitle_353_homepage.html (last visited on 9 January 2012). (AU)

[116] *Id.* at Division 6(91)(c).

[117] *Id.* at 109(a-b).

[118] *Spent Convictions Act 1988 (WA)* (1988). (AU)

[119] Acrod/Cofa Police Certificate Working Party, *A Resource Manual for the Use of Police Certificates*. (2005), at http://www.ideaswa.net/Resources/Other/documents/ACRODCOFAPoliceCertificateResourceManualVersion2.pdf (last visited on 23 January 2012). The standard is under the provisions of Section 7(1) of the Spent Convictions Act 1988 only 'lesser convictions' can be spent by the WA Police Service, after a time period of 10 years plus any term of imprisonment that may have been imposed. A lesser conviction is one for which imprisonment of 12 months or less, or a fine of less than $15,000 is imposed. All other convictions, such as 'serious convictions' applicable under Section 6 of the Spent Convictions Act 1988 can be spent only by applying to the District Court.

[120] *Id.* at 4.1.4.

[121] *Surveillance Devices Act of 1998 (WA AU)*. (1998), at http://www.austlii.edu.au/au/legis/wa/consol_act/sda1998210/ (last visited on 12 February 2012).

4.7 Australian State Case Law

Some AU State Courts have ruled on cases that have DPSIP implications. The States include the courts of NSW, Qld, and Vic.

4.7.1 New South Wales Case Law

The Supreme Court of NSW has not found a cause of action based on an invasion of privacy tort.[122] The Administrative Decision Tribunal has issued judgments based on the NSW 1998 *Privacy and Personal Information Protection Act.*

In *PN v Department of Education and Training,*[123] the applicant, aka PN, was a school teacher who was unemployed due to a disability. The school district shared the teacher's records with investigators and treatment providers, including personal comments made by PN regarding plans to return to work. The Administrative Decision Tribunal found that Sections one and two of the Act were violated.

In *SW v Forests NSW,*[124] the applicant's position was not supported. However, the tribunal issued an order that agencies should review and update policies on a regular basis. Regulations should be clear, detailed, and cover a broad range of possible privacy breaches.

Some agencies take advantage of legislative wording to avoid the spirit of the law. The tribunal addressed the issue in *HW v Director of Public Prosecutions.*[125] Section ten and eleven of the PPIPA addresses the agency responsibility when collecting *information from an individual*. Some agencies used the terminology to avoid responsibility for code violations. The tribunal

---

[122] *NRMA v John Fairfax*, NSWSC 563, (2002) (NSW AU).
[123] *PN v Department of Education and Training*, NSWADT 122, (2006) (NSW-AU).
[124] *SW v Forests NSW*, NSWADT 74, (2006) (NSW-AU).
[125] *HW v Director of Public Prosecutions (No 2)*, NSWADT 73, (2004) (NSW-AU).

suggests that the legislative language be changed or interpreted as information *about an individual.* The change would cover situations where the agencies obtain information from third parties.

The Administrative Decision Tribunal found that the NSW law does not apply to private information shared with parties in another state. Section eleven of the AU national Information Privacy Principles can be intentionally diverted by sending the information to a third party and who then provides the information to an intended party without penalty. The ruling allows for *information laundering*.[126]

When a medical practitioner was subject to a Department of Health investigation, the Department did not insure that the data collected was accurate as required by IPP Section nine. The tribunal required that the Department delete all inaccurate, irrelevant, misleading or out-of-date information and communicate the same to any agencies that had been given the information.[127]

In the *SW v Forests NSW* case,[128] a community volunteer agreed to allow the Forest Department to take photos of her while at a meeting in her professional capacity. A senior officer later took a photo of her in her pajamas without her permission and then shared the picture with others. The department did an internal review and found no privacy violations. The tribunal found that the photograph was personal information and a violation of the IPP Sections one, three, four, nine, and eleven of the NSW Act. The agency was found liable for the unauthorized actions of the senior officer. When an employee acts outside the course of employment, the agency is not held liable.[129]

---

126 *GQ v NSW Department of Education and Training (No 2)* NSWADT 319, (2008) (NSW-AU).

127 *JD v Director General, NSW Department of Health (No 2)* NSWADT 256, (2007) (NSW-AU).

128 *SW v Forests NSW*, NSWADT 74, (2006) (NSW-AU).

129 *Director General, Department of Education and Training v MT*, NSWCA 270 (2006) (NSW-AU).

The Administrative Decision Tribunal maintained that, for employment purposes, academic, and professional data is not personal information. The tribunal declared that depending on the content and context of the information, it could lead to a different conclusion.[130] Some other exemptions are also given deference. For example, the tribunal found that computerized operational policing systems are exempt because the data is not an administrative function.[131]

In *Vice-Chancellor Macquarie University v FM*,[132] the NSW Court of Appeals ruled on a case of a doctoral student who was dismissed from Macquarie University for behavioral issues. The student applied to the University of New South Wales and was accepted. Transcripts were provided. The Macquarie staff shared additional information in subsequent telephone calls with staff from the University of New South Wales. The court found that the additional information was in the *minds of the employees*[133] and thus was a breach of the Statute.

Under the authority of the Medical Practices Act, the NSW Medical Board inquired into the practices of a physician. The Board then released private information to the Pharmaceutical Services Branch of the Department of Health. The Medical Board was found to have contravened Sections 18(1) and 19 of the Privacy Act. The NSW Administrative Decision Tribunal found that personal information can be redacted when issuing reports. Agencies must carefully evaluate what is "reasonably necessary" and can not blindly claim an exception.[134] Agencies also must check the accuracy of personal information under IPP nine prior to using or disclosing any information even when complying with other principles.[135] The NSW privacy law differs from the

---

[130] *OD v Department of Education and Training*, NSWADT 161, (2005) (NSW-AU).
[131] *OQ v Commissioner of Police*, NSWADT 240, (2005) (NSW-AU).
[132] *Vice-Chancellor Macquarie University v FM*, NSWCA 192, (2005) (NSW-AU).
[133] A term of art meaning known by the employees.
[134] *JD v NSW Medical Board*, NSWADT 247, (3 November 2005) (NSW-AU).
[135] *Director General, Department of Education and Training v MT (GD)*, NSWADTAP 77, (23 December 2005) (NSW-AU).

federal statute in that the law does not allow for any type of injunctive relief or means to change policy.[136]

A cancer patient received a psychiatric and psychological consultation and the data was placed in a general medical record. The data was then shared with two outside physicians without an informed consent. The hospital was found to have violated Section ten—collection of information and Section nineteen—disclosure of personal information under the Privacy Act. Agencies must be clear, open, and obtain an informed consent. The standards apply to internal and external disclosures.[137]

The NSW Appeals Panel addressed the issue of exceptions under the Privacy Law. The panel maintains that its scope should be defined broadly; any exceptions should be defined narrowly, and a plain reading standard should apply.[138] Data holders must not only safeguard personal information from a policy and physical security perspective, wide-scale awareness and training programs are also needed.[139]

4.7.2 Queensland Case Law

The District Court of Qld has found justification for an invasion of privacy cause of action. The court awarded aggravated, compensatory, and exemplary damages for the invasion. The defendant willed the act that intruded on the privacy of the plaintiff.[140] The case provides some common law support for DPSIP legal principles.

---

[136] *ON v Marrickville Council*, NSWADT 274, (2 December 2005) (NSW-AU).
[137] *KJ v Wentworth Area Health Service*, NSWADT 84, (3 May 2004) (NSW-AU).
[138] *GA & Ors v Department of Education and Training and NSW Police (GD)*, NSWADTAP 18, (25 May 2004) (NSW-AU).
[139] *MT v Director General, NSW Department of Education & Training*, NSWADT 194, (3 September 2004) (NSW-AU).
[140] *Grosse v Purvis*, QDC 151, (2003) at ¶ 442 (Qld AU).

4.7.3 Victoria Case Law

The Supreme Court of Vic has also not found a cause of action based on an invasion of privacy tort.[141] However, the County Court of Vic has found a basis for a privacy invasion tort. Senior Judge Skoien found that there is a "civil action for damages based on the actionable right of an individual person to privacy."[142]

The Victorian Civil and Administrative Tribunal adjudicates privacy issues in Vic. The tribunal found that even when obvious identifying information is redacted, the data can not be released because the identity of the person may be directly or indirectly discovered.[143] The case recognizes the impact of modern data mining approaches.

In a case involving the release of two private letters related to an employment dispute, the author of the letter claimed that the release of the letters to an administrative agency was a violation of the Vic *Information Privacy Act*. The tribunal found that IPP 2.1(f) provides for an exemption for releases authorized by law. An administrative agency can release data when it is reasonably obligated to perform an inquiry.[144] The case reinforces the importance of legislative exceptions.

When the Australian Domain Name Administrator withdrew Nicholas Bolton's company right to administer and sell domain names, he appealed to the Vic Supreme Court. The Court upheld the Domain Name Administrator's ruling. Bolton's company had done nothing when the personal data of 40,000 of the total 60,000 customers was breached and 25,000 credit card holders' data was sold on the Internet. Bolton did not notify customers of the breach as

---

[141] *Gilleer v Procipets*, VSC 113, (2004) (Vic AU).
[142] *Jane Doe v ABC*, VCC 281, (2007) (Vic AU).
[143] *Beauchamp v Department of Education (General)*, VCAT 1653, (2006) (Vic-AU).
[144] *Dodd v Department of Education and Training*, VCAT 2207, (21 October 2005) (Vic-AU).

ordered. The legal basis of the dispute related to contractual obligations; however, the finding does have DPSIP implications.[145]

4.8 Australian Standards and Remedies

In 2001, the AU Privacy Commissioner defined the nature of privacy. He wrote the following:

> Privacy is about protecting our sense of self – that is, who we are, what we know, what we think, what we have done and what we want to do. One important aspect of this is the extent of control we have over personal information about us. Exercising choice about our own information can also be an important aspect of retaining personal dignity and humanity in a relationship with another party.[146]

The Office of the Privacy Commissioner addresses privacy in the workplace in a specialized set of guidelines. The Commissioner found that access to electronic records may be necessary at times; however, broad privacy policies and interventions can be seen as "intrusive and oppressive and have a negative impact on morale and productivity."[147] The managerial guideline suggested:

1. The policy should … ensure that it is known and understood by staff. Ideally the policy should be linked from a screen that the user sees when they log on to the network.
2. The policy should be explicit as to what activities are permitted and forbidden. … and refer to appropriate Commonwealth legislation sections.

---

[145] *Australian Style Pty Ltd v .au Domain Administration Limited*, VSC 422, (25 September 2009) (Vic SC-AU).

[146] Office of the Federal Privacy Commissioner, *Privacy and Public Key Infrastructure: Guidelines for Agencies Using PKI to Communicate or Transact With Individuals* (Office of the Federal Privacy Commissioner. 2001). at 12.

[147] Australian Government Office of the Privacy Commissioner, *Guidelines on Workplace E-mail, Web Browsing and Privacy* (Australian Government Office of the Privacy Commissioner. 2000). at 1.

3. The policy should clearly set out what information is logged and who in the organization has rights to access the logs and content of staff e-mail and browsing activities.
4. The policy should refer to the organization's computer security policy. Improper use of e-mail may pose a threat to system security, the privacy of staff and others, as well as the legal liability of the organization.
5. The policy should outline, in plain English, how the organization intends to monitor or audit staff compliance with its rules relating to acceptable usage of e-mail and web browsing.
6. The policy should be reviewed on a regular basis to keep pace with the accelerating development of the Internet and Information Technology. The policy should be re-issued whenever significant change is made.[148]

The guidelines do not have legal status but do establish a standard of care. The standard also services as a public awareness function for workers at all levels and corporations.

Under the Privacy Act of 1988, the Federal Court or Federal Magistrates Court has the power to enforce a violation determination.[149] The court can make any order that it determines to be fair, including a declaration of right. The court can issue an interim injunction.

The Privacy Commissioner can issue determinations that include a cease-and-desist order, redress for loss and damages – including psychological damages.[150] The legislation does not set statutory damages.

---

[148] *Ibid.*
[149] See Privacy Act of 1988, Section 55A.
[150] *Id.* at Section 52

4.9 Australian Implementation System

The AU approach to DPSIP legal issues is evolving. The Commonwealth government and most states have passed specific legislation with exceptions that are troublesome. Several governmental agencies have privacy offices; however, the power and independence does not meet the standards of CA and the EU approach. The approach also does not meet the US standard of independent regulatory agencies similar to the Federal Trade Commission (FTC).

The common law of AU has not found a direct privacy right. Some DPSIP principles can be argued based on breach of confidence, copyright, defamation, nuisance, or trespass.[151] The government is considering enacting a Statutory Cause of Action for Serious Invasion of Privacy.[152]

The Vic Privacy Commission, similar to the CA Commissioners, provides extensive consulting and educational materials. The Vic Commission issues a *Privacy Audit Manual* that provides a structured method to conduct and report on an audit.[153]

4.10 Australian Sociolegal Concerns

The AU Office of the Federal Privacy Commission conducted research on public privacy concerns for a number of years. In 2001, the levels of privacy concerns were higher than a similar 1997 study. In the 2001 study,[154] ninety-one percent of the sample thought that businesses should ask permission prior to collecting personal data even if it cost companies inconvenience. The

---

[151] Victoria Government, *Privacy Regulation Across Australia*. (2003), at http://www.privacy.vic.gov.au/privacy/web.nsf/download/11344F7F3050AF9ECA256D58000597A7/$FILE/03.03_Interstate.pdf (last visited on 27 March 2012).

[152] Australian Government, *Issues Paper: A Commonwealth Statutory Cause of Action for Serious Invasion of Privacy*,(Australian Government ed. 2011 September).

[153] Privacy Victoria, *Privacy Audit Manual* (Author. 2007).

[154] Australian Office of the Federal Privacy Commission, *Privacy and the Community* (Author 2001).

sample reported that businesses that collected data should inform customers regarding the uses of the data (eighty-nine percent). Over ninety-two percent reported privacy violations including businesses transferring personal data without permission and using the data for purposes other than that claimed at the time of collection. The highest ranked concern in the survey was that businesses ought to show *'respect for, and protection of, my personal information.'*[155] A third of those surveyed ranked respect higher than quality, efficiency, price and convenience. The exception was age. Fifty-nine percent of those eighteen to twenty-four reported that they would trade private information for cost discounts. Those with lower household incomes and lower education would do the same. Only forty-three percent knew that federal privacy legislation existed. Fifty-two percent knew very little or nothing about their privacy rights. The majority, sixty-six percent, thought that they should control the use of their personal data. Seventy percent did not want the government sharing collected data with businesses. Fifty-seven percent thought that the data should be secure. Fifty-five percent reported concerns about how companies obtained information to make unsolicited marketing contacts. Based on the survey, examples of what would be a privacy violation would include:

> A business that you do not know gets hold of your personal information – 95 percent. A business monitors your activities on the internet, recording information on the sites you visit without your knowledge – 90 percent. You supply your information to a business for a specific purpose and the business uses it for another purpose – 94 percent. A business asks you for personal information that does not seem relevant to the purpose of the transaction – 93 percent.[156]

In a related study of Australian business executives' attitudes toward privacy concerns, ninety-five percent reported that maintaining customer privacy was important or very important. Eighty percent saw businesses being dependent

---

[155] *Id.* at 4.
[156] *Id.* at 39–40.

on protecting customer privacy. Data protection breaches were seen as a negative by ninety percent of the sample. Ninety-five percent reported support for data protection laws including those that apply to businesses, yet only forty percent had appointed company privacy officers.[157]

In 2004, an additional study[158] showed that the level of awareness of federal privacy laws increased to sixty percent from the prior forty-three percent. Eighty-one percent reported that businesses transferred and sold personal data without permission.

Sixty-one percent of the sample reported being angry or annoyed over receiving unsolicited marketing materials. Sixty-two percent were concerned about the security of their data, up from fifty-seven percent in the prior study. Sixty-two percent were concerned about Internet personal data misuses.[159]

The 2007 study focused on a number of different issues; however, only some of these issues were relevant to the focus of this thesis.[160] Ninety percent reported concerns regarding business use of personal data and transborder transfers including sixty-three percent who were very concerned. Awareness of federal legislation had increased to sixty-nine percent of the sample. Internet monitoring was reported as a violation by ninety-four percent of the sample reported that a privacy violation occurred when a business (eighty-seven percent for a governmental agency) asked for information not relevant to the transaction. The same percentage reported that businesses (eighty-six percent for governmental agencies) should not collect data for one purpose and then use it for another. Ninety-three percent of the sample reported that being contacted by businesses and eighty-six percent for governmental agencies you do not know or consent to interact with is a privacy violation.

---

[157] Australian Office of The Federal Privacy Commission, *Privacy and Business* (2001, July), http://www.privacy.gov.au/publications/rbusiness.html (last visited on 5 January 2012).

[158] Australian Office of The Federal Privacy Commission, Community Attitudes towards Privacy 2004 (Author 2004).

[159] *Ibid.*

[160] Australian Office of The Federal Privacy Commission, *Community Attitudes towards Privacy 2007* (Author 2007).

Seventy-three percent reported that governmental agencies with which they had no dealings should not have access to personal data.[161]

The research showed that in AU, citizens and even business executives were concerned about DPSIP issues and violations. Representative governments should establish laws that reflect citizen concerns rather than those of special interests.

Dr Mark Andrejevic and the University of Queensland[162] reported on a national study related to Australians' 2012 attitudes related to DPSIP issues. Ninety-seven percent wanted to be able to initiate legal action for serious privacy breaches. Ninety percent supported governmental regulations that allow them to control the capture and use of personal information. Seventy-nine percent refused to provide personal information for access to web sites or to use an application. Sixty-nine percent thought that applications and sites requested too much information and refused to comply with such requests. Seventy-five percent want to know and have some say in how companies collect and use personal information. Sixty-four percent did not want filtered news stories based on personal information. Sixty percent reported that they never or rarely read privacy policies. Fifty-six percent did not approve of targeted advertising based on personal information.

Politicians and jurists can and certainly do argue and maneuver around DPSIP issues. Businesses and corporations can and do corrupt the process.[163] The above research shows that the majority of AU citizens want strong DPSIP legislation and regulation.

---

[161] *Ibid.*

[162] University of Queensland Social Research Centre, *Australians Concerned for Online Privacy: Study*. (2012), at http://www.uq.edu.au/news/?article=24504 (last visited on 15 March 2012).

[163] See: Jeffrey D. Clements, *Corporations Are Not People: Why They Have More Rights Than You and What You Can Do About it* (Berrett-Koehler Publishers, Inc ed. 2012). Thom Hartmann, *Unequal Protection: The Rise of Corporate Dominance and the Theft of Human Rights* (Rodale ed. 2002). Robert G. Kaiser, *So Damn Much Money: The Triumph of Lobbying and the Corrosion of American Government*,(Alfred A. Knopf ed. 2009). Lawrence Lessig, *Republic, Lost: How Money Corrupts Congress - and a Plan to Stop It* (Twelve - Hachette Hook Group ed. 2011).

4.11 Australian Critique

Some basic principles of the AU federal privacy law are open to question. The AU DPSIP standards are not considered adequate by the EU DPSIP standards.[164] The AU approach allows for significant exceptions for small businesses. Employee records also have an exemption. Much like the US, significant inconsistencies exist regarding how the government and businesses deal with DPSIP issues. Under both systems there is no legal or regulatory remedy for DPSIP violations, even when the violations are serious. The *Telecommunication Act of 1997* does not provide for a consistent standard for addressing DPSIP standards. The AU government has suggested that these issues be addressed. However, despite voiced concerns, the government has not scheduled any projected date for addressing these issues.[165] The history of group decision-making reveals that several ways exist to stop any proposals that might be made to address DPSIP issues. The approaches include referring the issue to a committee, passing but not funding resolutions, and not developing a timeline for implementing resolutions.

The AU government proposed some legislative and regulatory changes to the 1998 *Privacy Act* to address other DPSIP deficiencies and complications in 2010. Perhaps the clearest change is to combine the NPPs' and IPPs' standards in the legislation into a clearer standard of Uniform Privacy Principles (UPPs). The UPPs would apply to Commonwealth agencies and private organizations. The proposal would clarify what is included in the practices authorized by or under law as "Commonwealth, State and Territory

---

[164] Tim Wright, *Cross-border data transfer - delusions of adequacy?*(2012), at http://www.sourcingspeak.com/2012/04/cross-border-data-transfer---delusions-of-adequacy.html (last visited on 24 April 2012).

[165] Lisa Vanderwal, *Australia: Proposed Changes to the Privacy Act, and the Privacy Act in Action: the Privacy Commissioner's decisions in 2009 Privacy: Who cares?* (2010, March 15), at http://mondaq.com/australia/article.asp?articleid=95892 (last visited on 17 March 2012).

Acts and delegated legislation, common law or equitable duties, an order of a court or tribunal, or documents given the force of law by an Act." In order to prevent people from circumventing the UPPs by contracting out their obligations under an Act, contracts are excluded under the new definition.[166]

The AU and NSW Law Reform Commission have recommended the establishment of a statutory privacy tort. The UPPs' recommendations include eleven principles. The principles include the areas of anonymity and pseudonymity; collection, notification, openness, use, disclosure, direct marketing, data quality, data security, access, correction, identifiers, and cross-border data flows.[167] The purpose of the new principles is to establish uniformity of all federal, state, and local privacy-related legislations. The proposal suggests modification of some troublesome and out-of-date language in the current legislation. The UPPs apply to all governmental agencies and private organizations. The proposal eliminates the small business exception in the current law. The proposal further suggests that the government should establish a statutory Office of the Information Commissioner. When the report was submitted, the Attorney General tabled the proposal to give the government additional time to prepare a detailed response.[168]

When an organization receives unsolicited personal information, it must determine if the information is to be held. If not, the organization must immediately destroy the data. If the information is to be held, the organization must notify the person addressed and follow standards in the UPPs. The change addresses some key regulatory discrepancies. Under the proposed changes, when organizations share information with one another, and the data is subsequently changed, the organizations must notify and request an

---

166 *Id.* at 5.

167 New South Wales Law Reform Commission, *Privacy Principles: Report 123* (New South Wales Law Reform Commission. 2009, August).

168 Catherine Kelso, *Australia: A Step Towards Harmony in the Regulation of Privacy and Access to Government Information Legal Update*, Mondaq: Government & Public Sector. (2010 March 30), at http://www.mondaq.com/australia/article.asp?articleid=97214&email_access=on (last visited on 1 April 2012).

update for all information provided. An interesting twist is that when a direct marketing business makes unsolicited contacts with non-current customers, it must reveal the source of the contact data. However, the person must first ask for the data.[169]

The proposed changes ignore some significant data transfer issues. While organizations are accountable for DPSIP transnational transfers, the requirement for a contract that would be binding on the parties will be eliminated. This change ignores the standards in CA and the EU but will still be better than standards in other regions, including Asia, the US, and South America, which have less stringent DPSIP regulation approaches.[170]

Consistent with the principle that all change is not progress, the proposed changes prohibit credit reporting businesses from sharing credit data with foreign credit reporters or data collectors and eliminate the need to store foreign data. However, the changes include an expansion of what types of data can be collected and shared.[171] Perhaps the most unwise change relates to health and life exemptions. The current law allows an exemption when a person's health or life is in imminent danger. The proposed change is to lower the standard for exemption by eliminating the term "imminent".

In general, AU law provides for an opt-in approach with consent being required. The Australian Communications and Media Authority conducted a compliance study and found that online businesses were not following the legal standards. Businesses were found to have "sloppy or cavalier consent practices."[172]

---

[169] *Ibid.*
[170] *Ibid.*
[171] *Ibid.*
[172] Munir Kotadia, *ACMA Slams Retailers Over Spam Act Breaches*, SC Magazine For IT Security Professionals. (2009), at 6. http://www.securecomputing.net.au/News/161769,acma-slams-retailers-over-spam-act-breaches.aspx (last visited on 1 December 2012).

The federal and state privacy law in AU has not followed the US state law standard of requiring governmental and private business sites to provide a notification when a breach occurs. The Australian Law Reform Commission (ALRC) recommends that breach notification should be submitted to the Privacy Commissioner and to all individuals affected. Cross-border data transfers including outsourcing of data needs to be controlled and should require informed consent of the individual. The standards should apply to all governmental and business organizations. The ALRC further recommends that all AU privacy laws be harmonized at all levels, and that the small business exemption and the employee records exemption be removed. The small business exemption is the main reason that the EU has not found AU adequate.[173] While exemption removal would involve increased business costs, the costs could be limited by the Privacy Commissioner providing consulting, education, materials, and compliance templates. The ALRC also recommends that serious DPSIP violations should require a statutory cause of action and increased civil penalties. The Privacy Commissioner must have strengthened enforcement powers.[174]

The Government responded to some of the ALRC recommendations. The first response was that it agreed to consider civil penalties for serious data

---

[173] European Commission, *Submission to the House of Representatives Committee on Legal and Constitutional Affairs Concerning its Inquiry into the Privacy Amendment (Private Sector) Bill 2000. MARKT/E1//FB/fb D(2000)*. (2000), at http://www.aph.gov.au/house/committee/laca/Privacybill/sub113.pdf (last visited on 30 December 2012).

[174] Australian Law Reform Commission, *Australian Privacy Law and Practice* (Commonwealth of Australia. 2008); Richard Smith, *Australia: ALRC Report On Australian Privacy Laws*. (2008), at http://www.mondaq.com/australia/article.asp?articleid=64940 (last visited on 12 December 2012); Australian Office of the Federal Privacy Commission, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (Author. 2005); Government Of Australia, *Government Response to the Privacy Commissioner's Report - Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2006).

breaches.[175] A 2009 study found that breaches cost an average of $2 million dollars per incident. The average per record cost was $123.00 dollars.[176]

The government was not willing to make major changes, especially with exemptions. The government announced thirteen new Australian Privacy Principles. The first seven included open and transparent management of personal information, anonymity and pseudonymity, collection of solicited personal information, receiving unsolicited personal information, notification of the collection of personal information, use or disclosure of personal information, and direct marketing controls. The remaining six principles included cross-border disclosure of personal information, adoption, use or disclosure of government-related identifiers, quality of personal information, security of personal information, access to personal information, and correction of personal information standards.[177]

At the same time the Attorney General's office was holding confidential consultations with Internet industry leaders regarding a new data retention plan. Under the plan, ISPs would be required to hold and release to police all Internet activities in AU with no warrant.[178] Rather than following the EU

---

[175] Lisa Banks, *Commissioner Launches Privacy Guide* IDG News Service (2010), at http://www.networkworld.com/news/2010/051110-commissioner-launches-privacy.html (last visited on 11 May 2012).

[176] Karen Dearne, *Data Breach Costs $2m Per Incident* Australian IT. (2010), at http://www.theaustralian.com.au/australian-it/data-breach-costs-2m-per-incident/story-e6frgakx-1225851401246?from=marketwatch_rss (last visited on 8 April 2012). See also Ponemon Institute, *Australia 2009 Annual Study: Cost of a Data Breach*. (2010), at http://www.encryptionreports.com/costofdatabreach.html (last visited on 22 June 2012).

[177] Australian Government, *Australian Privacy Principles: Companion Guide*, Author. (2010 June), at http://www.aph.gov.au/senate/committee/fapa_ctte/priv_exp_drafts/Guide/companion_guide.pdf (last visited on 26 June 2012). See also Australian Government, *Australian Privacy Principles: Exposure Draft*. (2010), at http://www.aph.gov.au/senate/committee/fapa_ctte/priv_exp_drafts/Guide/exposure_draft.pdf (last visited on 26 June 2012).

[178] Asher Moses, *Web Snooping Policy Shrouded in Secrecy* Sydney Morning Herald. (2010), at http://www.smh.com.au/technology/technology-news/web-snooping-policy-shrouded-in-secrecy-20100617-yi1u.html (last visited on 17 June 2012).

standard of six to twenty four-month retention, the AU approach would cover five to ten years.[179]

During the last six months of 2009, the government made 155 requests that Google release personal data of users. The government also made seventeen requests to remove content so that citizens could not access the sites. The sites did not include child pornography materials.[180]

The Privacy Commissioner did issue a recommended Privacy Impact Assessment Guide (PIA Guide) for businesses involved in DPSIP issues.[181] The guide was an educational tool rather than a regulatory guide. Starting in 1995, Roger Clarke[182] and Tim Dixon[183] have been writing about and advocating for the use of privacy impact assessments (PIA) in AU DPSIP law and regulation. Since then, recommendations have been made, self regulation suggestions have been published, and little actual progress has been established. None of the efforts have been more than recommendations; no legally binding standards have been established in AU. Quality research on-point has been suppressed. None of the states or the federal government have substantially addressed or implemented measures to deal with substantive PIA issues. The AU legal and political history on PIA issues can,

---

[179] Ben Grubb, *Govt Wants ISPs to Record Browsing History*, ZDNet.com.au (2010), at http://www.zdnet.com.au/govt-wants-isps-to-record-browsing-history-339303785.htm (last visited on 12 June 2012).

[180] Asher Moses, *Google Exposes Government Takedown and Data Requests* Sydney Morning Herald. (2010), at http://www.smh.com.au/technology/technology-news/google-exposes-government-takedown-and-data-requests-20100421-stas.html (last visited on 22 April 2012). Google publishes a tally of different governmental requests at http://www.google.com/governmentrequests/

[181] Australian Government Office of the Privacy Commissioner, *Privacy Impact Assessment Guide (Revised May 2010)*. (2010), at http://www.privacy.gov.au/ (last visited on 20 June 2012).

[182] See Roger V. Clarke, *Privacy Impact Assessment*. (2012), at http://rogerclarke.com/DV/PIA.html (last visited on 8 March 2012) and Roger V. Clarke, PIAs in Australia: A Work-In-Progress Report, in *Privacy Impact Assessment* (Davide Wright & Paul De Hert ed.^eds., Springer 2012).

[183] Tim Dixon, Communications Law Centre wants IPPs revised in line with Australian Privacy Charter, 3 *Privacy Law and Policy Reporter*, 9, 171 (1997).

at best, be seen as a flirtation. At best, the overall AU DPSIP approach can be seen as a "very-soft-touch regulatory" approach.[184]

Roger Clarke, an AU privacy expert and professor, maintains that the public sector law is weak and is made increasingly more ineffective by bureaucrats establishing increased exceptions. The law addressing the private sector is atrocious.[185] A classic example includes McAffee's release of personal information on 1,408 security professionals that attended a security conference. At first, the company argued that the breach was a human error. The company asked recipients to delete any unwanted data; however, there are no legal steps established for reasonable responses.[186]

In a 2009 study, sixty-nine percent of companies reported at least one breach, which is up from fifty-six the year before. Of those reporting a breach, sixty-five percent never informed the public.[187]

The AU government wanted to issue 16 digit identification numbers as part of its E-health initiative. Opponents maintained that the number will become a national ID number that has historically been rejected.[188] The legislature passed the enabling bill and $466.7 million was allocated over the next two

---

[184] Roger V. Clarke, PIAs in Australia: A Work-In-Progress Report, in *Privacy Impact Assessment* (David Wright & Paul De Hert ed., Springer 2012), p. 148.

[185] Liz Tay, *Privacy Must Be Addressed, For Innovation's Sake*, IT News For Australian Business. (2009), at http://www.itnews.com.au/News/163197,privacy-must-be-addressed-for-innovations-sake.aspx (last visited on 18 December 2012).

[186] Ben Grubb, *McAfee Keeps Leaked Details to Itself: Biggest Companies in Australia on List*, IT New for Australian Business. (2009), at http://www.itnews.com.au/News/151609,mcafee-keeps-leaked-details-to-itself.aspx (last visited on 31 July 2012).

[187] Brett Winterford, *Two in three Australian companies leak data*, SC Magazine For IT Security Professionals. (2009), at http://www.securecomputing.net.au/News/152610,two-in-three-australian-companies-leak-data.aspx (last visited on 11 August 2012).

[188] Suzanne Tindal, *COAG Commits to Health IDs in 2010*. (2009), at http://www.zdnet.com.au/coag-commits-to-health-ids-in-2010-339299911.htm (last visited on 8 December 2012).

years.[189] The action allowed the development of *PositiveID* RFID-implanted microchips.[190]

Westfield, a large shopping center chain in the AU and US, has announced that in addition to surveillance cameras, it wants to install facial recognition software. Not only will customers be monitored for current behavior; they will be identified and compared to other databases. The local police think that it is a great idea. The Australian Privacy Foundation chair, Dr. Roger Clarke, suggests that the move is "extremely dangerous" and has no controls; therefore, everyone will be identified with no legal justification.[191]

The AU police, AU Securities & Investments Commission, Fair Work Ombudsman, and AU Taxation Office want the power to share secret tax records. Not only will the data be shared; it will be allowed to be introduced in various trials.[192]

The AU government and businesses are sharing massive amounts of personal data. A company called VicRoads sells data to 190 third-party contracted organizations and covers millions of people. The data includes comprehensive dossiers including data on personal address, age, banking information, employment, financial information, health history, name, and tax information. Such data can also be used for identity theft purposes.[193]

---

[189] Josh Taylor, *Healthcare Identifier Legislation Passes*, ZDNet.com.au. (2010), at http://www.zdnet.com.au/healthcare-identifier-legislation-passes-339304038.htm (last visited on 25 June 2012).

[190] Greg Nikolettos, *Kevin Rudd's e-Health Bill Paves the way for PositiveID Human Implantable RFID Microchips*, OEN: OpEdNews. (2010), at http://www.opednews.com/articles/Kevin-Rudd-s-e-Health-bill-by-Greg-Nikolettos-100408-839.html (last visited on 26 June 2012).

[191] Saffron Howden, *No Place for Crooks to Hide*, Sydney Morning Herald. (2009), at ¶ 10. http://innovya.com/2009/12/10/no-place-for-crooks-to-hide/ (last visited on 9 December 2012).

[192] Natasha Bita, *Australian Police Get Access to Tax Data for Trials*, The Australian. (2010), at http://www.sott.net/articles/show/204287-Australian-Police-get-access-to-tax-data-for-trials (last visited on 8 March 2012).

[193] Ellen Whinnett, *All Your Details at Click of a Mouse: Your Personal Details are Being Spied on by Hundreds of Government and Private Agencies as New Technology Sees Data-sharing Reach Record Levels* Sunday Herald Sun. (2009), at http://www.heraldsun.com.au/news/victoria/all-your-details-at-click-of-a-mouse/story-e6frf7kx-1225759387740 (last visited on 9 August 2012).

Governmental authorities and the ALRC are not exempt from the law of unintended consequences and group think.[194] Graham Greenleaf argues that the latest recommendations on data export allow businesses to pass on data misuse and privacy breaches. Security standards are relaxed so that AU is subject to American spammers, Nigerian scammers, and the Russian mafia. Data can be transferred to data protection-free countries with no consent or regulation.[195]

Neo-Conservative legislators, governmental officials, and jurists resist DPSIP legal efforts. Some business groups are opposed to regulation and the costs of DPSIP standards. The AU experience shows that in practice the Neo-Conservative concerns are not warranted. A study on the impact of AU federal privacy legislation on businesses showed that seventy-three percent of the business leaders reported the legislation as positive; only twelve percent were somewhat negative. The minority negative responses addressed were costs as well as the perception that businesses might be restricted from doing whatever they want with the data. The majority positive response noted that DPSIP laws increased company benefits, corporate social responsibility, increased ethical behavior and honesty, customer confidence, relationships, and satisfaction, and protects important data.[196]

4.12 Summary of Australian Literature and Issues Reviewed

The intent of this thesis is to conduct a comparative analysis of DPSIP responses in five different nations. Part of the comparison uses a benchmark approach of key issues. The issues include legal support of DPSIP

---

[194] Group think is a decision-making effect found in cohesive groups of like minded persons. Such groups then adopt a consensus that is devoid of analysis, critical thinking, and evaluation.

[195] Karen Dearne, *Privacy Changes Put Data at Mercy of Scams* The Australian. (2009), at http://www.theaustralian.com.au/news/privacy-changes-put-data-at-mercy-of-scams/story-e6frgal6-1225788524304 (last visited on 20 October 2012).

[196] Australian Office of the Federal Privacy Commission, *Privacy and Business*. (2001, July), at http://www.privacy.gov.au/publications/rbusiness.html (last visited on 5 January 2012).

protections, legal support of corporate privacy and data protection standards, information privacy data protection and security declarations, the use of regulatory agencies, sectoral legislation, and data controllers. The benchmark standards also include data processor requirements, rights of data subjects, data security destruction, cross-border data flow regulations, exemptions and exceptions, and the current stage of the approach based on evolutionary stages. The following table presents the summary based on the benchmark model.

Table 4.1 Comparative Model of Australian Legal Support of DPSIP Models

ISSUE DESCRIPTION	AU CURRENT RESPONSE
CM.1: Legal Support of DPSIP Protections	
Signatory, Adheres and/or Complies with International Human Rights Standards	(See Appendix A)
Signatory, Adheres and/or Complies with EU DPSIP Standards	Attempted, but not granted adequate status.
Signatory, Adheres and/or Complies with APEC DPSIP Standards	AU helped to form the APCE
Federal Constitutional Law	No
Federal Legislative Efforts	Yes
Federal Common Law	No
Province /State Constitutional Law	No
Province / State Legislative Efforts	Some
Province /State Common Law	Some
CM.2: Legal Support of Corporate Privacy and Data Property Protection Issues	**AU CURRENT RESPONSE**
Copyright Protections	Yes
Database Protection	Yes
Patient Protections	Yes
Service Mark Protections	Yes
Trade Mark Protections	Yes
Trade Secret Protections	Yes
Privacy Impact Audit Required	No

Before Use	
Privacy Impact Audit Required Before Government Protections Granted	Some
Checks and Balances on Corporate Collection, Use, and Transfer of Individual DPSIP Data	Limited
CM.3: Information Privacy – Data Protection and Security Declarations	**AU CURRENT RESPONSE**
Definitions Provided	Yes
Personal and Sensitive Data Defined	Yes
Definitions Effectively Address Advanced Data Mining Technologies	No
All Holders and Users Held Accountable	No
CM.4: Regulatory Agency	**AU CURRENT RESPONSE**
Independent of Legislative and Executive Branches	No
Administrative Power	Yes
Investigative Power	Limited
Regulatory Powers	No
Education Function	Yes
Enforcement Powers	No
Structure	Federal and State
Responsibilities Defined	Prevent Harm and Punish Violators
Accountability	Civil and Criminal
Governmental Chief Privacy Officer/ Commissioner Required	Yes
Governmental Privacy Audits Required as Part of Legislation Passage	Yes
Business Chief Privacy Officer/ Commissioner Required	No
Employees are Personally Liable for Violations	Civil and Criminal
Business Privacy Audits Required	No
Agency Educational Function	Yes
CM.5: Sectoral DPSIP Legislation	**AU CURRENT RESPONSE**
Credit Reporting Agencies	Strong
Criminal Justice Record	Strong

Restrictions	
Health Information	Yes
Health Information Exceptions	Yes
Electronic Medical/Health Record Controls	Limited
CM.6: Data Controllers	**AU CURRENT RESPONSE**
Notice Required	Generally
Opt-In	Limited
Opt-Out	Generally
Must Be Lawful and Fair	Yes
System Access Controls	Yes
Data Quality And Integrity	In theory
Accurate	In theory
Complete	In theory
Up to Date	In theory
Limited to Needed Data	In theory
Relevant	In theory
Not Misleading	In theory
Data Retention Limitation	Not within current standards
Data Transfer Controls	Limited
Openness on Information Held	Limited
Breach Disclosures Required	No
Breach Penalties	No
CM.7: Data Processor Requirements	**AU CURRENT RESPONSE**
Informed Consent Required	Limited
Rationale Is Provided	Yes
Fair Processing	Yes
Legal Processing	Yes
General Data	Yes
Sensitive Data	Yes
Accuracy	Yes
Timely	Yes
Duration of Record Keeping Controls	Limited
CM.8: Data Subjects	**AU CURRENT RESPONSE**
Ownership by the Subject	Limited
Control Over Access	No
Alter, Amend, Correct, and Delete Errors	Yes
Notification Requirement	Limited
CM.9: Data Security and Destruction	**AU CURRENT RESPONSE**
Security Must be State-of-the-Art	Generally

Technology Use – Cost of Implementation Not a Defense	Yes
Tracking	Not once data is merged
Safeguards Required	Adequate encryption
Protects from Alteration	Yes
Protects Against Disclosure	Yes
Protects Misuse	Yes
Protects Against Unauthorized Internal and External Access	Yes
Unauthorized Access Penalties	Civil, criminal, cause of action
Timely Notice of Breaches	Limited
Strong Remedies Provided	Limited
CM.10: Cross-Border Data Flow	**AU CURRENT RESPONSE**
Individual Informed Consent Required	No
Transfer Source Is Accountable	Generally
Outsource Service Controls	Limited
CM.11: Exemptions and Exceptions	**AU CURRENT RESPONSE**
Only Permitted Where There is a Compelling Justification	No
Checks and Balances – Court Order Required	Limited
Government Agencies	Yes
Intelligence and Defense	Yes
Police Actions	Yes
Small Business Exemption	Yes
CM.12 DPSIP Evolutional Stages	**AU CURRENT RESPONSE**
DPSIP.0 Limited DPSIP legal Issues	Passed
DPSIP.1.0 Establishes PII; does not fully address security issues; focus on limited legal consent and notice.	Yes
DPISP.2.0 Accepts PII standards; does not fully address security issues; focus on a legally based harm based analysis.	Limited
DPSIP.3.0 PII and non-PII data fused; privacy, data protection and security issues are interrelated; legal audits, checks, and balances	No

needed for all personal information stakeholders. New technologies are required to pass privacy audits (example – RFID, Internet of Things) and require use of privacy enhancing technologies in all new IP approvals.	

The selection of AU approaches to DPSIP legal issues is warranted in the current study. The AU experience is best described by the children's game of *two steps forward and one step back*. The AU response is related to the impact of EU principles that established international DPSIP legal standards. The AU deference to small business exceptions and political pressures resulted in an EU refusal to grant adequate status. In establishing DPSIP laws, regulations, and standards, SA should not make the same errors in judgement. By definition, special interests often ignore general interests.

On a state and federal level, the AU approach reveals problems related to a lack of constitutional recognition of an information privacy right. This issue applies to all of the countries studied with the exception of SA. The AU example reveals problems related to establishing privacy commissioner offices that are not independent. The establishment of different sectoral privacy principles reveals some inherent problems.

The AU experience shows that DPSIP legal issues are too important to be left solely to the common law. AU judges, like their UK counterparts, resist such

actions. Some argue that the task should be left to the legislature whereas others resist finding a general legal principle that applies.[197]

The AU approach does set a standard that should be recognized in SA and internationally. The first is the approach to spent convictions. The second is that under the Vic statute, every Member of Parliament—on every legislative action—must affirm that any legislation does not violate DPSIP principles. The Vic Statute also binds the attorney general, courts, and public authorities to the same standard. This standard would prohibit the granting of intellectual property protections status to technologies that can limit DPSIP protections. The legal principle in Vic law reinforces the need for privacy audits at all levels.

SA can learn from the AU experience in a number of ways. Attending to immediate self-interest group pressures can result in faulty legal and long-term goals. Cost versus benefit analysis can distort the legal and policy issues. In a global economy, local political interests may be trumped by international standards.

Chapter Five addresses the CA approaches to DPSIP legal issues. Both the AU and CA are former colonies of the UK but have addressed DPSIP in different ways. CA has been approved as adequate, whereas AU has not. The CA approach is certainly relevant to how SA should address DPSIP legal issues.

---

[197] *Lenah Game Meats* (2001) 208 CLR 199. See also *Wainwright v Home Office* (2004) 2 AC 406. (AU) Compare *Hosking v Runting* (2005) 1 NZLR 1.).

CHAPTER FIVE: DATA PROTECTION AND SECURITY LAW:

CANADIAN LEGAL STANDARDS

The popularity of the Internet has created a new awareness of threats to personal privacy. The collection and use of personal data has evolved into a major industry, with companies willing to pay thousands of dollars for consumer databases that provide contact information and personal preference data. … The growth of the personal information industry has left many concerned about the loss of personal privacy. Michael Geist[1]

5.0 Overview

Of the countries addressed in the current study, CA is the only non-EU country that has been evaluated by the EU as having adequate DPSIP standards and systems. Starting in the 1980s, CA became aware of the massive privacy threats posed by computers, the Internet, and information business practices. The current approach includes regulation of DPSIP threats from the private and public sectors.

The CA chapter begins with presenting background on the country. The analysis continues with an examination of the CA federal constitutional declarations. CA federal legislation and federal case law is examined. The research then focuses on CA Provincial Constitutional declarations, Provincial legislation, and case law. An analysis of the CA standards, remedies, and implementation system are reviewed. CA sociolegal concerns are presented. A critic of the CA approach is then addressed. A summary of the CA literature and issues using the thesis comparative model of the current legal support is then reviewed and presented.

---

[1] Michael Geist, *Internet Law in Canada*. (Captus Press 3rd. ed. 2002), at 284.

5.1 Background

Historically, the Canadian attitude toward data protection and information privacy was based on the English Common Law. The British North American Act of 1867 established CA as part of the British Empire.[2] The British court ruled that privacy issues should be left to the legislature.[3] Richard Clayton and Hugh Tomilson determined that "English law gives little clear recognition of privacy rights outside the fields of misuse of information…and intrusion."[4]

CA, a former colony of the UK, is now a Federal State that consists of a federal government, ten provinces, and three territories.[5] Each unit has special obligations and opportunities. All these provinces and territories were former British colonies except Quebec. When formed, special provisions were made to incorporate Quebec's Roman Catholic religion, French language, and civil law traditions. During the American Revolution, CA maintained ties with England and maintained membership in the Commonwealth of Nations. In 1867, in response to the US Civil War, a more formal structure was required.

In 1867, the Constitution Act established governmental structure.[6] In 1982, CA became an independent nation; however, it remains one of the member states of the Commonwealth of Nations.[7]

---

[2] Statutes of Great Britain, *The British North America Act*. (1867), at http://home.cc.umanitoba.ca/~sprague/bna.htm (last visited on 29 February 2012).

[3] *Kaye v. Robertson,* FSR 62, (1991). (UK)

[4] Richard Clayton & Hugh Tomlinson, *Privacy and Freedom of Expression* (Oxford University Press. 2001), at 35.

[5] Government of Canada, *Government of Canada*. (2010), at http://www.canada.gc.ca/home.html (last visited on 5 August 2012). Site contains reference data for this section.

[6] Canadian Constitution Act, *Constitution Acts from 1867 to 1982*. (1867), at http://laws.justice.gc.ca/en/const/c1867_e.html (last visited on 2 August 2012).

[7] Canadian Constitution Act, *Constitution Act, 1982, being Schedule B to the Canada Act 1982. (UK) 1982, c. 11. (CA)* at http://www.canlii.org/en/ca/const/const1982.html (last visited on 3 August 2012).

The chief executive is the Prime Minister[8] who is usually selected by the majority party of the House of Commons. The cabinet is composed of parliamentarians. The Prime Minister responds to questions from the House, similar to the UK system. The Governor General is appointed by and serves as the representative of the UK monarch; and is the Commander-in-Chief.

The parliament[9] consists of 308 democratically elected members of the House. The Senate has 105 members appointed by the Governor General with the advice of the Prime Minister. The senate rarely opposes the House of Commons.

The Supreme Court of Canada[10] is the highest court in the country. A system of appeals courts and specialty courts also functions. Each province has a similar structure.

Civil liberty groups in CA are a recent development. In 1917, the first US civil liberties organization, the National Civil Liberties Bureau (NCLB), was formed. Three years later, the group was expanded into the American Civil Liberties Union (ACLU). In contrast to the early development of such organizations in the US, non-business and agricultural interest groups did not begin in CA until two developments occurred in the 1960s; in 1962, the British Columbia Civil Liberties Association was formed, and in 1964 the Canadian Civil Liberties Association was formed. Subsequently, regional groups were formed over the next twenty plus years. The groups focus on legislative reform more than litigation.[11]

---

[8] Government of Canada, *Prime Minister of Canada*. (2010), at http://pm.gc.ca/eng/index.asp (last visited on 5 August 2012).

[9] Government of Canada, *Parliament of Canada*. (2010), at http://www.parl.gc.ca/common/index.asp?Language=E (last visited on 5 August 2012).

[10] Government of Canada, *Supreme Court of Canada*. (2010), at http://www.scc-csc.gc.ca/home-accueil/index-eng.asp (last visited on 5 August 2012).

[11] Dominique Clément, *Canada's Rights Movement: A History*. (2010), at http://www.historyofrights.com/ngo.html (last visited on 25 June 2012).

Such groups advocate legal and regulatory changes including data protection and information privacy. In the US, such groups support legal appeals. In CA, such actions are supported by Provincial Legal Aid programs that are controlled by the Provinces with some federal support. The approach started in 1970 under the Trudeau government.[12]

Pierre Trudeau was the fifteenth Prime Minister of CA. He served from 20 April 1968 to 4 June 1979 and 3 March 1980 until 30 June 1984 as one of the most charismatic leaders in CA history. Trudeau was a major force in the enactment of the Charter of Rights and Freedoms, which was longer and more detailed than the US Bill of Rights. The Charter includes democratic rights, equality rights, fundamental freedoms, legal rights, minority language educational rights, mobility rights, and official languages of CA. Trudeau also appointed Chief Justice Laskin, Puisne Justice Wishart Spence, and later Chief Justice Brian Dickson, all of whom supported civil liberties.[13]

In 1960, the Canadian Parliament passed a statutory *Bill of Rights* that had little impact on Supreme Court decisions. The 1982 passage of the constitutional Charter of Rights and Freedoms had a different impact on court decisions. The Charter of Rights and Freedoms changed principles in law and attitudes, and allowed an opportunity for a fair hearing on human rights based cases. The 1960s was a time of international awareness and concern about civil and human rights. Time is needed for such concerns to reflect in the law and in judicial decisions. The period of time between the 1960s and 1990s was an era of massive change for CA. The country became formally independent from the UK, established a new flag, established judicial review over parliament, and dealt with a number of mass movements (including terrorism from French separatists) and political changes. Canada's formal independence started in 1931; however, it was not until 1949 that decisions of

---

[12] Frederick H. Zemans, Legal Aid and Advice in Canada, 16 *Osgoode Hall Law Journal,* 663 (1978).

[13] Ian Bushnell, *The Captive Court: A study of the Supreme Court of Canada*. (McGill-Queen's University Press. 1992).

the Canadian Supreme Court could no longer be appealed to the Privy Council for final determination.[14]

In 1970, the Government of CA suspended civil liberties under the War Measurements Act because of bombings, mail box bombs, and kidnappings by Quebec separatists.[15] In the latter part of the year, civil liberty groups mounted a major campaign against the Royal Canadian Mounted Police (RCMP). The groups exposed a strong pattern of illegal break-ins, intimidation, and wiretapping that resulted in Parliamentary hearings.[16] An equality rights component was started in 1985 but was stopped in 1992 by the Mulroney government.

The CA federal government has passed consumer protection laws and regulations. The major act is the *Financial Consumer Agency of Canada Act*,[17] which addresses banks, credit bureaus, collection agencies, and financial institutions. This act regulates information businesses and protects some personal information. Alberta, British Columbia, Manitoba, New Brunswick, Newfoundland, Nova Scotia, Ontario, Prince Edward Island, Quebec, and Saskatchewan have passed consumer information or consumer protection laws. The laws address unfair practices, warranty, service contract protections and remedies. Moreover, these laws can license agents and companies.[18]

---

[14] Peter H. Russell, The Growth of Canadian Judicial Review and the Commonwealth and American Experiences, *in Comparative Judicial Review and Public Policy* (Donald W. Jackson & C. Neal Tate eds., 1992); Francis Reginald Scott, The Consequences of the Privy Council Decisions, 15 *Canadian Bar Review*, 485 (1937).

[15] Seymour Martin Lipset, *Continental Divide: The Values and Institutions of the United States and Canad*a (C.D. Howe Institute. 1989).

[16] A. Alan Borovoy, *When Freedoms Collide: The Case for Our Civil Liberties* (Lester and Orpen Dennys. 1988).

[17] Canadian Laws, *Canadian Consumer Protection Laws*. (2010), at http://www.canadianlawsite.ca/consumer-protection.htm#g (last visited on 3 January 2012). (CA) See Canadian Marketing Association, *Consumer Protection*. (2010), at http://www.the-cma.org/public/?WCE=C=47|K=224338 (last visited on 27 July 2012).

[18] *Id.*

On January 18, 1994, then Canadian Prime Minister Jean Chretien announced a proposal for a Canadian strategy for the *Information Highway*.[19] The process started with the development of fifteen topics that the Industry Canada Commission should address. Of the fifteen, one topic specifically addressed DPSIP legal issues – "How can personal privacy and security of information be protected? In April, the final report was released in a discussion paper titled *The Canadian Information Highway: Building Canada's Information and Communications Infrastructure*."[20] The commission accurately assessed the DPSIP problems and the major players. The commission concluded that "There is no question that the ability to access, repackage and resell information can … raise concerns among the general public, the business community, and government alike about privacy protection and the security of sensitive information."[21]

The Industry Canada Commission reported that in 1992, the Ekos Research Associates study found that ninety-two percent of 3,000 Canadians studied reported that privacy was important to them and sixty percent believed they had less privacy than a decade before. Respondents wanted control over their information and wanted governmental intervention. A 1994 Gallup CA study found that eighty percent of Canadians reported that privacy was under siege and showed concerns about maintaining privacy.[22]

The commission found that privacy involved "the right to exercise control over one's personal information."[23] Individuals should be able to determine "when, how and to what extent information about them is communicated to others."[24] A 1992 Equifax study of Canadians "found that 84 percent of the insurance, financial and credit bureau executives surveyed believed that federal

---

[19] Industry Canada, *The Canadian Information Highway: Building Canada's Information and Communications Infrastructure / Privacy*. (1994), at http://www.ifla.org/documents/infopol/canada/cihac003.txt (last visited on 1 August 2012).

[20] *Id.*

[21] *Id.* at 1.

[22] *Id.* at 2.

[23] *Id.* at 1:2.

[24] *Id.* at 1:3.

legislation is required to set rules for the collection and circulation of consumer information."[25]

The commission further reported on the Canadian Standards Association model privacy code, which was built on the OECD Guidelines. The standards include accountability, accuracy, challenging compliance, consent (new), identifying purposes, individual access, limiting collection, limiting use, disclosure, retention, openness, and safeguards.[26]

The final Industry Canada Commission report declared that the rule of law should be applied to the information highway. The commission also recommended that federal legislation should protect information privacy and data security – protection that applied to the private and governmental sectors.

5.2 Canadian Federal Constitutional Declarations

In 1867, a Constitutional Act, formerly known as the *British North American Act*, was passed.[27] Much of the structure was not written in the traditional sense. There was no formal Bill of Rights but the Act did establish a British-style parliament with a Senate and a House of Commons, as well as a judicature.

Section ninety-one provided for federal powers while Subsection twenty-nine enumerated powers to the provinces. Using this clause, the Court[28] considered that the regulation of Broadcasting was a provincial matter. The constitution also provided the Federal government power related to issues concerning treaties – similar to the US, CA, and Mexico broadcasting treaty assigning frequencies. Thus, the Federal government had some control over broadcasting.

---

[25] *Id.* at 5:6.
[26] *Id.* at Annexes B. ¶ 5.
[27] Canadian Constitution Act, *Constitution Acts from 1867 to 1982*. (1867), at http://laws.justice.gc.ca/en/const/c1867_e.html (last visited on 2 August 2012). (CA)
[28] *A-G Canada v A-G Quebec*, 2 D.L.R. 81 (JCPC), (1932) (CA).

The CA Constitution Act of 1867[29] does not mention privacy. Section 92(13) addresses property and civil rights. The section applies when personal information is considered a form of personal rather than corporate property or is a civil rights issue.

In 1982, CA passed the Constitution Act which identified fundamental freedoms. The fundamental freedoms included "(*a*) freedom of conscience and religion; (*b*) freedom of thought, belief, opinion and expression, including freedom of the press and other media of communication; (*c*) freedom of peaceful assembly; and (*d*) freedom of association."[30] Part one establishes the rule of law and the need for reasonable limits for a free and democratic society.[31] This charter, much like the US Bill of Rights, establishes a number of fundamental freedoms that creates a zone of privacy and data protection, even if only by inference.

The adoption of the *Canadian Charter of Rights and Freedoms* was not without its critics.[32] The charge was that such macro-legal principles detract from the power of political majorities and resultant political institutions. W. A. Bogart[33] argued that such legislative and political documents give false hope to the poor and disadvantaged because the law generally favors those with power and resources. Others like David Beatty[34] argued that establishment of such legal principles opens the doors of Justice to previously excluded groups, causes, and individuals. The charter does initiate a new role for the Courts and legal support for issue of civil and human rights. Although it has been proposed, the final charter has no provisions for the protection of

---

[29] Canadian Constitution Act, *Constitution Acts from 1867 to 1982*. (1867), at http://laws.justice.gc.ca/en/const/c1867_e.html (last visited on 2 August 2012).
[30] *Id.* at § 2.
[31] Canadian Constitution Act, *The Canadian Charter of Rights and Freedoms*. (1982), at http://laws.justice.gc.ca/en/charter/ (last visited on 25 July 2012).
[32] Rainer Knopff & F. L. Morton, *Charter Politics* (Nelson. 1992).
[33] W. A. Bogart, *Courts and Country: The Limits of Litigation and the Social and Political Life of Canada* (Oxford University Press. 1994).
[34] David Beatty, *Talking Heads and the Supremes: The Canadian Production of Constitutional Review* (Carswell. 1990).

property or property-related due process.[35] In CA, the business community was not as involved in policymaking and litigation as in AU and the US. The only exception was the tobacco business interests and lobbyists.

Chris Schafer identified the major issue in constitutional rights, noting that the *Canadian Charter of Rights and Freedoms* "has the potential to protect our valuable freedoms from state intrusion and interference, but it is up to our judges on the Supreme Court to defend them."[36]

Schafer studied Canadian Supreme Court decisions from 1 January 2000 through 31 December 2006 on the basis of economic freedom, equality before the law, and individual freedom.[37] The court issued pro-freedom decisions eighty-six percent of the time. Sixty percent of the justices were supporters of economic freedom. Seventy percent of the justices supported a pro-equality position.[38] In contrast to the US judiciary, the Canadian judges are appointed as long as there is good behavior.[39] Judges must be members of the Bar,[40] and they must retire at 75 years of age.[41]

5.3 Canadian Federal Legislation

In CA, legal issues related to DPSIP are, in part, addressed under the law of confidential information and tort law. Confidential information law is a part of intellectual property law. Private data is an asset with value. The connection between data protection and information privacy with intellectual property law makes sense. Personal information can be considered as a form of intellectual and personal property. The connection makes even more sense

---

[35] Alexander Alvaro, Why Property Rights Were Excluded from the Canadian Charter of Rights and Freedoms, 24 *Canadian Journal of Political Science*, 309 (1991).
[36] Chris Schafer, *Judging the Judges: How Do Supreme Court Judges Rank?*, Canadian Constitution Foundation. (2007), at http://www.canadianconstitutionfoundation.ca/files/pdf/News-Release-PDF-Judging-the-Judges-10-April-2007.pdf (last visited on 25 July 2012), at 6.
[37] *Id.* at 6.
[38] *Id.* at 6-7.
[39] Canadian Constitution Act, *Constitution Acts from 1867 to 1982*. (1867), at § 99.
[40] *Id.* at § 97.
[41] *Id.* at § 99.

when one considers that intellectual property law can be used to insure that privacy protections are built into all protected technology. The issue is one of ownership. Does the persona who behaviorally creates the information own it or does the corporation that collects it without consent own it?[42]

In 1982, parliament passed the first *Privacy Act*[43] to regulate federal government institutions' collection and disclosure of personal information.[44] The focus of the Act was very narrow.

Prior to the establishment of the European Union Directive of Privacy and Data Protection, the Canadian protections were more advanced than those in the UK. The Canadian Charter of Rights and Freedoms set the federal standard. The provinces were more innovative. A statutory tort of invasion of privacy was established by a number of Canadian Provinces including British Columbia, Manitoba, Newfoundland, and Saskatchewan each of which established similar standards.[45] Such a standard was also found in Quebec's Charter of Human Rights and Freedoms, which established that "every person has a right to respect for his private life" that is directly enforceable between citizens.[46]

5.3.1 Canadian Criminal Code of 1985 - Part VI: Invasion of Privacy

The Canadian Criminal Code (1985) declares that:

> Every one who, by means of any electro-magnetic, acoustic, mechanical or other device, willfully intercepts a private communication

---

[42] See Daniel J. Solove, *Understanding Privacy* (Harvard University Press. 2008). Solove traces the concept back to John Locke. See Lawrence Lessig, *Code and Other Laws of Cyberspace* (Basic Books. 1999).

[43] Canadian Federal Government, *Canadian Privacy Act - R.S.C. 1985, c. P-21*. (1982), at http://laws.justice.gc.ca/en/P-21/index.html (last visited on 7 November 2012). (CA)

[44] *Id.*

[45] John D. R. Craig, Invasion of Privacy and Charter Values: The Common-Law Tort Awakens 42 *McGill Law Journal,* 355, footnote 2. (1997).

[46] Province of Quebec, *Charter of Human Rights and Freedoms*. (2006), at http://www.cdpdj.qc.ca/en/commun/docs/charter.pdf (last visited on 23 July 2012), at § 5.

> is guilty of an indictable offence and liable to imprisonment for a term not exceeding five years.[47]

However, the code provides a number of exceptions. The principle does not apply when one or the other party consented, is legally authorized, has quality monitoring, or protects the system functions. A private communication is defined as when "it is reasonable for the originator to expect that it will not be intercepted" by another and it is set to prevent "intelligible reception" by another not intended.[48] The reasonable expectation clause can be problematic. The definition ignores the principle of proportionality, a balancing of interest measure, or why the interception would be done. The Canadian Criminal Code does not require that the consent be informed.

5.3.2 The Federal Privacy Act of 1985

The purpose of the Canadian Federal Privacy Act of 1985 was to "extend the present laws of Canada that protect the privacy of individuals with respect to personal information about themselves held by a government institution and that provide individuals with a right of access to that information."[49] This act focused only on information held by the government.

The Canadian Federal Privacy Act of 1985 defines personal information as identifiable information that is recorded in any form. The key elements include protected classes; criminal, education, employment, or medical information; identifying numbers; address; or physical markers.[50] The Act proclaims a number of general privacy law principles and limits implementation by listing a number of exceptions and potential bases of non-compliance.

---

[47] Canadian Criminal Code, *R.S.C. 1985, c. C-46*. (1985), at http://www.canlii.org/ca/sta/c-46/sec184.html (last visited on 15 August 2012), at § 184, ¶ 1.

[48] *Id.* at § 184, ¶ 6.

[49] Canadian Privacy Act, R.S.C. 1985, c. P-21 (1985), at ¶ 2.

[50] *Id.* at § 3:14. The section reads - "(a) information relating to the race, national or ethnic origin, color, religion, age or marital status of the individual, (b) information relating to the education or the medical, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved, (c) any identifying number, symbol or other particular assigned to the individual, (d) the address, fingerprints or blood type of the individual."

Under Section Three Part J, personal information does not include information about an individual who is or was an officer or employee of a government institution that relates to the person's government position or functions, such as government business address and phone number, classification of position, personal opinions on subjects in the course of government employment, responsibilities, salary, titles, and written documents.[51] The Act allows the head of a governmental institution to release personal information for any purpose. The head must only argue the release benefits the individual or that the public interests supersede.[52]

Section Five of the Act provides key elements ignored in the US approach. The code declares that collected information should be obtained directly from the person except where the individual authorizes otherwise or where the collection is acceptable under Subsection 8(2), which enumerates certain circumstances where personal information may be collected and disclosed.[53] The government must inform the person of the data collection and the purpose of the record.[54]

The Act also adopts a significant structural approach ignored in the US. The Act appoints a Privacy Commissioner of CA (PCC) who has wide powers of investigation and the power to consider complaints. However, the Commissioner, who reports to the Parliament, can be removed from office for cause from the statutory seven year term at any time and functions in an advisory and conciliatory function. The Commissioner does not have the power to adjudicate cases or issue legally binding opinions.[55] The office is not an independent agency.

---

[51] *Id.* at § 3:J.
[52] *Id.* at § 8(2)(m).
[53] *Id.* at § 5: ¶ 1.
[54] *Id.* at § 5: ¶ 2.
[55] *Id.* at § 53.

5.3.3 The Personal Information Protection and Electronic Document Act (PIPEDA)

On April 13, 2000, the *Personal Information Protection and Electronic Document Act* (PIPEDA) was enacted.[56] The Act focuses on how personal information is collected, secured, and shared within CA and with its trading partners. Personal information is defined as "information about an identifiable individual, but does not include the name, title or business address or business telephone number of an employee of an organization."[57] A major constraint is that PIPEDA applies only to conduct and transactions of a commercial nature. The provinces could pass substantially similar legislation and bypass the federal statue for intra–provincial actions. The federal legislation would apply to all provinces, inter-provincial, and international personal data collection, disclosure, and use. PIPEDA applies to all data collection of personal information of all Canadians and all data collected in CA.

PIPEDA was described as a new gold standard: "the first (Canadian) determined effort to place a check upon, and ultimately to reverse, the massive erosion of individual privacy rights brought about by the application of computer and communications technology in the commercial world."[58]

PIPEDA was implemented in three phases. On 1 January 2001, all commercial functions that were subject to the Canadian Labor Code were covered. On 1 January 2002, all data collection of personal health information was covered. On 1 January 2004, the full impact of PIPEDA took effect. The phased approach allowed the government time to inform the target stakeholders, establish regulations, and enforce the standards. Business

---

[56] Canadian Federal Government, *Personal Information Protection and Electronic Document Act*. (2000), at http://laws.justice.gc.ca/en/showtdm/cs/P-8.6 (last visited on 1 November 2012). (CA)

[57] *Id.* at Part 1, ¶.13.

[58] Bruce Phillips, *Foreword*, *in The Personal Information Protection and Electronic Documents Act: An Annotated Guide* (Stephanie Perrin, et al. eds., 2001), at ix.

organizations and all concerned parties were informed of the new policy so the principle of predictability was met.

Under PIPEDA, notice and consent was required for the collection, disclosure, or use of personal information in the course of commercial activities. The principle of consent was also required whenever the information was used for any secondary purpose.

Ten principles governed the collection and the use of data under PIPEDA. Organizations were required to ensure that any parties that were involved in the transfer of data follow the principles of accountability, accuracy, consent, identifying purpose, individual access, limited collection, limited use, disclosure and retention, openness, and safeguards.[59]

PIPEDA regulated the collection, disclosure, storage, and use of personal data by businesses. In 2001, the Act applied to federally regulated organizations including airlines, banks, broadcasting, and

[59] Canadian Federal Government, *Personal Information Protection and Electronic Document Act*. (2000), at http://laws.justice.gc.ca/en/showtdm/cs/P-8.6 (last visited on 1 November 2012), at Schedule 1. The terms are defined as: **Accountability:** Organizations have to appoint a compliance officer within the organization. The officer and the organization are responsible for all personal information collected, disclosed, used, or transferred. **Accuracy:** All personal information must be accurate, complete, and current. The sensitivity of the information and purpose of holding the data impacts the risks. **Consent:** With a few exceptions, individuals must actively know and consent. Consent applies to the collection, disclosure, transfer, or use of one's personal information. One can also withdraw consent at any time. **Identifying purpose:** Organizations must identify all purposes for handling personal information. The purpose communication must be done before or at the time of the collection. **Individual access:** Individuals, upon request, must be given access to held information. The disclosure, existence, and use of the information must be divulged. The individual has the right to challenge the accuracy and completeness of the data. The individual can have the organization amend the data as appropriate. Complaints related to access denial must be filed with the PCC within six months of the refusal. **Limiting collection:** The collection of personal information must be limited to the necessary identifying purpose. Legal collection policies also apply. **Limiting use, disclosure, and retention:** Use or disclosure of personal information can be used only for the purpose for which it was collected. Legal standards and individual consent can override the limitation. The data can only be retained as long as necessary determined by its purpose. **Openness:** Information practices and organizational privacy policies must be available. Individuals can make requests related to how the information is managed. **Safeguards:** Organizations must establish and maintain security safeguards. The more sensitive the data, the higher the safeguards must be.

telecommunications companies in all ten provinces and all three territories. The Act included individual health information the next year. In 2004, all Canadian businesses were expected to comply with the Act or equivalent provincial regulation and all inter-provincial and international personally identifiable information. In 2002, the European Union classified the Canadian approach as equivalent to the 1995 Data Protection Directive. The action allowed free data flow between EU countries and CA.

With privacy legislation and court decisions, the issue of effectiveness of DPSIP protection is usually found in the exemptions. The PIPEDA provisions provide some common but troublesome exemptions that allow information to be collected and shared.

Given the current fervor related to terrorism, perhaps the most emotional and easiest exception in the standard can occur when an organization or person "suspects that the information relates to national security, the defence of Canada or the conduct of international affairs."[60] A secondary standard is when an organization or person "has reasonable grounds to believe that the information relates to a breach of an agreement or a contravention of the laws of Canada, a province or a foreign jurisdiction that has been, is being or is about to be committed."[61] The person or organization making the judgment determines if it is reasonable. No checks or balances are required.

The CA government can ignore the provisions of informational privacy provisions when "required by law" or "it is specified by the regulations" or the "disclosure is requested for the purpose of administering or enforcing any law of Canada, a province or a foreign jurisdiction."[62] Both of the standards are of course determined by the government itself. Governmental administrations have violated the spirit and letter of the principles of the Rule of Law; both CA and the US have violated civil liberties and human rights.

---

[60] *Id.* at §1 (3)(i), 8.
[61] *Id.* at (d)(i), 8.
[62] *Id.* at (c.1) (iii), 8.

The governmental exemption includes whenever "it suspects that the information relates to national security, the defence of Canada or the conduct of international affairs;"[63] or the government is "carrying out an investigation relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing any such law."[64] Privacy can also be violated whenever the government determines that the "the disclosure is requested for the purpose of administering any law of Canada or a province" or "made by an investigative body and the disclosure is reasonable for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province."[65] Organizations may also claim an exemption. The major factor required is that the organization has reasonable grounds to believe that the information could be useful in investigating or contravening possible unlawful activities.[66] Organizations also have a further exemption. Organizations can take the initiative to "an investigative body, a government institution or a part of a government institution and the organization."[67]

Some exemptions include court action. Two provisions are noted. The first is that the release is "required to comply with a subpoena or warrant issued or an order made by a court, person or body with jurisdiction to compel the production of information, or to comply with rules of court relating to the production of records."[68] The second applies when a request is "made to a government institution or part of a government institution that has made a request for the information and identified its lawful authority to obtain the information."[69] When the information is publicly available, a general exemption from PIPEDA applies. The problem may be that the legislation does not require that the public information meet legal standards. Private information that is "publicly available and is specified by the regulations" is exempt.[70] The

[63] *Id.* at (c.1) (i), 7.
[64] *Id.* at (c.1) (ii), 7.
[65] *Id.* at (h) (2), 9.
[66] *Id.* at (3)(a), 6.
[67] *Id.* at (3)(c), 6.
[68] *Id.* at (3)(c), 7.
[69] *Id.* at (3)(c.1), 7.
[70] *Id.* at (7)(d), 7.

exemption even applies when the information is unlawfully released to the public.

The law makes exceptions for public policy reasons. No knowledge or consent is required when the private information is collected "solely for journalistic, artistic or literary purposes."[71] A further exemption covers when the "collection is made for the purpose of making a disclosure"[72] as in whistle blowing. Debt collection efforts are an exception when the individual owes a debt to the organization. An exemption also covers data made available "to an institution whose functions include the conservation of records of historic or archival importance, and the disclosure is made for the purpose of such conservation."[73]

A confidentiality principle applies when relevant and needed data is used for research, scholarly study, or statistical analysis. In such situations, notice must be provided to the Privacy Commissioner prior to any use. A typical but potential area of abuse of an exception relates to legal investigations. PIPEDA exempts privacy protections when the organization reasonably expects that obtaining consent would compromise the data accuracy or there might be an agreement breach or would be unlawful.[74]

Section Four, Principle Four, specifies limitations on the collection of data protection and information privacy information. The code specifies that "The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means."[75] PIPEDA further declares that data can not be indiscriminately collected and must be used for identified purposes. The openness principle requires that the organization specify purposes and

---

[71] *Id.* at (7)(c), 7.
[72] *Id.* at (7)(e), 7.
[73] *Id.* at (3)(g), 8.
[74] *Id.* at (7)(1)(g),6.
[75] *Id.* at (4.4) (4), 36.

policies.[76] Data collection must be fair and lawful rather than deceitful and misleading.[77]

Under Section Four, Part Three, consent is required except in situations involving legal, medical, or security issues. The problem incorporates the fact that charity and direct marketing are also included. The two principles serve very different purposes. PIPEDA specifies that "Consent is required for the collection of personal information and the subsequent use or disclosure of this information."[78] The organization must provide knowledge to the individual about the purpose of the information collection, disclosure, and use. The attempt need only be reasonable.[79] Consent can not be a condition to receive products, services, or supplies.[80] Price or other inducements can be used. The Act does not require a standard informed consent formula. Consent provisions are contradictory and can delude the spirit of the principle. Provisions allow for express or implied consent depending on circumstance, types of data, or sensitivity based on the organization's position.[81]

Section Four, Part Five, Principle Five limits the disclosure, use, and retention of DPSIP data. PIPEDA requires that data can only be held for as long as the purpose requires. Unless the individual consents, the data can be used for the stated purpose only. If the data is used for a new purpose, the organization needs only to document the change.[82]

Organizations are required to develop and follow minimum and maximum retention periods.[83] Organizations must also develop and follow guidelines to guarantee that "personal information that is no longer required to fulfill the

---

[76] *Id.* at (§4.8) (4.4.1), 36.
[77] *Id.* at (§ 4.4.21), 36.
[78] *Id.* at (¶ 4.3.1), 34.
[79] *Id.* at (¶ 4.3.2), 35.
[80] *Id.* at (¶ 4.3.3), 35.
[81] *Id.* at (¶ 4.3.6), 35.
[82] *Id.* at (§ 4.5.1), 36.
[83] *Id.* at (§ 4.5.2), 37.

identified purposes should be destroyed, erased, or made anonymous unless a new purpose is documented."[84]

Section Four, Principle Six, establishes a standard of accuracy. "Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used." When information is used on an on-going basis, the data must still be accurate and up-to-date.[85]

A set of potentially ambiguous and subjective exceptions was also written into PIPEDA. Collection of personal information may occur when it "is clearly in the interests of the individual and consent cannot be obtained in a timely way."[86] A further potential abuse may occur when the information is "used for the purpose of acting in respect of an emergency that threatens the life, health or security of an individual."[87] The person must be alive; if collected without the individual's knowledge or consent, the organization must provide written notice to the person "without delay."

A reasonable timeline for exemptions includes a twenty year protection that tolls after the death of the person. Another standard may exempt data for one hundred years after the information record was created. The later standard may be similar to the continuing closure of the John F. Kennedy secret files related to his assassination. Rather than protecting informational privacy of the person, the goal may be related to political purposes.

5.3.4 The Canadian Anti-Spam Act

The CA Anti-Spam Act (CA-ASA)[88] was passed in 2010 and in 2012 began to be enforced. CA-ASA has considerable DPSIP implications. The Act establishes a standard of expressed or implied consent for processing of

---

[84] *Id.* at (§ 4.5.3), 37.
[85] *Id.* at (§ 4.6.3), 37.
[86] *Id.* at (¶ 7.1.a), 6.
[87] *Id.* at (¶ 2.b), 7.
[88] *Statutes of Canada 2010; Chapter 23: Anti-Spam* amend. Third Session, Fortieth Parliament, 59 Elizabeth II, 2010 § (2010). (CA)

individual information. Consent is required for all malware and spyware programs. CA-ASA requires a clear unsubscribe mechanism. The Act allows for a private cause of action. The maximum penalty for an individual is $1 million CAD and $10 million CAD for a corporation.[89] CA-ASA establishes that business interests are not above checks and balances constraints.

5.4 Canadian Federal Case Law

The CA and US court structure and system are similar. While CA is more closely connected to British common law tradition than the US, comparing the two structures and powers provides insights into how DPSIP case law decisions are processed.

Table 5.0 Comparison of Canadian and United States Supreme Court

Factor	Canadian Supreme Court[90]	US Supreme Court[91]
Established	1875	1789
Power of decisions	Applies to all courts and jurisdictions in the country	Applies to all courts and jurisdictions in the country
Membership	One Chief Justice and eight puisne justices.	One Chief Justice and eight associate justices (currently)
Appointee Background	Leading appellate courts judges, politicians, and law professors.	Leading appellate courts judges, politicians, and law professors.
Term of Office	Retire at 75 years old	Life or until retires
Jurisdiction	Original and appellate	Original and appellate
Role	Law-clarification	Error-correction
Operations	Hears oral arguments but relies heavily on arguments presented in written briefs	Hears oral arguments but relies heavily on arguments presented in written briefs

[89] *Ibid*.

[90] World Wide Legal Information Association, *Legal Resources*. (2010), at http://www.wwlia.org/LegalResources.aspx (last visited on 4 July 2012). See also Supreme Court of Canada, *About the Court*. (2010), at http://www.scc-csc.gc.ca/court-cour/index-eng.asp (last visited on 5 July 2012).

[91] Kermit L Hall, *The Oxford Companion to the Supreme Court of the United States* (Oxford University Press 2nd. ed. 2005). See also Supreme Court of the United States, *About the Supreme Court*. (2010), at http://www.supremecourt.gov/ (last visited on 5 July 2012).

Decisions	Opinion of the majority, written by one justice, and concurring and dissenting opinions of other justices.	Opinion of the majority, written by one justice, and concurring and dissenting opinions of other justices.
Judicial Review	Recent - 1970	Historic since Marshall.
Appointment	Prime Minister directly appoints justices; no Parliament confirmation.	President nominates, Senate confirms.
Representation	Generally regional	Recently more political
Opinions	Reference cases - Can render advisory opinions	No advisory opinions
Case Assignment	Since 1975, Court has discretion on selected cases.	Court determines what cases it will hear based on writ of certiorari. Since 1925, has discretionary docket control.

Canadian jurists accept British common law traditions. The UK case of *Morison v. Moat*[92] verified an obligation to not violate confidence. The case involved a confidential media formula that was shared with a business partner. The partner then shared the formula with his son who used the information to set up another company. The court found that the son had breached the faith of confidentiality or privacy. Dispersion of information was a breach of faith and an obligation of confidence. The Vice-Chancellor wrote, "[that] the Court has exercised jurisdiction in cases of this nature does not, I think, admit of any question."[93]

In 1970, The Canadian Supreme Court, for the first and only time, ruled that an act of Parliament was a violation of the 1960 Canadian Bill of Rights. The Act was Section 94(b) of the Indian Act that made it illegal for *Indians* to be

[92] *Morison v. Moat*, 68 Eng. Rep. 492, 9 HARE 241, (1851), 498 (U.K.).
[93] *Id*.

intoxicated when off the reserve.[94] The Court ruled that the section violated Section 1(b) of the Bill of Rights.[95]

Starting in 1974 through 1984, the Canadian Supreme Court established new criterion for standing. Three major cases, the standing trilogy, included *Thorson v. A. G. of Canada,* [96] *Nova Scotia Board of Censors v. McNeil*,[97] and *Minister of Justice of Canada v Borowski.*[98] In *Minister of Justice of Canada v Borowski,* Justice Martland summarized the new standing factor. The plaintiff must show that he is affected directly, has a genuine interest, or that "there is no other reasonable and effective manner in which the issue may be brought before the Court."[99]

In *Finlay v. Minister of Finance of Canada*,[100] the Canadian court allowed for standing in non-constitutional cases. Standing is an essential factor in DPSIP law.

The Canadian Supreme Court rulings on privacy protections in criminal cases mirrored similar rights found by the US Warren Court findings. The rights included protections against unreasonable search or seizure.[101]

Three members of the Court helped to establish an agenda of civil liberties during the pre-1982 statutory period. Bora Laskin (Chief Justice, 1973 to 1984 and puisne justice 1970 to 1973), Emmett Hall (Puisne Justice, 1962 to 1973), and Ivan Rand (puisne justice, 1943 to 1959) led the movement.[102]

---

[94] The more politically correct term is now native peoples See Daphine A. Dukelow & Betsy Nuse, *The Dictionary of Canadian Law* (Carswell 2 ed. 1995).
[95] *R. v. Drybones*, S.C.R. 282, 9 D.L.R. (3d) 473, 3 C.C.C. 355, 10 C.R.N.S. 334, 71 W.W.R. 161, (1970). (CA)
[96] *Thorson v. Attorney General of Canada*, 1 S. C.R. 138, (1975). (CA)
[97] *Nova Scotia Board of Censors v. McNeil*, 2 S.C.R. 265, (1976). (CA)
[98] *Minister of Justice of Canada v. Borowski*, 2 S.C.R. 575, (1981). (CA)
[99] *Id.* at 598.
[100] *Finlay v. Minister of Finance of Canada*, 2 S.C.R. 607, (1986). (CA)
[101] Robert Harvie & Hamar Foster, Different Drummers: The Supreme Court of Canada, American Jurisprudence and the Continuing Revision of Criminal Law Under the Charter, 24 *Ottawa Law Review*, 39 (1992).
[102] James G. Snell & Frederick Vaughan, *The Supreme Court of Canada: History of the* Institution (University of Toronto Press. 1985).

The 1982 Constitution Act established a base for establishing a right to privacy. Justice Dickson[103] in *Hunter v. Southam Inc* ruled that Section Eight of the Constitution Act protected the right of people to be left alone by others. Four years later, the Canadian Supreme Court declared that "privacy is at the heart of liberty in a modern state, (and) grounded in a man's physical and moral autonomy, privacy is essential for the well-being of the individual."[104] The court ruled that there were three zones of privacy including territorial or spatial, physical space, and informational privacy. Under Section Eight of the Constitution Act, informational privacy was more important than physical privacy.

Hunter v Southam[105] also interpreted Section Eight on the issue of "unreasonable search or seizure." The Court determined that the Constitution Act protects an "individual's reasonable expectation of privacy." Chief Justice Dickson declared that "an assessment must be made as to whether in a particular situation the public's interest in being left alone by the government must give way to the government's interest in intruding on the individual's privacy in order to advance its goals."[106]

Justice La Forest also found three zones of privacy in Canadian law. In *R. v. Dyment*,[107] La Forest found informational, personal, and territorial privacy zones. He argued that the law should "identify[ing] those situations where we should be most alert to privacy considerations … Grounded in a man's physical and moral autonomy, privacy is essential for the wellbeing of the individual. For this reason alone, it is worthy of constitutional protection." The Justice determined that information privacy was essential to the democracy and the individual person.[108]

---

[103] *Hunter v. Southam Inc,* 2 S.C.R. 145, 11 D.L.R. (4th) 641, 41 C.R. (3d) 97, (1984). (CA)
[104] *R. v. Dyment*, 2 S.C.R. 417 at 427-428, 55 D.L.R. (4th) 503, 66 C.R. (3d) 348, (1988), at 427-428. (CA)
[105] *Hunter v Southam*, 2 S.C.R. 145, (1984), 159-160. (CA)
[106] *Id.*
[107] *R. v. Dyment*, 2 S.C.R. 417 at 427-428, 55 D.L.R. (4th) 503, 66 C.R. (3d) 348, (1988), 427. (CA)
[108] *Id.*

Under Canadian law, information privacy is based on the principle that "all information about a person is in a fundamental way his own, for him to communicate or retain for himself as he sees fit."[109] The *Dyment* court ruled the following:

> [I]n modern society, especially, retention of information about oneself is extremely important. We may, for one reason or another, wish or be compelled to reveal such information, but situations abound where the reasonable expectations of the individual that the information shall remain confidential to the persons to whom, and restricted to the purposes for which it is divulged, must be protected.[110]

Matthew Englander purchased unlisted residential telephone service from Telus Communications. Telus imposed an initial set-up cost and charged monthly fees. Englander objected because he had not been given informed consent, which was a violation of PIPEDA on the ground of collection, disclosure, and use of personal data.

In *Englander v. Telus Communications, Inc*,[111] the Federal Court of Appeals found that Telus did not provide informed consent and in fact, sold the listing information. Telus was found in violation of Section Five of PIPEDA in "not informing its first-time customers, at the time of enrollment, of the primary and secondary purposes for which their personal information was collected and in not informing them at the time of availability."[112] The justices suggested that common sense, flexibility, and pragmatism should be applied to DPSIP legal decision-making. Organizations must fully inform persons regarding all of the purposes of the collected information at or before collection and before use. New uses must be communicated to data subjects, unless the use is

---

[109] Information Canada, *Privacy and Computers* (A Report of a Task Force Established Jointly by Department of Communications/Department of Justice) (Author. 1972), 13.
[110] *Id.* at 429-430.
[111] *Englander v. Telus Communications, Inc*., 2004 FCA 387 (Federal Court of Appeal 2004), §, 89. (CA)
[112] *Id.*

mandated by law. Consent is not informed if the person is not aware of opt-out options at the time of giving the consent.

Elizabeth Paton-Simpson argued that public privacy furthers the common good. Privacy protection is connected to "freedom, individual self-fulfillment, autonomy, independent thought, and human dignity."[113] The issue of public privacy is related to DPSIP law and policy. The argument that computer and Internet activities are public is flawed. If accepted, there can be no expectation of privacy. The principle is logically challenged and diminished.

In *X. v. Accusearch Inc., dba Abika.com et al*, [114] the Canadian Federal Court ruled that the Privacy Commissioner's Officer had jurisdiction over US companies operating in CA. The issue was related to transborder flow of personal information.[115] The decision also has implications for outsourcing data functions.

Telus Communications instituted a voice recognition security system. The employees filed a complaint. The Federal Appeals Court found that voice prints are personal information, but the company has a reasonable right to have a security system. Employees consented[116] to the system by sharing the data; the company told the employees of the consequences if they refused.[117]

In *R. v. Plant*, [118] Justice McLachlin declared:

> Computers may and should be private places, where information they contain is subject to the legal protection arising from a reasonable expectation of privacy. Computers may contain a wealth of personal information. Depending

---

[113] Elizabeth Paton-Simpson, Privacy and the Reasonable Paranoid: The Protection of Privacy in Public *Places*, 50 *University of Toronto Law Journal* 3, 305-346 (2000), 305.

[114] *X. v. Accusearch Inc., dba Abika.com et al*. Federal Court File No. T–2228–05, (2007). (CA)

[115] *Id.*

[116] Is it really informed consent when pressure is applied?

[117] *X. v. Telus Communications Inc*. Federal Court of Appeal File No. A–639–05, (2007). (CA)

[118] *R. v. Plant,* 3 S.C.R. 281 (S.C.C.), (1993), at 303-304. (CA)

> on its character, that information may be as private as any found in a dwelling house or hotel room.[119]

The Supreme Court found that when confidential or personal information is involved, the government needs prior authorization to search or seize the data from data bases. No authorization is needed when the information is not confidential or personal.

The case of *Dr. Jeffrey Wyndowe*[120] was decided by the Federal Court of Appeals. The case involved a patient who wanted access to medical records that were obtained during an insurance company's independent medical examination (IME). The Court found the notes were subject to PIPEDA because the data was obtained during a commercial activity and clearly contained personal information. The patient has legal access rights and the right to correct any errors. The Court also found that the notes had personal information related to the IME and that the review should be mediated.[121]

The principle of informed consent is, in part, based on Section Seven of the Canadian Charter of Rights and Freedoms. The section reads: "Everyone has a right to life, liberty and security of the person and the right not to be deprived thereof except in accordance with the principles of fundamental justice."[122] The concept was validated in *Rodriguez v. British Columbia.*[123]

In *Marcoux v. Bouchard*, [124] the Canadian Supreme Court ruled that no one can interfere with the integrity of another except with one's free and enlightened consent or legal authorization. Persons, procedures, and purpose must be protected.[125]

---

[119] *Id.*
[120] *Dr. Jeffrey Wyndowe (Psychiatric Assessment Services Inc.) v. X*. Federal Court of Appeal File No. A–551–06, (2008). (CA)
[121] *Dr. Jeffrey Wyndowe (Psychiatric Assessment Services Inc.) v. X*. Federal Court of Appeal File No. A–551–06, (2008). (CA)
[122] Canadian Constitution Act, *The Canadian Charter of Rights and Freedoms*. (1982), at http://laws.justice.gc.ca/en/charter/ (last visited on 25 July 2012), § 7.
[123] *Rodriguez v. British Columbia* (Attorney-General) 107 D.L.R. (4th) 342 (SC.C.), (1993). (CA)
[124] *Marcoux v. Bouchard*, 204 D.L.R. (4th) 1 [S.C.C.], per Heureux-Dube, Gonthier, Bastarache, Arbour and LeBel JJ. (decided on September 13, 2001). (CA)
[125] *Id.*

Under the 1996 Ontario Health Care Consent Act,[126] a pivotal special tribunal was established to intercede in consent issues. The tribunal functions as an arbitration body but with legal powers. Such a function may be needed in data protection and information privacy cases. The Courts tend to give deference to its decisions. Personal autonomy and best interests are a major focus that is fully recognized.

In *R. v O'Connor,*[127] the Supreme Court addressed privacy of confidential medical records and the accused's ability to mount a defense.[128] The case involves a charge of sexual assault. The accused requested copies of the complainant's counseling and medical records held by third parties. The DPSIP legal issue is the complainants' privacy interest in confidential records and the accused's right to answer the charges. The Court wanted to balance the interests. Lamer and Sopinka wrote that given that the complainant shared the records with the Crown, there is no expectation of privacy. Part of the balancing test also includes the impact on one's dignity, privacy, and security. L'Heureux-Dubé dissented, with La Forest and Gonthier concurring. Privacy is a right protected by the right to liberty. While privacy is not absolute, it is equal in balancing other rights or interests. The majority of the Court agreed.

In partial response to the *O'Connor* decision, the Parliament amended the Criminal Code, which is different from the Court's prior ruling. The *R. v Mills*[129] case found that the legislative adjustment was constitutional. The majority of the Court found that Section Eight of the Constitution Act protects the right to privacy. The court determined that in information privacy situations, Sections Seven and Eight of the Constitution Act may apply.

---

[126] Ontario Health Care Consent Act amend. c. 10, Sched. R, s. 14 (1996). (CA)

[127] *R. v O'Connor*, 1995 CarswellBC 1098, [1996] 2 W.W.R. 153, [1995] 4 S.C.R. 411, 44 C.R. (4th) 1, 103 C.C.C. (3d) 1, 130 D.L.R. (4th) 235, 191 N.R. 1, 68 B.C.A.C. 1, 112 W.A.C. 1, 33 C.R.R. (2d) 1, (14 December 1995). (CA)

[128] *Id.*

[129] *R. v Mills*, 1999 CarswellAlta 1055, 139 C.C.C. (3d) 321, 248 N.R. 101, 28 C.R. (5th) 207, [2000] 2 W.W.R. 180, 244 A.R. 201, 209 W.A.C. 201, 75 Alta. L.R. (3d) 1, 180 D.L.R. (4th) 1, 69 C.R.R. (2d) 1, [1999] 3 S.C.R. 668, 1999 CarswellAlta 1056, [1999] S.C.J. No. 68, (19 January 1999). (CA)

In a long history of *Ruby v Canada*[130] litigation, Ruby challenged provisions of the *Privacy Act.*[131] Ruby wanted complete access to his personal information held by three governmental agencies and argued that Section fifty-one of the Privacy Act was invalid under the Constitution Act. Ruby argued freedom of speech, security, and access issues. The Court found that privacy is the heart of liberty and that it includes information privacy. The Court found that Section fifty-one of the Privacy Act was only a procedural provision. A challenge of Section Seven of the Constitution Act was rejected.

After *Mills*, the court has found that the right to privacy includes control of personal information. In *R v Wise,*[132] the Supreme Court found that Section Eight of the Charter provides some privacy rights. The section protects against unreasonable search and seizure. When there is no reasonable expectation of privacy, the section is not engaged. Where there is a reasonable expectation of privacy, broad and general rights protect one from unreasonable searches.

An interesting and related test case involved a number of people who donated blood and provided personal information for that purpose to the Canadian Red Cross. About ten years later, the Red Cross tested some of the frozen donations for AIDS. The organization reported the names of those that tested positive to public health officials as required under the *Health Protection and Promotion Act*.[133] The Canadian AIDS Society filed suit alleging violation of an expectation of privacy and no consent for future release was given. The Supreme Court found that there was a reasonable expectation of privacy that was violated. The Court also found that there is a lower standard of

---

[130] *Ruby v Canada (Solicitor General)* 2000 CarswellNat 1106, 256 N.R. 278, 184 F.T.R. 159 (note), 6 C.P.R. (4th) 289, [2000] 3 F.C. 589, 2000 CarswellNat 3423, 187 D.L.R. (4th) 675, 3 F.C. 589, 2000 F.C.J. No. 779, 42 Admin. L.R. (3d) 214). (CA)

[131] *Id.*

[132] *R. v. Wise*, 1992 CarswellOnt 71, 11 C.R. (4th) 253, [1992] 1 S.C.R. 527, 70 C.C.C. (3d) 193, 133 N.R. 161, 8 C.R.R. (2d) 53, 51 O.A.C. 351, (27 February 1992). (CA)

[133] Health Protection and Promotion Act amend. R.S.O. 1990, CHAPTER H.7

reasonableness when there is a legitimate public health state interest. In this case, the public interest outweighs the information privacy right.[134]

A further clarification of Canadian DPSIP protections arose when the Treasury Board of Canada Secretariat issued Privacy Impact Assessment Guidelines.[135] The guidelines require a privacy impact assessment on the government's adoption of initiatives, information systems, proposed policies and programs, and new technologies. The guidelines help organizations comply with the federal DPSIP law and establish a gold standard for compliance. The Court ruled that the standards are not binding but do help in interpretation of the legislation.[136]

In another important case, a newspaper reporter requested access to audited financial records that included public grant and distribution data. The Supreme Court found that access to membership records of small groups can include protected personal information.[137] The decision has implications for data mining situations.

---

[134] *Canadian AIDS Society v. Ontario (1995)*, 1995 CarswellOnt 1720, 25 O.R. (3d) 388 (Ont. Gen. Div.); affirmed Canadian AIDS Society v. Ontario (1996), [1996] O.J. No. 4184, 39 C.R.R. (2d) 236, 31 O.R. (3d) 798, 1996 CarswellOnt 4604 (Ont. C.A.); leave to appeal refused Canadian AIDS Society v. Ontario (1997), [1997] S.C.C.A. No. 33, (sub nom. Canadian Aids Society v. Ontario) 107 O.A.C. 80 (note), 216 N.R. 159 (note), 43 C.R.R. (2d) 188 (note) (S.C.C.), (1997). (CA)

[135] Treasury Board of Canada Secretariat, *Privacy Impact Assessment Guidelines: A Framework to Manage Privacy Risks*. (2002), at http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paipg-pefrld2-eng.asp (last visited on 20 July 2012).

[136] *Canada Post Corp. v. Canada (Minister of Public Works) (1995)*, [1995] F.C.J. No. 241, 60 C.P.R. (3d) 441, 91 F.T.R. 320 (note), (sub nom. Societe Canadienne des postes v. Canada) [1995] 2 F.C. 110, 179 N.R. 350, 30 Admin. L.R. (2d) 242, 1995 CarswellNat 688, 1995 CarswellNat 652 (Fed. C.A.), (10 February 1995). (CA) See also *Canada (Information Commissioner) v. Canada (Minister of Citizenship & Immigration)*, 2002 CarswellNat 1476, 2002 FCA 270, 291 N.R. 236, 228 F.T.R. 319 (note), [2003] 1 F.C. 219, 21 C.P.R. (4th) 30, 1 Admin. L.R. (4th) 270, (21 June 2002). (CA)

[137] *Montana Band of Indians v. Canada (Minister of Indian & Northern Affairs) (1988)*, 1988 CarswellNat 723, 26 C.P.R. (3d) 68, [1989] 1 F.C. 143, 51 D.L.R. (4th) 306, [1988] 5 W.W.R. 151, 31 Admin. L.R. 241, 18 F.T.R. 15, 59 Alta. L.R. (2d) 353, [1988] 4 C.N.L.R. 69, 1988 CarswellNat 1202 (Fed. T.D.), (15 April 1988). (CA)

In *Rousseau v. Wyndowe*,[138] a disability claimant wanted full release of the notes written by an independent medical examiner. The notes included personal and non-personal information. The claimant had obtained a copy of the report but wanted total access to the physician's records on the case. The Supreme Court ruled that the information is personal information and personal health information. The claimant could only have access to notes directly related to him.

Under the common law tradition, the Federal Courts help to define and refine DPSIP legal standards. In CA, the Office of the Privacy Commission of Canada also has power to establish regulatory findings. The Commissioner publishes relevant findings.[139]

5.5 Canadian Provincial Constitutional Declarations

Most modern countries have a set written constitution. The pattern usually applies to subunits like states or provinces. CA uses a Constitution Act at the Federal and Provincial level. The governmental levels also have a range of conventions and unwritten laws. All of these documents have the force of law.[140] The Federal and Provincial Acts do not directly grant any constitutional DPSIP legal standards. Specific provincial legislation does address such issues; however, not at a constitutional level.

5.6 Canadian Provincial Legislation

The various Canadian provinces have enacted privacy-related legislation. Most provinces have enacted laws that basically apply to governmental or public entities.

---

[138] *Rousseau v. Wyndowe* A-551-06, 2008 FCA 39, (2008) 2 F.C.R. D-12, (1 February 2008). (CA)

[139] See Office of the Privacy Commission of Canada, Commissioner's Findings - http://www.priv.gc.ca/cf-dc/index_e.cfm (last visited on 25 July 2012).

[140] Canadian Constitutional Documents, *A Legal History*. (2004), at http://www.solon.org/Constitutions/Canada/English/ (last visited on 6 July 2012). The source includes federal and provincial documents.

The strongest provincial declaration of privacy is Section Five of *Quebec's Charter of Human Rights and Freedoms.*[141] The section declares that "Every person has a right to respect for his private life."[142] British Columbia,[143] Manitoba,[144] Newfoundland,[145] and Saskatchewan[146] have enacted tort legislation for invasion of privacy. The laws provide for a balancing–proportionality test. Expressed or implied consent and actions to protect a legal right are legitimate exceptions. David H. Flaherty maintains that provincial tort privacy laws have "rarely been used, they have not been very successful, and they really do not address, successfully, the four privacy torts that Dean William Prosser identified."[147]

Three provinces, Alberta, British Columbia, and Quebec have enacted DPSIP legislation. Some CA provinces have also enacted some sectoral laws related to privacy concerns.

5.6.1 Alberta Personal Information Privacy Act

In 2003, the Province of Alberta passed the Personal Information Protection Act. Section Three explains the purpose as protecting individual rights related to the "collection, use and disclosure of personal information by organizations … that recognizes both the right of an individual to have his or her personal information protected and the need of organizations to collect, use or disclose personal information for purposes that are reasonable."[148]

---

[141] Province of Quebec, 2006, § 5.
[142] *Id.*
[143] Province of British Columbia, 2005, §1,4.
[144] Province of Manitoba, 1998, § 2,3,5.
[145] Province of Newfoundland, 2002, § 3,4.
[146] Province of Saskatchewan, 2006, § 2,4,6.
[147] David H. Flaherty, Some Reflections on Privacy and Technology, 26 *Manitoba Law Journal* 2, 219 (1999), at 219. Also take note of Flaherty *Protecting Privacy in Surveillance Societies* (1989)
[148] Province of Alberta, 2003, § 3.

The legislation defines personal information as "information about an identifiable individual."[149] The legislation applies to all organizations that have or use personal information in the province.[150]

In 2009, the Act was updated by amendment.[151] On 19 January 2010, the provisions went into effect. The amendments require that the Commissioner be notified when there is a privacy breach that causes a significant harm. No penalties are required for failure to comply. The individual does not always have to be notified. When information is transferred to a service provider outside of CA, the individual must be notified. Record destruction and retention standards applied to personal data are refined by the Act. The amendment protects whistleblower employees and requires employee consent for the collection, use, and/or disclosure of employee personal data. The Federal government has not enacted any breach notification standards.

Research conducted by the Office of the Privacy Commissioner of Canada found that more businesses are collecting personal information. Of the businesses surveyed, sixty-eight percent reported personal data, which is an increase of five percent in the 2007 study. Forty-two percent of the businesses reported that they have no security breach concerns.[152]

---

[149] *Id.* at ¶ 2. This includes a person's name, address, telephone number, gender, ID numbers, income, blood type, credit records, loan records, and other information. It also includes sensitive personal information such as a person's health or medical history, racial or ethnic origin, political opinions, religious beliefs, trade union membership, and financial information.

[150] *Ibid*.

[151] Government of Alberta, *Personal Information Protection Amendment Act, 2009*. (2009), at http://www.qp.alberta.ca/546.cfm?page=CH50_09.CFM&leg_type=fall (last visited on 8 July 2012). See also Province of Alberta, *PIPA Compared*. (2010), at http://servicealberta.ca/pipa/documents/PIPAcompared.pdf (last visited on 19 March 2012).

[152] Office of the Privacy Commissioner of Canada, *Poll: Canadian Businesses Unconcerned About Privacy Breach Risk*. (2010), at http://www.priv.gc.ca/media/nr-c/2010/nr-c_100527_e.cfm (last visited on 27 May 2012).

5.6.2 British Columbia Personal Information Privacy Act

The Office of the Information and Privacy Commissioner in British Columbia is independent from the government and has governmental powers. The office is an independent federal agency. Under the British Columbia Personal Information Protection Act, personal information is defined as "information about an identifiable individual … (and) includes sensitive personal information."[153] The Act does not provide special attention for non-profit organizations or professional regulatory organizations.

Section Two of the Act defines the purpose of the legislation, which is to govern organizations that collect, disclose, and use personal information. This section also uses a reasonable personal standard of care to determine appropriateness.[154]

The law in British Columbia establishes that individuals own their own information and have a right to information privacy. Individuals do not have total control over the information, but they are major stakeholders. The Privacy Commission has the power to make binding orders, which can be reviewed by the provincial Supreme Court.

5.6.3 New Brunswick Protection of Personal Information Act

The province established DPSIP enabling legislation in the passage of the *Protection of Personal Information Act*[155]. The Act is administered by the provincial Ombudsman,[156] and is similar to the Federal legislation.

---

[153] Provence of British Columbia, 2004, ¶, 2.
[154] *Ibid.*
[155] Province of New Brunswick, *Protection of Personal Information Act*. (1998), at http://www.gnb.ca/acts/acts/p-19-1.htm (last visited on 25 September 2012).
[156] *Id.*

5.6.4 Quebec Privacy Protections

The Civil Code of Quebec identified key DPSIP legal issues. "Every person has the right to the respect of his reputation and privacy. No one may invade the privacy of a person without the consent of the person or his heirs unless authorized by law."[157]

Quebec passed the 2000 *Personal Information Protection and Electronic Documents Act*.[158] The purpose of the act was to protect personal information to promote and support electronic commerce.[159]

Section Two defines personal information as "information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization."[160] The aim of the act was to protect an individual's right to privacy and organizations in the information industry.[161] The act applies to every organization that involves personal information.[162]

In 2010, the Province of Quebec established the *Act Respecting the Protection of Personal Information in the Private Sector.*[163] The function of the Act was to make Provincial standards conform to the Federal standards.

The Quebec *Charter of Human Rights and Freedoms*[164] established privacy of personal data as a priority. The preamble declared, amongst other statements the following:

---

[157] Civil Code of Quebec amend. 1991, c. 64, a. 35; 2002, c. 19, s. 2. (1991).
[158] Province of Quebec, 2000. ¶ 1.
[159] *Id.*
[160] *Id.* at § 2.
[161] *Id.* at § 3.
[162] *Id.* at § 4.
[163] Province of Quebec, *An Act Respecting the Protection of Personal Information in the Private Sector, R.S.Q. c. P-39.1*. (2010), at http://www.canlii.org/en/qc/laws/stat/rsq-c-p-39.1/latest/rsq-c-p-39.1.html (last visited on 26 July 2012). (CA)
[164] *Ibid.*

> [E]very human being possesses intrinsic rights and freedoms designed to ensure his protection and development; all human beings are equal in worth and dignity, and are entitled to equal protection of the law; … [and] the rights and freedoms of the human person are inseparable from the rights and freedoms of others and from the common well-being.[165]

The chapter on fundamental freedoms and rights, paragraph five, declared that "Every person has a right to respect for his private life." Section Six declared that "Every person has a right to the peaceful enjoyment and free disposition of his property, except to the extent provided by law." Section Eight stated that "No one may enter upon the property of another or take anything therefrom without his express or implied consent." Section Nine set the standards that "Every person has a right to non-disclosure of confidential information."[166]

5.6.5 Sectoral Legislation

CA provinces have passed some sectoral legal approaches related to information. Two significant areas include freedom of information acts, with some privacy protections and health privacy acts. The approach is in sharp contrast to the US sectoral approach to all DPSIP legal issues.

5.6.5.1 Provincial Freedom of Information Acts

The provinces have passed model freedom of information acts that addressed some privacy concerns. These acts apply only to governmental agencies; the major focus is on freedom of information requests on records held by governmental agencies. The acts do not address key DPSIP legal issues, and their administration is not consistent. The acts define personal

---

[165] Province of Quebec, *Charter of Human Rights and Freedoms*. (2006), at http://www.cdpdj.qc.ca/en/commun/docs/charter.pdf (last visited on 23 July 2012), at 2. (CA)

[166] *Ibid.*

information and personal health information held by governmental agencies and contractors. The function of the freedom of information acts is to allow persons to request information and allow the government justifications for not complying. Individuals do have a right to request correction of data held.

The Alberta *Freedom of Information and Protection of Privacy Act*[167] is administered by the Information and Privacy Commissioner.[168] The British Columbia *Freedom of Information and Protection of Privacy Act*[169] is also administered by the provincial Information and Privacy Commissioner.[170] The government wants to change the Act so that it can collect and share more personal data, without consent, and store it outside of Canada.[171] The Manitoba *Freedom of Information and Protection of Privacy Act*[172] is administered by the provincial Ombudsman.[173] The New Brunswick *Right*[174] *to Information Act* is administered through the various governmental Ministers.[175]

In 2002, the Newfoundland *Freedom of Information Act*[176] was replaced by the *Access to Information and Protection of Privacy Act*.[177] The Act is administered by the Department of Justice[178] rather than an independent agency. The Northwest Territories *Access to Information and Protection of*

---

[167] Province of Alberta, *Freedom of Information and Protection of Privacy Act*. (2006), at http://foip.gov.ab.ca/ (last visited on 24 September 2012). (CA)

[168] *Id.*

[169] Province of British Columbia, *Freedom of Information and Protection of Privacy Act*. (1996), at http://www.qp.gov.bc.ca/statreg/stat/F/96165_00.htm (last visited on 24 September 2012). (CA)

[170] *Id.*

[171] Andrew Macleod, *Sweeping New Powers Would Threaten Privacy: Watchdog*, The Tyee. (2010), at http://thetyee.ca/News/2010/03/25/NewPowers/ (last visited on 25 March 2012).

[172] Province of Manitoba, *Freedom of Information and Protection of Privacy Act*. (1998), at http://web2.gov.mb.ca/laws/statutes/ccsm/f175e.php (last visited on 20 September 2012). (CA)

[173] *Id.*

[174] New Brunswick, *Right to Information Act Chapter R-10.3*. (1978), at http://www.gnb.ca/0062/PDF-acts/r-10-3.pdf (last visited on 8 July 2012). (CA)

[175] *Id.*

[176] Province of Newfoundland, *Access to Information and Protection of Privacy Act*. (2002), at http://www.hoa.gov.nl.ca/hoa/chapters/2002/A01-1.c02.htm (last visited on 25 September 2012). (CA)

[177] *Id.*

[178] *Id.*

Privacy Act[179] is administered by the Information and Privacy Commissioner.[180] The Nova Scotia *Freedom of Information and Protection of Privacy Act*[181] is administered by the Freedom of Information and Privacy Review Officer.[182]

Ontario has enacted a *Freedom of Information and Protection of Privacy Act*[183] that is administered by the Information and Privacy Commissioner.[184] The province also enacted the *Municipal Freedom of Information and Protection of Privacy Act*, [185] which is also administered by the Information and Privacy Commissioner.[186]

The Prince Edward Island *Freedom of Information and Protection of Privacy Act*[187] is administered by the Information and Privacy Commissioner.[188] Quebec enacted the *Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information Act*,[189] which is administered by the Commission d'accès à l'information.[190]

---

[179] Government of The Northwest Territories, *Access to Information Protection of Privacy Act*. (1996), at http://www.justice.gov.nt.ca/pdf/ACTS/Access_to_Information.pdf (last visited on 24 September 2012).

[180] *Id.*

[181] Province of Nova Scotia, *Freedom of Information and Protection of Privacy Act*. (1993), at http://www.gov.ns.ca/legislature/legc/statutes/freedom.htm (last visited on 22 September 2012). (CA)

[182] *Id.*

[183] Province of Ontario, *Freedom of Information and Protection of Privacy Act*. (1990a), at http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_90f31_e.htm (last visited on 21 September 2012). (CA)

[184] *Id.*

[185] Province of Ontario, *Municipal Freedom of Information and Protection of Privacy Act*. (1990b), at http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_90m56_e.htm (last visited on 21 September 2012). (CA)

[186] *Id.*

[187] Province of Prince Edward Island, *Freedom of Information and Protection of Privacy Act*. (2006), at http://www.gov.pe.ca/law/statutes/pdf/f-15_01.pdf (last visited on 26 September 2012). (CA)

[188] *Id.*

[189] Province of Quebec, *An Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information*. (2007), at http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=//A_2_1/A2_1_A.htm (last visited on 19 September 2012). (CA)

[190] *Id.*

The Saskatchewan *Freedom of Information and Protection of Privacy Act*[191] and the *Local Authority Freedom of Information and Protection of Privacy Act*[192] are both administered by the Freedom of Information and Privacy Commissioner. The Yukon *Access to Information & Protection of Privacy Act*[193] is administered by the Ombudsman and Information and Privacy Commissioner.[194]

5.6.5.2 Provincial Health Privacy Acts

The Alberta *Health Information Act*[195] is administered by the Information and Privacy Commissioner.[196] This act seeks to protect personal health information while enabling the use of electronic health or medical records. Traditional DPSIP legal standards are applied. A personal right to access and correction is established. The Act requires an informed consent; moreover, the consent may be withdrawn in writing.

The Manitoba *Personal Health Information Act*[197] is administered by the Ombudsman.[198] The act provides a legal regulatory scheme for electronic health records and attempts to provide some limited DPSIP legal constraints. The Act provides for an expressed or implied consent. The person may place conditions on the consent and withdraw the consent by notifying the health trustee. The Act does allow name and address sharing with fundraising

---

[191] Province of Saskatchewan, *Freedom of Information and Protection of Privacy Act*. (2006a), at http://www.qp.gov.sk.ca/documents/English/Statutes/Statutes/F22-01.pdf (last visited on 23 September 2012). (CA)

[192] Province of Saskatchewan, *Local Authority Freedom of Information and Protection of Privacy Act*. (2006b), at http://www.qp.gov.sk.ca/documents/English/Statutes/Statutes/L27-1.pdf (last visited on 23 September 2012). (CA)

[193] Government of Yukon, *Access to Information and Protection of Privacy Act*. (2002), at http://www.gov.yk.ca/legislation/acts/atipp.pdf (last visited on 19 September 2012). (CA)

[194] *Id.*

[195] Province of Alberta, *Health Information Act*. (2000), at http://www.qp.gov.ab.ca/Documents/acts/H05.CFM (last visited on 22 September 2012). (CA)

[196] *Id.*

[197] Province of Manitoba, *Personal Health Information Act*. (1997), at http://web2.gov.mb.ca/laws/statutes/ccsm/p033-5e.php (last visited on 21 September 2012). (CA)

[198] *Id.*

bodies. The province waited until 1 May 2008 (eleven years) to hire its first privacy chief.

Newfoundland and Labrador is the latest province to pass health privacy laws in the form of the *Personal Health Information Act.*[199] This act was passed in 2008 with a 2010 effective date. The Act allows for readiness audits. The purpose of this act is similar to other provincial health privacy acts. Under the law, informed consent is required for the collection, disclosure, and use of personal health data. The consent may be expressed or implied. The consent may also be withdrawn. Violation complaints may be filed with the Commissioner, who can seek informal resolution, investigate, review, and make recommendations. Appeals can be made to the courts.

After years of work, the Ontario government passed the *Personal Health Information Protection Act of 2004*[200] to protect personal health data.[201] The Act establishes rules for collection, disclosure, and use; provides a right to access and correction; reviews, and legal remedies. The Act requires a form of informed consent, but the consent may be expressed or implied. Expressed consent is required if the data is given to a non-healthcare custodian. A person may withdraw an expressed or implied consent by filing a notice with the custodian. The Act addresses the issue of capacity to consent and allows for substitute decision makers.[202] Violation complaints are filed with the Information and Privacy Commissioner. The Commission can inspect, review, and request a mediation process. Appeals can be made to the Courts, which can impose financial fines for violations.

---

[199] St. John's Newfoundland and Labrador, *Personal Health Information Act. SNL2008. c. P-7.01*. (2010), at http://www.assembly.nl.ca/legislation/sr/statutes/p07-01.htm (last visited on 17 July 2012). (CA)

[200] Service Ontario, *Personal Health Information Protection Act, 2004. S.O. 2004, c. 3.* (2010), at http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_04p03_e.htm (last visited on 17 July 2012). (CA)

[201] *Id.*

[202] *Id.* at 22, 23, 24, 26.

The Saskatchewan *Health Information Protection Act*[203] is administered by the Freedom of Information and Privacy Commissioner.[204] The Act attempts to protect personal information while enabling the use of electronic health or medical data bases. This act requires an informed expressed or implied consent with a revocation right. Amendments to the act allow hospitals to release patient information for fundraising purposes without the patient's consent. Business interests trump privacy rights under the change.[205] Under this Saskatchewan statute, it is impossible to terminate an employee's employment for violating a patient's privacy.[206]

The CA provincial acts set some informed consent requirements; however, the acts provide a number of exceptions and no clear definitions. Consent is not required for all personal health collections, disclosures, or uses. The acts define what a record means as well as establish accuracy standards, safeguards, openness, and individual access. If a case reaches the courts, fines range from 50,000 CA dollars up to 500,000 CA dollars depending on the province and if the offending party is a natural person or a corporation.

A significant failure of all these provincial Health Privacy Acts is that there is no clear, consistent, or understandable legal standard that establishes requirements for identifiable and non-identifiable health information. The distinction may, in fact, be irrelevant considering data mining and sharing programs. These acts ignore proclaimed aggregated, anonymized, and de-identified data; they do not require minimum training requirements for employees; they do require disposal and retention requirements, but they do not establish a clear standard.

---

[203] Province of Saskatchewan, *Health Information Protection Act*. (2003), at http://www.health.gov.sk.ca/adx/aspx/adxGetMedia.aspx?DocID=272,94,88,Documents&MediaID=122&Filename=health-info-overview-update.pdf (last visited on 23 September 2012). (CA)

[204] *Id.*

[205] CBC News, *Sask. Patient Privacy Rule Changes Slammed*. (2010), at http://www.cbc.ca/canada/saskatchewan/story/2010/05/03/sask-privacy-dickson-heath-information.html (last visited on 3 May 2012)

[206] CBC News, *Sask. Needs Privacy Upgrade: Report*. (2010), at http://www.cbc.ca/canada/saskatchewan/story/2010/06/30/sk-dickson-privacy-upgrade.html?ref=rss (last visited on 30 June 2012).

5.7 Canadian Provincial Case Law

Some provincial courts have ruled on DPSIP cases related to provincial laws and conflicts. The provinces include Alberta, British Columbia, Northwest Territories, Nova Scotia, Ontario, Prince Edward Island, and Quebec. Those provinces that have privacy commissioners or other officials that have investigative powers often do note regulatory decisions.[207]

5.7.1 Alberta Case Law

In *Stubicar v Alberta (Information & Privacy Commissioner*),[208] the Alberta Court of Appeals found that the courts should defer to privacy commissions' determinations, especially when there are mixed fact and legal issues. The court further found that a reasonable expectation of privacy standard is appropriate.[209] Later, the Alberta Court of Queen's Bench ruled in *Lycka v Alberta (Information & Privacy Commissioner).*[210] The case established that when procedural fairness is an issue, a standard of correct expectation can be appropriate.[211] The Court further found that the term *person* incorporates the term *custodian* in the text of the law.[212] Thus a custodian is a person under the law.

---

[207] **Alberta:** Office of the Information and Privacy Commissioner, Orders and Reports - http://www.oipc.ab.ca/pages/OIP/description.aspx; **British Columbia:** Office of the Information & Privacy Commissioner, Orders, Investigations, and Decisions - http://www.oipc.bc.ca/index.php?option=com_content&view=article&id=81&Itemid=8; **Manitoba:** Ombudsman Manitoba, Selected Case Studies - http://www.ombudsman.mb.ca/casesummaries.htm; **Newfoundland and Labrador:** Office of the Information and Privacy Commissioner, Investigative Results & Analysis - http://www.oipc.nl.ca/investigation.htm; **Ontario:** Information and Privacy Commissioner, Decisions and Resolutions - http://www.ipc.on.ca/english/decisions-and-resolutions/; **Prince Edward Island:** Office of the Information and Privacy Commissioner Orders, Orders - http://www.assembly.pe.ca/index.php3?number=1021416; **Quebec:** Commission of Access and Information, CAI decisions - http://www.cai.gouv.qc.ca/index-en.html (last visited on 25 July 2012).

[208] *Stubicar v Alberta (Information & Privacy Commissioner*, 2008 CarswellAlta 1625, 2008 ABCA 357 (Alta. C. A.) (CA - Alberta).

[209] *Id.*

[210] *Lycka v Alberta (Information & Privacy Commissioner)*, 2009 CarswellAlta 588, 2009 ABQB 245 (Alta. Q. B.) ¶¶ 21-27. (CA - Alberta).

[211] *Id.*

[212] *Id.* at ¶ 95.

5.7.2 British Columbia Case Law

The British Columbia Government and Services Employees' Union sued the Minister of Health Services for British Columbia.[213] The issue related to the release of medical billing and related medical data being a violation of Sections Seven and Eight of the *Canadian Charter of Rights and Freedoms*. The data was government collected records processed by a private company. The Court found a reasonable privacy expectation and that Sections seven and eight of the charter protect the information.

The provincial privacy commissioner challenged Royal Canadian Mounted Police practices in the courts. The Supreme Court of British Columbia ruled that the commissioner does not have the power to sue in any capacity. The Privacy Commissioner can only appear in court to present evidence of a review of a decision or apply exemptions.[214]

In *Hung v Gardiner*,[215] the plaintiff was an attorney and certified public accountant. The government investigated the plaintiff's supervisor and the processing of data regarding the plaintiff. After the investigation regarding the supervisor was concluded, the agency submitted the plaintiff's information to accounting and legal organizations. The plaintiff argued that the release was a violation of privacy law. The Court found for the plaintiff and concluded that once the supervisor's investigation was concluded, the release violated the original purpose of the collection.

---

[213] *B.C.G.E.U. v. British Columbia (Minister of Health Services)*, 2005 CarswellBC 672, 2005 BCSC 446, 27 Admin. L.R. (4th) 125, 129 C.R.R. (2d) 301, (25 March 2005) (CA-BCSC).

[214] *Canada (Privacy Commissioner) v. Canada (Attorney General) (2003)*, [2003] B.C.J. No. 1344, 14 B.C.L.R. (4th) 359, [2003] 9 W.W.R. 242, 2003 BCSC 862, 2003 CarswellBC 1394 (B.C. S.C.), (5 June 2003). (CA)

[215] *Hung v. Gardiner (2002)*, 2002 CarswellBC 1953, 2002 BCSC 1234, [2002] B.C.J. No. 1918, 45 Admin. L.R. (3d) 243 (B.C. S.C.); additional reasons at Hung v. Gardiner (2003), 2003 CarswellBC 509, 2003 BCSC 285, [2003] B.C.J. No. 499 (B.C. S.C.); affirmed Hung v. Gardiner (2003), [2003] B.C.J. No. 1048, 13 B.C.L.R. (4th) 298, 32 C.P.C. (5th) 1, 302 W.A.C. 4, 184 B.C.A.C. 4, 1 Admin. L.R. (4th) 152, 227 D.L.R. (4th) 282, 2003 CarswellBC 1060, 2003 BCCA 257 (B.C. C.A.), (21 August 2002). (CA)

5.7.3 Northwest Territories Case Law

The Northwest Territories Supreme Court addressed the issue of access to personal information. The Court found that the information must be personal, as defined by the statute. The question was raised whether there was a presumption that release would be unreasonable. The court held that there was such a presumption and that this presumption can be rebutted only by a strict application of the statute. All relevant circumstance must be addressed.[216]

5.7.4 Nova Scotia Case Law

The Supreme Court of Nova Scotia established the standard for determining if personal information could be released. The judicial task includes assessing if the personal information met the criteria as determined by the Act. The next task is to determine if the release of the data would be an unreasonable invasion of personal privacy. The final judicial task is to balance all relevant circumstances related to the decision to disclose or not.[217]

The Nova Scotia Privacy Coordinator refused to release information to Lee Keating, a former employee of Shelburne School for Boys (a provincial reformatory institution), related to charges made against him in a case that was resolved in an alternative dispute resolution process. In *Keating v. Nova Scotia (Attorney General),*[218] the provincial Supreme Court ruled that Keating had the right to know the information and should have an opportunity to correct the record. The Court ruled that the release of the data was not an unreasonable invasion of privacy. The Court followed the standard set in

---

[216] *Canadian Broadcasting Corp. v Northwest Territories (Minister of Finance)*, 2006 CarswellNWT 41, 2006 NWTSC 33 (N.W.T. S.C.). (6 July 2006). (CA)

[217] *Dickie v. Nova Scotia (Department of Health) (1999), (sub nom. Dickie v. Nova Scotia (Minister of Health))*, 538 A.P.R. 333, 176 N.S.R. (2d) 333, 173 D.L.R. (4th) 656, [1999] N.S.J. No. 116, 1999 CarswellNS 97 (N.S. C.A.), (4 February 1999). (CA)

[218] *Keating v. Nova Scotia (Attorney General) (2001)*, 2001 CarswellNS 206, 2001 NSSC 85, [2001] N.S.J. No. 227, 606 A.P.R. 290, 194 N.S.R. (2d) 290, 42 Admin. L.R. (3d) 66 (N.S. S.C.); additional reasons at Keating v. Nova Scotia (Attorney General) (2001), 621 A.P.R. 110, 198 N.S.R. (2d) 110, 2001 CarswellNS 371, 2001 NSSC 150 (N.S. S.C.), (13 June 2001). (CA)

Dickie.[219]

5.7.5 Ontario Case Law

In *Somwar v. McDonald's Restaurants of Canada Ltd*.,[220] the Ontario Superior Court of Justice found for the plaintiff. Somar worked as a manager for McDonald's restaurant. The employer ran a credit check on him without his permission. The court found McDonald's behavior unlawful under credit reporting statutes and that it was also considered a violation of Somwar's privacy rights.[221]

The Ontario Superior Court of Justice also decided two cases related to police officers requesting personal information when the person is not facing criminal charges. In *R. v Harris*,[222] a passenger in a vehicle stopped for a traffic violation was asked for a name, address, and date of birth. In *R. v E. (M)*,[223] a youth fell asleep at a computer at an Internet Café. The police demanded the youth provide name, address, date of birth, and any outstanding criminal charges. In both cases, the Court found that there was an expectation of privacy and a right to control the information. Having such information can open databases that can be mined for additional intimate data.

Sandra Jones was a customer of a bank for which she also worked. Winnie Tsige was a co-worker at the bank; however, they did not know one another. Tsige had established a relationship with Jones' ex-husband. As a bank employee, Tsige accessed Jones' banking records at least 174 times over

---

[219] *Dickie v. Nova Scotia (Department of Health) (1999), (sub nom. Dickie v. Nova Scotia (Minister of Health))*, 538 A.P.R. 333, 176 N.S.R. (2d) 333, 173 D.L.R. (4th) 656, [1999] N.S.J. No. 116, 1999 CarswellNS 97 (N.S. C.A.), (4 February 1999) (CA).

[220] *Somwar v. McDonald's Restaurants of Canada Ltd.* (2006), 79 O.R. (3d) 172 • (2006), 263 D.L.R. (4th) 752, (2006). (CA)

[221] *Id.*

[222] *R. v. Harris (2006)*, [2006] O.J. No. 1321, 2006 CarswellOnt 2015, 2006 ONCJ 106 (Ont. C.J.); reversed R. v. Harris (2007), 87 O.R. (3d) 214, [2007] O.J. No. 3185, 49 C.R. (6th) 220, 51 M.V.R. (5th) 172, 2007 CarswellOnt 5279, 2007 ONCA 574, 163 C.R.R. (2d) 176, 225 C.C.C. (3d) 193, 228 O.A.C. 241 (Ont. C.A.), (24 August 2007) (CA).

[223] *R. v. E. (M.) (2006)*, 2006 CarswellOnt 2482, 2006 ONCJ 146, [2006] O.J. No. 1657 (Ont. C.J.), (8 March 2006). (CA)

four years. When her actions were confronted, Tsige confessed, apologized, and was disciplined by the bank. Jones sought judicial relief.

In *Jones v. Tsige*[224] the Ontario Court of Appeals recognized an "intrusion upon seclusion" or invasion of privacy cause of action. The court found that modern information technology poses a real threat to the right of privacy that is critical to the political and social order. In an action under an "intrusion upon seclusion," the plaintiff must establish three factors. There was an invasion of the plaintiff's private affairs or concerns without lawful justification. The invasion was deliberate, intentional, reckless, or significant. A reasonable person would consider the invasion as highly offensive. The plaintiff does not have to establish economic damages. Damages may be symbolic based on infringement or to vindicate rights. If established, the defendant would be liable for the crime and pay up to $20,000 CA dollars plus the costs of aggravating damages. A defendant's defense may be a claim of freedom of expression or of the press.

5.7.6 Prince Edward Island Case Law

The Supreme Court upheld the Privacy Commissioner's right to refuse the release of names and salaries of employees of a governmental board. The Court established an analysis standard for determining when data can be released.[225] The standard is the same as that determined in the *Dickie v. Nova Scotia* case. The Prince Edward Island Supreme Court found that employment history is personal information.

5.7.7 Quebec Case Law

For years, the Canadian courts followed the American view that a person does not have an expectation of privacy in public places. Both legal systems

---

[224] *Jones v. Tsige*, 2012 ONCA 32, (18 January 2012). (CA)

[225] *MacNeill v. Prince Edward Island (Information & Privacy Commissioner) (2004)*, 22 Admin. L.R. (4th) 144, 2004 PESCTD 69, 2004 CarswellPEI 88, [2004] P.E.I.J. No. 86, 719 A.P.R. 231, 242 Nfld. & P.E.I.R. 231 (P.E.I. T.D.), (23 November 2004). (CA)

have modified this simplistic view. In *Aubry v. Editions Vice-Versa Inc*.,[226] the Quebec court found a privacy cause of action for a seventeen year-old girl sitting on a building door step when a photographer took her picture without her consent. When the photographs were published, the girl sued for privacy violation. The court agreed in a unanimous decision. The photographer had violated her privacy by not obtaining her consent and had in fact, appropriated her image. The court determined that the girl had a reasonable expectation of privacy in the street.[227]

The informed consent or informed choice principle developed through the British Common Law tradition. The Canadian courts accept the reasonable person standard that requires an adequate disclosure of the process, risks, and whether the lack of disclosure could cause damage.[228]

5.8 Canadian Standards and Remedies

Starting in the early 1990s, CA began to address Internet-based personal information privacy issues. In 1996, Industry Canada published a number of DPSIP options that covered a wide range of options.

CA can consider following the Netherlands model that sets norms of acceptable behavior and compliance but with no administrative, legislative, or oversight supervision. CA can follow the Registration and Licensing System that requires users to report activities in a public registry and meet DPSIP legal standards. CA can follow the Privacy Data Commissioner Model that establishes a single person or commission to use persuasion to meet standards.[229] CA chose to follow the data commissioner model after reviewing the other options.

---

[226] *Aubry v. Editions Vice-Versa Inc*, 1 S.C.R. 591, (1998), 591. (CA)
[227] *Id.*
[228] *Nichols v. Young O.J.* No. 4367, per McMurtry C.J.O., Weiler and Sharpe D.A. (Ontario Court of Appeal) (2003). (CA)
[229] Industry Canada, *Privacy and the Information Highway Regulatory Options for Canada* (Author. 1996).

A number of regulatory issues must be considered. The privacy law can add powers to existing offices to cover new privacy related sectors. Cyber regulations can focus on the computer and computer systems rather than the persons using the system. The law can extend the power of the Privacy Commission of Canada to regulate the private sector. The law can coerce the private sector to meet public sector standards. The law can establish DPSIP standards and make violations an offense. The law can also address specific industry regulation that would address large and politically specific sectors.[230]

The counter position is for the law to embrace voluntarism. In such a case DPSIP issues would involve no governmental regulation. The government could establish an assistance standard that would allow for compliance. In this case rule-making would be shifted to the private sector. The final option would accept private sector rules with the government having ultimate coercive powers.[231]

The DPSIP standard in CA is the PIPEDA, which was enacted in response to the EU data protection directive. The provinces have adopted similar standards and laws. A federal privacy commissioner and several provincial commissioners work together on consultation, educational, enforcement, inquiry, and policy recommendation projects. Business organizations are encouraged to appoint chief privacy officers and abide by legal standards. Governmental agencies are required to perform a privacy impact assessment on new programs that assess privacy impacts on proposals and programs, including delivery methods. The approach may be used on current programs and systems; however, the assessment is required if the program is re-designed. The standard has not been applied to business organizations including those business organizations that turn to the government for protections when wanted or needed.

---

[230] *Ibid.*
[231] *Ibid.*

The current CA approach includes a focus on privacy enhancing technologies. A recent study by London Economics[232] reveals some key relevant data. The subjects of the study included business associations, consumer advocacy groups, and data protection authorities. All of the subjects found that the risks to privacy are serious and growing with new electronic personal data processing. Consumers generally rate the risk as low but this is partly due to consumer ignorance. However, the political–policy debate continues. DPSIP authorities are confronted with the argument that DPSIP regulation should stop because costs are an impediment. Businesses argue that there is no political imperative or encouragement and that the government is to blame for the most notorious cases of loss of data. Businesses further argue that since consumers refuse to pay a business tax for data protection, businesses should be allowed to do whatever they want.

CA privacy law provides for statutory remedies that are subject to court review. As noted previously, the system of imposing fines for violations has not been very effective. The issuing of fines has been rare and the costs have been low. The courts can order correction of violating practices, publish notices, and award damages.[233]

5.9 Canadian Implementation System

The CA implementation system involves two alternative approaches. The first is the industry attempt to establish self-regulatory model codes to prevent the industry from being accountable to the government. The second approach involves governmental regulations for both the private and public sectors.

---

[232] London Economics, *Study on the Economic Benefits of Privacy Enhancing Technologies (PETs): Final Report to The European Commission DG Justice, Freedom and Security*. (2010), at http://ec.europa.eu/justice_home/fsj/privacy/docs/studies/final_report_pets_16_07_10_en.pdf (last visited on 30 July 2012).

[233] See PIPEDA Division 2, Section 16 a-c. (CA)

5.9.1 Self-Regulation Approaches

The Canadian Standards Association (CSA) is a business-oriented, not-for-profit membership organization. CSA established a voluntary model code for protecting personal information.[234] The code is based on the OECD guidelines and advocated that a flexible governmental legislative process be instituted that allows industry sectors to establish their own private codes based on the CSA model code.[235] The CSA model code established ten DPSIP principles: accountability; identifying purposes; consent; limiting collection; limiting use, disclosure, and retention; accuracy; safeguards; openness; individual access; and challenging compliance.[236]

Communications Canada established comprehensive telecommunication privacy policies. The policies recognized the fact that Canadians value their information privacy. The policies noted that people must know the privacy implications of using telecommunications. People should not have to pay extra for privacy protections. Expressed and informed consent should be required except when there is a clear public interest. A balance test should be applied to protect the right to be left alone. Privacy expectations may change and must be periodically reviewed.[237]

---

[234] Canadian Standards Association, *Model Code for the Protection of Personal Information*. (1996), at http://www.csa.ca/standards/privacy/code/Default.asp?language=English (last visited on 15 June 2012).

[235] Information Highway Advisory Council (IHAC), Connection, Community, and Content: the Challenge of the Information Highway (Minister of Supply and Services Canada. 1995), 141.

[236] Media Awareness Network, *Your Guide to the CSA's Privacy Code*. (2010), at http://www.media-awareness.ca/english/resources/educational/handouts/privacy/csa_privacy_code_guide.cfm (last visited on 5 July 2012).

[237] Communications Canada, *Telecommunications Privacy Principles* (Supply and Services Canada. 1992) 6-8.

5.9.2 Privacy Commissioner Approaches

The Canadian Privacy Commissioner[238] Office issues periodic reports on its activities, findings, and the related and laws. This office consults and investigates issues related to PIPEDA and the Privacy Act. The consultations include reviewing legislation for privacy issues and preparing legal opinions. Complaints are received, investigated, closed, settled, and litigated. The office also provides considerable public information services to Canadians and the world as well as an excellent online self-assessment tool to help organizations determine how well the organization is in compliance with DPSIP standards.[239] The office also provides mediation services in appropriate cases. The Canadian Privacy Commissioner Office and the Act itself are reviewed every five years to make sure that the system is current.

The following table reveals the major areas of complaints and resolutions during the 2007 through the 2009 fiscal years.[240] The information provides insight into the key issues faced and how the areas of concern have changed over the years.

Table 5.1 Complaints Received and Closed between January 1, 2007 and December 31, 2009

Type	2007 Complaint Percentage	2008 Complaint Percentage	2009 Complaint Percentage
Access	19%	17%	28%
Accountability	2%	2%	4%

[238] Canadian Privacy Commissioner, *Privacy by the Numbers in 2007*. (2007), at http://www.privcom.gc.ca/information/ar/200708/2007_pipeda_e.asp (last visited on 4 September 2012), § 8.

[239] Office of the Privacy Commissioner of Canada, *PIPEDA Self-Assessment Tool: Personal Information Protection and Electronic Documents Act*. (2008. August 8), at http://www.privcom.gc.ca/information/pub/ar-vr/pipeda_sa_tool_200807_e.asp (last visited on 10 August 2012).

[240] Canadian Privacy Commissioner, 2007, § 10 and Office of the Privacy Commissioner of Canada, *Annual Report to Parliament 2009: Report on the Personal Information Protection and Electronic Documents Act*. (2010), at http://www.priv.gc.ca/information/ar/200910/2009_pipeda_e.pdf (last visited on 8 July 2012).

Accuracy	2%	2%	4%
Challenging Compliance	n/a	<1%	0%
Collection	19%	22%	14%
Consent	5%	6%	10%
Correction/Notation	<.1%	1%	<1%
Fee	<.1%	<1%	0%
Openness	1%	<1%	2%
Retention	2%	0%	1%
Safeguards	10%	7%	10%
Time Limits	4%	3%	1%
Use and Disclosure	34%	38%	26%
Other	0%	<1%	0%
Total	350	422	231

Based on the available data, the top-tier concerns related to use and disclosure, collection, access, and safeguards. The second-tier concerns are related to consent, time limits, accountability, accuracy, and retention. Some concerns were expressed related to openness, correction and notation, fees, and retaliation. While each area of complaint is important to the parties involved, the data also provides information useful in assessing the scope of privacy commissioner practices. The total number of complaints is currently the lowest reported in this comparative data. The data suggests that the Canadian Privacy Commissioner is making some progress in educational and enforcement efforts.

To make sense of the data and the operations of the commission, the reports provide some key definitions. The Canadian Privacy Commissioner defines unusual terms such as “not well-founded”, “well-founded”, and “resolved” to report the findings of investigations.[241]

[241] Canadian Privacy Commissioner, 2007, Appendix 1. The definitions include Not well-founded. The investigation uncovered no or insufficient evidence to conclude that an organization violated the complainant’s rights under *PIPEDA*. Resolved. The investigation substantiated the allegations; however, prior to the conclusion of the investigation, the organization took or committed to take corrective action to remedy the situation, to the satisfaction of the OPC. Well-founded and resolved. At the conclusion of the investigation, the Commissioner believed that the allegations were likely supported by the evidence. Before a finding occurred, the Commissioner made a recommendation to the organization for corrective action to remedy the situation, which the organization took or committed to take. Well-founded. An organization failed to respect a provision of *PIPEDA.*

The Privacy Commissioner's Report declares that privacy law must be periodically updated based on changes in the environment, technology, and related challenges. The current major issues as reported are information technology changes including the increased amount of data being collected and stored, as well as web-based mapping technology including Google's Street View. The commoditization of personal information and identity management is another area of concern. The misuse of or false national security claims must be balanced against the individuals' right to privacy. The practice of the government deputizing private corporations and professionals to aid the government in violating privacy rights must be controlled. The increased use of genetic information collection and use must be addressed in terms of data protection and information privacy concerns.[242] As new technology and information business interests evolve, new privacy challenges are created and must be considered. Cloud computing, *Facebook*,[243] Internet retailers, *Linked In*, *My Space*, online dating services,[244] RFID, smart grids,[245]

---

[242] *Ibid.* See also Jennifer Stoddart, *Privacy Guardians Warn Multinationals to Respect Laws*, Office of the Privacy Commissioner of Canada. (2010), at http://priv.gc.ca/media/nr-c/2010/nr-c_100420_e.cfm (last visited on 20 April 2012). See also Diane Bartz, *Analysis: Google's Private Data Grab Means Big Legal Trouble*, Reuters. (2010), at http://www.reuters.com/article/idUSTRE6604YG20100701 (last visited on 1 July 2012).

[243] Kate Raynes–Goldie, *Aliases, Creeping, and Wall Cleaning: Understand Privacy in the Age of Facebook*, First Monday, 1-4, (2010). The research shows that users are concerned about their privacy but have a different definition. Misty Harris, *The New Social Suicide: Facebook Users Jump Ship Over Privacy Concerns*, Canwest News Service. (2010), at http://www.vancouversun.com/socialsuicideFacebookusersjumpshipoverprivacyconcerns/3024192/story.html (last visited on 9 July 2012) shows that millions are stopping the service. Jacquie Mcnish and Omar El Akkad, *Facebook Users Risk Blackmail, Privacy Czar Warns* Globe and Mail (2010), at http://www.theglobeandmail.com/news/technology/facebook-users-risk-blackmail-privacy-czar-warns/article1545444/ (last visited on 26 April 2012) for PCC's analysis. The PCC told the company that it was in violation of CA law. See also Erin Power, *Rethinking Privacy on the "Digital Street,"* Troy Media. (2009), at http://www.troymedia.com/?p=2185 (last visited on 13 July 2012).

[244] Meagan Fitzpatrick, *Privacy Watchdog Probes Dating Site*, Canwest News Service. (2010), at http://www.ottawacitizen.com/life/Privacy+watchdog+probes+dating+site/3223965/story.html (last visited on 1 July 2012).

[245] Information and Privacy Commissioner/Ontario, *Commissioner Cavoukian to Unveil Best Practices for Smart Grid Privacy Protection at Toronto Summit, June 16*. (2010), at http://www.ipc.on.ca/images/Resources/2010-06-14-Smart-Grid-Paper-Media-Advisory.pdf (last visited on 14 June 2012).

and social networking sites in general[246] and practices are all current concerns.[247]

The Ontario CA Privacy Commissioner was the leader in the country and the world in establishing sound DPSIP principles. The Commissioner was the first to establish a dialogue on requiring privacy by design (PbD).[248] The approach requires that technology developers and providers must provide technology that protects DPSIP standards within the design of all systems. The CA Commissioner was an early advocate to propose that there should be a legal right to be forgotten in the information age. Subjects' data should not exist forever in the power of DPSIP organizations. Data retention should be time limited.

Ann Cavoukian,[249] the Ontario CA Privacy Commissioner maintains that personal information is the oil of the Internet. She described how the Personal Data Ecosystem (PDE) will make personal information protections more than best practices, laws, and regulations. The aim is to change the relationship between individuals and organizations to protect information privacy concerns. Individuals must have control over how personal information is collected, disclosed, and used. Individuals must become the point of data integration. Individuals must have control over their own privacy

---

[246] Sarah Schmidt, *Canadians Wary of Online Privacy Promises*, National Post. (2010), at http://www.nationalpost.com/news/story.html?id=2482724 (last visited on 24 January 2012). Seventy-nine percent of the population does not trust such sites while six percent does trust these sites.

[247] Office of the Privacy Commissioner of Canada, *Annual Report to Parliament 2009: Report on the Personal Information Protection and Electronic Documents Act*. (2010), at http://www.priv.gc.ca/information/ar/200910/2009_pipeda_e.pdf (last visited on 8 July 2012).

[248] See Ann Cavoukian, *What is Privacy by Design?*, Information & Privacy Commissioner Ontario. (2010), at http://www.privacybydesign.ca/ (last visited on 6 July 2012); Ann Cavoukian, *Privacy by Design and the Emerging Personal Data Ecosyste*. (2012), at http://www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=1244 (last visited on 31 October 2012).

[249] Ann Cavoukian, *Privacy by Design and the Emerging Personal Data Ecosyste*. (2012), at http://www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=1244 (last visited on 31 October 2012).

settings. The approach involves the creation of a Personal Data Vault (PDV)[250] that the individual person controls.

5.10 Canadian Sociolegal Concerns

As early as 1992, Ekos[251] survey of 3,000 Canadians reveled that ninety-two percent expressed moderate to high levels of DPSIP concern. Financial, medical, and purchasing information was especially high. The study identified a list of major industries that had violated information privacy principles. The list included banks, cable companies, credit bureaus, doctors and hospitals (the lowest), employers, governments, insurance companies, police, retail stores, survey companies (the highest), and telephone companies

The Federation Nationale des Associations de Consommateurs du Quebec/Public Interest Advocacy Centre[252] surveyed 2,000 Canadians in Ontario and Quebec. Over fifty percent reported privacy violations of concern and high information privacy concerns. The research of Smith, Milberg, and Burke[253] showed that the major privacy concerns were improper access and unauthorized secondary use.

The work of Milberg, Burke, Smith, and Kaltman[254] compared culture as a variable in information privacy concerns. The study indicated that Thailand showed the lowest level of concerns and CA the highest in the study. The Canadians also showed the highest rank order of unauthorized secondary use, improper access, collection issues, and errors. Unauthorized secondary use was the highest in seven of the nine countries studied

---

[250] AKA as a Personal Data Locker, Personal Cloud, Personal Data Service. And Personal Data Store.

[251] Ekos Research Associates, *Privacy Revealed: The Canadian Privacy Survey* (Ekos Research Associates 1993).

[252] Federation Nationale Des Associations De Consommateurs Du Quebec/Public Interest Advocacy Centre, *Surveying Boundaries: Canadians and their Personal Information* (Author 1995).

[253] H. Jeff Smith, et al., Information Privacy: Measuring Individuals' Concerns About Organizational Practices, 20 *Management Information Systems* 2 167 (1996, June).

[254] Sandra. J. Milberg, et al., Values, Personal Information Privacy Concerns, and Regulatory Approaches, 38 *Communications ACM* 12, 65 (1995).

and the second highest in the other two. The samples' rank order was consistent. Irwin Altman reasoned that the legal regulation of privacy was universal and was documented in all societies.[255]

Paul Tolchinsky, Michael McCuddy, Jerome Adams, Daniel Ganster, and Howard Fromkin studied the importance of information and perceptions of privacy. Data analysis included rankings from high to low. The data measured the importance based on "(1) disclosure permission, (2) disclosure location, (3) disclosure consequences, and (4) type of information disclosed."[256] The Graham Smith study[257] quantified that informed consent on the collection and use of the data was a major information privacy standard and that the employee's perception of the data's sensitivity determined corporate privacy protection standards.

Another study of 7,088 adults, by Ipsos/Queen's University[258] found that sixty-nine percent of Canadians were concerned about the protection of personal information. The table below demonstrated that the business response to privacy concerns were very different in CA and the US.[259]

Table 5.2 Privacy Concerns

Issue	CA	US
"Good privacy practices" were tied to customer trust and brand loyalty	61%	17%
Had dedicated privacy officers, resources, and training programs.	82%	50%
Had privacy awareness for new employees	71%	43%
Company assigned a senior executive as their privacy officer	75%	50%
Customers' privacy preferences captured and	79%	53%

[255] Irwin Altman, Privacy: *A* Conceptual Analysis, 8 *Environment and Behavior*, 7 (1976), at 26.

[256] Paul D. Tolchinsky, et al., Employee Perceptions of Invasion of Privacy: A Field Experiment, 66 *Journal of Applied Psychology* 3, 308 (1981).

[257] L. Graham Smith, *Impact Assessment and Sustainable Resource Management* (Longman Scientific and Technical 1993).

[258] Ipsos / Queen's University, *Interviews with 7,088 Adults in Brazil, Canada, France, Hungary, Mexico, Spain and the United States* (2006), http://www.angus-reid.com/polls/view/13849 (last visited on 3 March 2012).

[259] Nikki Swartz, *U.S., Canadian Firms Have Different Views of Privacy* (2004, September 1), http://www.allbusiness.com/legal/221693-1.html (last visited on 17 March 2012).

followed		
Companies had a policy regarding surveillance and computer monitoring in the workplace	70%	13%

In 2009, the Canadian Office of the Privacy Commissioner conducted a public research project. The data showed that eighty-seven percent of Canadians distrusted businesses in the protection of their private information, especially during hard economic times. The Commissioner reported that some businesses were complying with data protection principles because they thought that it was a source of competitive advantage. Sixty-six percent of the sample did not know which institutions or resources were available for privacy concerns. A majority – sixty-two percent claimed that privacy was one of the most important issues for the next ten years. Seventy-one percent of the sample favored stronger privacy protection laws. The vast majority eighty-three percent - were concerned about genetic privacy.[260]

As noted previously, politicians and jurists can and certainly do argue and maneuver around DPSIP issues. Businesses and corporations can and do corrupt the process.[261] Notwithstanding the behavior of politicians, courts, and industry, the research cited above shows that the majority of CA citizens want strong DPSIP legislation and regulation.

[260] Office of the Privacy Commissioner Of Canada, *Canadians Concerned Corporate Cost Cutting Could Affect their Privacy: Poll* (2009, April 27), http://www.priv.gc.ca/information/survey/2009/ekos_2009_01_e.cfm (last visited on 28 April 2012).

[261] See: Jeffrey D. Clements, *Corporations Are Not People: Why They Have More Rights Than You and What You Can Do About it* (Berrett-Koehler Publishers, Inc ed. 2012). Thom Hartmann, *Unequal Protection: The Rise of Corporate Dominance and the Theft of Human Rights* (Rodale ed. 2002). Robert G. Kaiser, *So Damn Much Money: The Triumph of Lobbying and the Corrosion of American Government*,(Alfred A. Knopf ed. 2009). Lawrence Lessig, *Republic, Lost: How Money Corrupts Congress - and a Plan to Stop It* (Twelve - Hachette Hook Group ed. 2011).

5.11 Canadian Critique

The Canadian approach to DPSIP law is certainly superior to the system in AU, US, and SA; however, DPSIP law and system in CA does have some weaknesses.

The CA legal and regulatory system does not include Internet Service Providers (ISPs) as holders of information. The Canadian Internet Policy and Public Interest Clinic at the University of Ottawa has called upon the Federal Privacy Commissioner to address this issue. The use of behavioral targeting is widespread in the UK and the US, but the Canadian Internet Policy and Public Interest Clinic maintains that the practice violates Canadian standards. ISPs do not provide adequate informed consent, adequate notice, or means of personal control. The issue is also being raised in the US but with a self-regulation approach.[262] These issues are a critique of the legislation and regulatory scheme. The issues also show that the CA system provides for a means to share issues with those stakeholders that are responsible for privacy.

The power of the Privacy Commissioner's office is limited in terms of rule making. The Privacy Commission has attempted to persuade the Parliament to update the Canadian Privacy Act for some time. The Canadian Bar Association confirms that the Act is out of date and needs modernization. The Bar has recommended that the Act be changed to insure that "personal information of Canadians is collected only when demonstrably necessary and once collected is subject to stringent safeguards and accountability requirements, including a breach notification requirement; and not shared within or beyond Canada's borders unless those safeguards and requirements

---

[262] Terry Pedwell, *Academics Ask Privacy Watchdog to Probe Online Profiling Practices*, Canadian Press. (2008, July 28), at http://www.cbc.ca/cp/technology/080728/z072825A.html (last visited on 29 July 2012).

can be guaranteed."[263] The Canadian Bar Association wants the government to provide clear and articulated goals and breach notification standards. The Chief Privacy Officer and its department must be able to do more than advocate and act as an ombudsman. To guard personal information, the Privacy Office must be able to write and enforce regulations subject to judicial review.

The legal and regulatory system in CA has some major flaws. For example, the auditor general for Alberta reports that, "Because information security in the government is not consistently enforced, all information assets are exposed to unacceptable risk."[264] The department studied 400 computer systems but the review stopped after sixty-nine were evaluated and found faulty. Contrary to DPSIP legal standards in CA, the government is considering radio frequency identification (RFID) Enhanced Driver's Licenses (EDL).[265]

Business interests can subvert the law through manipulation. Insurance companies, in one documented case, increased rates up to thirty-two percent for subscribers refusing to release credit data. New Brunswick is the only province that has banned the practice in all insurance concerns. Alberta and Ontario have banned the practice for auto insurance.[266]

Willingness to comply with DPSIP laws and regulations is a key factor to establishing the effectiveness of such regulation. CA established a *do-not-call* program where people can reject unwanted marketing calls. More than seven

---

[263] Canadian Bar Association, *Comprehensive Revision of Privacy Act: Resolution 08-06a*. (2008, September 26), at http://www.cba.org/cba/resolutions/pdf/08-06-a-pdf.pdf (last visited on 26 September 2012), 2.

[264] Jim Macdonald, *Alberta Data Hacked: Health, Drivers 'Licence Records Not Well Protected: Top Auditor*. (2008, October 3), at http://www.edmontonsun.com/News/Alberta/2008/10/03/pf-6962041.html (last visited on 4 October 2012), ¶ 5.

[265] Antonella Artuso, *New ID Card Threatens our Privacy: Commissioner Raises Concerns*. (2008, October 21), at http://www.torontosun.com/news/canada/2008/10/21/7151421-sun.html (last visited on 22 October 2012).

[266] CBC News, *Credit Scores Can Hike Home Insurance Rates: Insurance Companies Say Credit Scores are a Good Indicator of Risk*. (2010), at http://www.cbc.ca/consumer/story/2010/04/08/consumer-insurance-credit-score.html (last visited on 6 July 2012).

million citizens have registered for the service. Over 300,000 complaints for violations have resulted in 73,000 CA dollar fines. The problem is that the Commission has only collected 250 CA dollars in fines. An additional set of problems occurs with the exemptions in the law. Charities, businesses that have a prior customer relationship, newspapers, and political parties need not comply. The data shows that the DPSIP law must be revamped and enforcement methods must be revised.[267]

In Jennifer Stoddart's report[268] to parliament, she noted some similar concerns related to the Financial Transactions and Reports Analysis Centre of Canada. Under Canadian law, banks, insurance firms and securities dealers, as well as others are to monitor and report certain financial transactions. The problem is that no checks or balances are tied to privacy standards. According to the report, the financial institutions are collecting and using information that they do not actually use, need, or have legal authority to collect. A sound DPSIP legal approach must extend to all in the government and private sector.

Even if sound DPSIP legislation is passed and regulatory bodies are established, the battle is not over. Partisan parliamentarians supported by contrary business supporters and information business special interest groups, can prevail. One standard approach is to refrain from funding the activities at a level needed to be effective.[269]

The Federal Privacy Commissioner of Canada is an ombudsman who can investigate complaints and advocate for privacy issues. The Privacy

---

[267] Canadian Press, *Do-Not-Call Fines Total $73,000; Only $250 Collected*, Metro News. (2010), at http://www.metronews.ca/toronto/local/article/572775--do-not-call-fines-total-73-000-only-250-collected--page0 (last visited on 8 July 2012).

[268] Office of the Privacy Commissioner of Canada, *Annual Report to Parliament 2009: Report on the Personal Information Protection and Electronic Documents Act*. (2010), at http://www.priv.gc.ca/information/ar/200910/2009_pipeda_e.pdf (last visited on 8 July 2012). For a brief news report, see Alexandre Deslongchamps, *Canada Banks, Agency, May Violate Clients' Privacy, Report Says* Bloomberg Press. (2009), at http://www.bloomberg.com/apps/news?pid=newsarchive&sid=aT_A.1ec0oKY (last visited on 17 November 2012).

[269] The Starphoenix, *Citizens Deserve Adequate Funding for Privacy Office*. (2010), at http://www.thestarphoenix.com/citizensdeserveadequatefundingprivacyoffice/2710730/story.html (last visited on 22 March 2012).

Commission can make recommendations but does not have the power to issue orders or efforts to stop a privacy-violating practice. Enforcement is dependent on the relevant party's cooperation or on seeking judicial intervention. Yet, in 2002, the EU determined that the Canadian law and DPSIP system provided an *adequate level of protection*.[270]

Once established, DPSIP law can be thwarted by opponents and political forces. Saskatchewan is a classic example. The number of reviews and complaints are up 113 percent in a year. Reviews are taking up to three years. When the commission asked for 129,000 CA dollars to help remedy the needs, the government refused. Therefore, services are being cut back.[271] For DPSIP laws to be effective, the courts, legislature, governmental officials, and businesses that are committed to corporate social responsibility must help build a culture of privacy.

Given that the CA system for the DPSIP legal approach has been determined by the EU Data Protection Working Party as EU "adequate" in terms of section 25 of the EU Directive and is more advanced that the AU, SA, and the US approaches, the lack of independence and enforcement powers takes its toll. For example, the Landlord's Source Centre, a Toronto company, collects data on potential renters for profit. The data base provides names, addresses, social insurance numbers, medical and mental health history, family member history, educational data, renting dispute information, criminal records, and credit information. The company sells access to the information while denying that the database exists. When confronted by the privacy commissioner, it took four years for the Centre to drop some services. The

---

[270] See Commission Decision (EC) 2002/2 of 20 December 2001 pursuant to Dir (EC) 95/46 of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act (2002) OJ L2/13.

[271] Jennifer Graham, *Saskatchewan Privacy Commissioner Cuts Services Citing Lack of Resources*, The Canadian Press. (2010), at http://www.chroniclejournal.com/includes/datafiles/CP_print.php?id=245484&title=Saskatchewanprivacycommissionercutsservicescitinglackofresources (last visited on 22 February 2012).

data practices were illegal; however, there were no legal remedies.[272] The federal law fails to provide order-making powers.

The CA courts tend to support business interest agreements, even without informed consent. The judicial response is often myopic. The reality is that seventy percent of companies will reveal personal information, including in non-emergency situations, to the RCMP without a warrant. There is no court oversight.[273]

CA has tried to reach a middle ground in DPSIP legal issues. Whereas the EU approach is more detailed and regulatory in nature, the US approach is market oriented in most situations and therefore supports self-regulation. CA on the other hand, has some regulatory powers and establishes privacy commissioners. The CA approach does provide market flexibility.[274] A major problem is that privacy legislation has not allowed responsive parties to deal with technological environmental changes. To deal with changes, regulatory bodies may be more responsive than parliamentarians.[275]

The CA approach has taken an international lead in addressing DPSIP issues. The privacy commissions have established an exceptional educational system through their own websites and publications.[276] Commissioners focus on showing that complying with privacy standards equals good business practices.[277]

---

[272] John Goddard, *Tenants' Private Data Available on Internet*, The Star. (2009), at http://www.thestar.com/article/596808 (last visited on 5 March 2012).

[273] Michael Geist, *Canadian Privacy Rights Buried in the Fine Print*. (2009), at http://www.thestar.com/article/602772 (last visited on 16 March 2012).

[274] Michael Geist, *Standing on Guard for Privacy - Before Facebook*. (2009), at http://www.thestar.com/article/695147 (last visited on 14 September 2012).

[275] David H. Flaherty, *Reflections on Reform of the Federal Privacy Act*. (2008), at http://www.priv.gc.ca/information/pub/pa_ref_df_e.cfm (last visited on 29 June 2012).

[276] Office of the Privacy Commissioner of Canada, *PIPEDA: Processing Personal Data Across Borders Guidelines*, Author. (2009), at http://www.priv.gc.ca/information/guide/2009/gl_dab_090127_e.pdf (last visited on 2 July 2012).

[277] Jennifer Stoddart, *Canada Celebrates Privacy Awareness Week by Helping Businesses Improve Privacy Practices* CNW Telbec. (2009), at http://www.newswire.ca/en/releases/archive/August2008/27/c7355.html (last visited on 31 December 2012). See also Office of the Privacy Commissioner of Canada, *PIPEDA Self-Assessment Tool: Personal Information Protection and Electronic*

The Commissioners are taking a lead in advocating for building-in technological standards as a means to protect DPSIP issues from becoming a problem[278] by requiring that new technology that may impact DPSIP legal issues should have built-in protection methods. Such technology producers must conduct a privacy impact assessment (PIA) prior to adoption of government protections and subsequent periodic audits.

CA was one of the first and is the most influential country in the world advocating the use of PIAs. The government requires some form of PIA process under national and provincial governmental DPSIP law. The laws, however, only apply to public agencies. The private sector is relieved of any PIA actions except as a voluntary good business practices standard and as a strategic business advantage. No independent DPSIP audits are required under CA law or self-regulation standards. To be effective, PIA and audit efforts must involve a serious analysis of the issues rather than merely completing a standard form. CA PIAs have become common, however, there are not always conducted adequately.[279]

For DPSIP efforts to be effective, the traditional reactive policy approach needs to also establish more proactive approaches.[280] Basic standards and

---

Documents Act. (2008. August 8), at http://www.privcom.gc.ca/information/pub/ar-vr/pipeda_sa_tool_200807_e.asp (last visited on 10 August 2012). See Government of Canada, *Privacy and Your Business* (2010), at http://www.canadabusiness.ca/eng/guide/2338/ (last visited on 19 July 2012).

[278] Ann Cavoukian, et al., *SmartPrivacy for the Smart Grid: Embedding Privacy into the Design of Electricity Conservation* (Information and Privacy Commissioner of Ontario and The Future of Privacy Forum. 2009). See also Information and Privacy Commissioner/Ontario, *The New Federated Privacy Impact Assessment (F-PIA): Building Privacy and Trust-enabled Federation*, Author. (2009), at http://www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=836 (last visited on 2 March 2012). Ann Cavoukian, *What is Privacy by Design?* Information & Privacy Commissioner Ontario. (2010), at http://www.privacybydesign.ca/ (last visited on 6 July 2012). Process examples include Anonymizers, Anonymous payment methods, Privacy icons, Privacy labels, and Pseudonymizers.

[279] Robin M. Bayley & Colin J. Bennett, Privacy Impact Assessments in Canada, in *Privacy Impact Assessment* (David Wright & Paul De Hert ed.^eds., Springer 2012).

[280] Jennifer Stoddart, *The Future of Privacy Regulation: Remarks at the 11th Annual Privacy and Security Conference*, Office of the Privacy Commissioner of Canada. (2010), at

privacy audits must be established.[281] Technology is constantly evolving; however, the legal issues do not change. Business innovation and its global implications need to be considered. Regulatory—not just legislative efforts—need to be able to address cultural and technological changes. Governments must reject Intellectual Property protections that have not addressed DPSIP concerns by sound privacy audit protections. DPSIP authorities must have strong independent investigatory, enforcement, and order-making powers. Traditional nation states and innovative DPSIP global approaches are needed. SA has the opportunity to take the lead in implementing such approaches.

5.12 Summary of Canadian Literature and Issues Reviewed

The intent of this thesis is to conduct a comparative analysis of DPSIP responses in five different nations. Part of the comparison uses a benchmark approach of key issues. The issues include legal support of DPSIP protections, legal support of corporate privacy and data protection standards, information privacy data protection and security declarations, the use of regulatory agencies, sectoral legislation, and data controllers. The benchmark standards also include data processor requirements, data subjects, data security destruction, cross-border data flow, exemptions and exceptions, and the current stage of the approach based on evolutionary stages. The following table presents the summary based on the benchmark model.

---

http://www.priv.gc.ca/speech/2010/sp-d_20100210_e.cfm (last visited on 11 February 2012).

[281] Ann Cavoukian & Tyler J. Hamilton, *The Privacy Payoff: How Successful Businesses Build Customer Trust* (McGraw-Hill Ryerson Ltd. 2002). See also Information and Privacy Commissioner/Ontario, *The New Federated Privacy Impact Assessment (F-PIA): Building Privacy and Trust-enabled Federation*, Author. (2009), at http://www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=836 (last visited on 2 March 2012). *"A privacy risk assessment should become an integral part of the design stage of any initiative. Once the risk to privacy is identified, then the necessary protections can be built in to minimize or ideally eliminate the risks." (p. 290).*

Table 5.3 Comparative Model of Canadian Legal Support of DPSIP Models

ISSUE DESCRIPTION	CA CURRENT RESPONSE
CM.1: Legal Support of DPSIP Protections	
Signatory, Adheres, and/or Complies with International Human Rights Standards	(See Appendix A.)
Signatory, Adheres, and/or Complies with EU DPSIP Standards	Yes
Signatory, Adheres, and/or Complies with APEC DPSIP Standards	Yes
Federal Constitutional Law	No
Federal Legislative Efforts	Yes
Federal Common Law	Mixed
Province /State Constitutional Law	No
Province / State Legislative Efforts	Varies
Province / State Common Law	Some

CM.2: Legal Support of Corporate Privacy and Data Property Protection Issues	**CA CURRENT RESPONSE**
Copyright Protections	Yes
Database Protection	Yes
Patient Protections	Yes
Service Mark Protections	Yes
Trade Mark Protections	Yes
Trade Secret Protections	Yes
Privacy Impact Audit Required Before Use	No
Privacy Impact Audit Required Before Government Protections Granted	No
Checks and Balances on Corporate Collection, Use, and Transfer of Individual DPSIP Data	Yes

CM.3: Information Privacy – Data Protection and Security Declarations	**CA CURRENT RESPONSE**
Definitions Provided	Yes
Personal and Sensitive Data Defined	Yes
Definitions Effectively Address	No

Advanced Data Mining Technologies	
All Holders and Users Held Accountable	No

CM.4: Regulatory Agency	**CA CURRENT RESPONSE**
Independent of Legislative and Executive Branches	No
Administrative Power	Yes
Investigative Power	Yes
Regulatory Powers	Some
Education Function	Yes
Enforcement Powers	Some
Structure	Yes
Responsibilities Defined	Yes
Accountability	Yes
Governmental Chief Privacy Officer/ Commissioner Required	Yes
Governmental Privacy Audits Required as Part of Legislation Passage	No
Business Chief Privacy Officer/ Commissioner Required	Suggested
Employees are Personally Liable for Violations	No
Business Privacy Audits Required	No
Agency Educational Function	Yes

CM.5: Sectoral DPSIP Legislation	**CA CURRENT RESPONSE**
Credit Reporting Agencies	Yes
Criminal Justice Record Restrictions	No
Health Information	Some
Health Information Exceptions	Some
Electronic Medical/Health Record Controls	Limited

CM.6: Data Controllers	**CA CURRENT RESPONSE**
Notice Required	In theory
Opt-In	Limited
Opt-Out	Generally
Must Be Lawful and Fair	Yes
System Access Controls	Yes
Data Quality and Integrity	Yes
Accurate	Yes
Complete	Yes
Up to Date	Yes
Limited to Needed Data	In theory

Relevant	In theory
Not Misleading	In theory
Data Retention Limitation	Not with current standards
Data Transfer Controls	Limited
Openness on Information Held	Limited
Breach Disclosures Required	Considering
Breach Penalties	No

CM.7: Data Processor Requirements	**CA CURRENT RESPONSE**
Informed Consent Required	Limited
Rationale Is Provided	Yes
Fair Processing	Yes
Legal Processing	Yes
General Data	Yes
Sensitive Data	Yes
Accuracy	Yes
Timely	Limited
Duration of Record-Keeping Controls	Limited

CM.8: Data Subjects	**CA CURRENT RESPONSE**
Ownership by the Subject	Limited
Control Over Access	No
Alter, Amend, Correct, and Delete Errors	Yes
Notification Requirement	Limited

CM.9: Data Security and Destruction	**CA CURRENT RESPONSE**
Security Must Be State of the Art	Generally
Technology Use – Cost of Implementation Not a Defense	Yes
Tracking	Not once merged
Safeguards Required	Adequate encryption
Protects From Alteration	Yes
Protects Against Disclosure	Yes
Protects Misuse	Yes
Protects Against Unauthorized Internal and External Access	Yes
Unauthorized Access Penalties	Based on cause of action
Timely Notice of Breaches	Limited
Strong Remedies Provided	Limited

CM.10: Cross-Border Data Flow	**CA CURRENT RESPONSE**
Individual Informed Consent Required	In theory
Transfer Source Is Accountable	Generally
Outsource Service Controls	Limited

CM.11: Exemptions and Exceptions	**CA CURRENT RESPONSE**
Only Permitted Where There Is a Compelling Justification	Yes
Checks and Balances – Court Order Required	Limited
Government Agencies	Yes
Intelligence and Defense	Yes
Police Actions	Yes
Small Business Exemption	Yes

CM.12 DPSIP Evolutional Stages	**CA CURRENT RESPONSE**
DPSIP.0 Limited DPSIP legal Issues	Yes
DPSIP.1.0 Establishes PII; does not fully address security issues; focus on limited legal consent and notice.	Yes
DPISP.2.0 Accepts PII standards; does not fully address security issues; focus on a legally based harm based analysis.	Yes
DPSIP.3.0 PII and non-PII data fused; privacy, data protection and security issues are interrelated; legal audits, checks, and balances needed for all personal information stakeholders. New technologies are required to pass privacy audits (example – RFID, Internet of Things) and require use of privacy enhancing technologies in all new IP approvals.	Exploring

Chapter Six addresses the actual approach and potential options in the SA approach to DPSIP legal issues. From a logical and alphabetical perspective, the next chapter should address SA concerns. SA must address a classic

strategic planning analysis. First, SA can conform to the historic model of catching up with the standards established of other countries and regions to conform. The secondary strategy is to meet and raise or *leap frog* the existing responses to the issues. SA can either catch up or take the lead. The author's analysis is that SA should take the lead. Recent actions suggest that SA will take the catch up approach.

CHAPTER SIX: DATA PROTECTION AND SECURITY LAW:

SOUTH AFRICAN LEGAL STANDARDS

> *There is a worldwide concern growing regarding the increasing potential threats to the personal privacy of individuals caused by technologies and governments. The international response of governments has been to draught comprehensive privacy legislation in order to protect their citizen's personal information and to enable their citizens to have control over their personal information. In South Africa, the right to privacy is protected by both Section 14 of the Constitution and the provisions of the Common Law.* Hano N. Olinger, Johannes J. Britz, & Martin M. Oliciwe[1]

6.0 Overview

At the time of this writing, SA is in the process of establishing DPSIP legislation and regulatory processes. The SA Constitution establishes a privacy right for natural persons that the other countries in the study have not clearly established. The Constitution also establishes constitutional protections for juristic persons,[2] which may have unintended consequences; such consequences are evidenced in the political power shift in AU, the UK, and certainly in the US.[3] The SA Constitution and case law clearly establish a right to identity and privacy. However, these traditional legal principles do not translate into adequate DPSIP principles.[4] Sufficient DPSIP legal protection

---

[1] Hano N. Olinger, et al., Western Privacy and/or Ubuntu? Some Critical Comments on the Influences in the Forthcoming Data Privacy Bill in South Africa, 39 *The International Information & Library Review* 1, 31 (2007), at 31.

[2] Companies and corporations

[3] See Chapters 2, 4, 7, and 8 of the current work.

[4] For a detailed analysis see J Neethling, et al., *Neethling's Law of Personality* (Butterworths 1st ed. 1996); J Neethling, et al., *Neethling's Law of Personality* (LexisNexis 2nd ed. 2005); and Anneliese Roos, *The Law of Data (Privacy) Protection: A Comparative and Theoretical Study* (2003) (LL.D. thesis, UNISA).

requires a legislative act, with all of the foibles such an approach seems to require. SA must establish state-of-the-art DPSIP legislation to protect its citizens from data- and security-related abuses and provide checks and balances on business and government activities. SA must join the DPSIP community of countries, especially its major trading partners.

Hanno Olinger, Johannes Britz, and Martin Olivier argue that the *Ubuntu* belief system opposes adopting a Western focus on individual privacy protection needs.[5] SA must make the principles consistent with its values and worldview. The country generally accepts the principle of *Ubuntu,* which requires consideration of the community rather than just an individual when making ethical decisions.[6] The underlying concept is that a person is defined in terms of others within a family or quality community. The value is based on caring, compassion, happiness, humanness, interdependence, respect, and universal brotherhood. However, none of these values directly conflict with the intention of DPSIP legislation and standards. The concepts of the dignity of the person and the community are certainly consistent with DPSIP legislation and standards. Sound DPSIP laws and regulations protect the individual as well as the community from abuses.

SA uses the term “data protection” to address information privacy concerns. Information privacy is defined as follows:

> [A]n individual condition of life characterized by seclusion from the public and publicity. This condition embraces all those personal facts which the person concerned has himself determined to be excluded

---

[5] Hanno N. Olinger, et al., *Western Privacy and Ubuntu - Influences in the Forthcoming Data Privacy Bill in* Ethics of New Information Technology - Proceedings of the Sixth International Conference of Computer Ethics: Philosophical Enquiry (CEPE2005), P Brey, F Grodzinsky and L Introna (eds.), Enschede, The Netherlands, 291-306, July 2005 (Philip Brey, et al. eds., 2005).

[6] Nkonko M. Kwamwangamalu, Ubuntu in South Africa: a Sociolinguistic Perspective to a Pan-African Concept 13 *Critical Arts Journal* 2, 24 (1999). See also Johann Broodryk, *Ubuntu: Life lessons from Africa* (Ubuntu School of Philosophy 2nd ed. 2002).

> from the knowledge of outsiders and in respect of which he has the will that they be kept private.[7]

This definition has been accepted in a number of SA court decisions.[8] The majority of SA legal scholars believe it is critical and urgent to enact data protection legislation.[9]

The SA chapter begins with presenting background on the country. The analysis continues with an examination of the SA Constitutional declarations. SA national legislation and case law is examined. The research then focuses on the background and provisions of the SA *Protection of Personal Information Bill*. SA standards, remedies, and implementation system are reviewed. SA sociolegal concerns are presented. A critique of the SA approach is then addressed. A summary of the SA literature and issues, using the thesis comparative model of the current legal support, is then reviewed and presented.

6.1 Background

SA is a constitutional parliamentary democratic republic.[10] The government includes the national government and nine provinces.[11] The executive branch consists of the President who is the Head of Government and Head of State.[12] The President serves a fixed term and is elected from Parliament. The executive also includes the Deputy President, as well as ministers who are

---

[7] J Neethling, et al., *Neethling's Law of Personality* at 32. (LexisNexis 2nd ed. 2005).
[8] *Id.* at fn 335.
[9] Ibid.
[10] South Africa Government, *South Africa Government Online*. (2010), at http://www.gov.za/ (last visited on 5 August 2012). Site contains reference data for this section.
[11] The provinces include Eastern Cape, Free State, Gauteng, KwaZulu-Natal, Limpopo, Mpumalanga, North West, Northern Cape, and Western Cape.
[12] South Africa Government, *Executive Authority*. (2010), at http://www.info.gov.za/aboutgovt/exec.htm (last visited on 5 August 2012).

members of parliament. The legislature[13] is made up of the National Council of Provinces[14] and the National Assembly.[15]

The SA judiciary[16] functions within the Roman-Dutch common law tradition while accepting some English common law legal traditions.[17] The Constitutional Court[18] is the highest court of appeals for constitutional issues. The Supreme Court is the highest court for non-constitutional issues. The High Court[19] addresses civil and criminal cases and appeals from Magistrate courts.

DPSIP legislation in SA can be based on the concept that identity and privacy are personality interests that are indivisible from the individual and are protected under the law of delict.

> Personality rights are characterized by the fact that they cannot be transferred to others, cannot be inherited, are incapable of being relinquished, cannot be attached and that they come into existence with the birth and are terminated by the death of a human being.[20]

---

[13] South Africa Government, *National Legislature - Parliament*. (2010), at http://www.info.gov.za/aboutgovt/parliament/index.htm (last visited on 5 August 2012).

[14] The National Council of Provinces includes the Premier and nine members selected by the provincial legislatures based on actual proportional elected officials in the nine provinces, including fifty–four permanent members and thirty-six special delegates.

[15] The National Assembly has between 350 to 400 members democratically elected including 200 elected from the provinces and 200 elected from a national roster.

[16] South Africa Government, *Justice System*. (2010), at http://www.info.gov.za/aboutgovt/justice/courts.htm (last visited on 5 August 2012).

[17] English common law as applied to constitutional or statutory law, criminal, corporate and mercantile law procedures. Roman-Dutch law predominates in private law including law of persons, property, succession, and the law of sale and lease. See Alan Watson, *Law Out of Context*, (University of Georgia Press ed. 2000).

[18] The court consists of eleven members including a Chief Justice and ten Deputy Chief Justices. Each serves a twelve-year term and is appointed by the President, Chief Justice, and National Assembly political leaders.

[19] The High Court has general jurisdiction and is headed by a Judge President.

[20] Anneliese Roos, *The Law of Data (Privacy) Protection: A Comparative and Theoretical Study* (2003) 545 (LL.D. thesis, UNISA). See also J Neethling, et al., *Neethling's Law of Personality* (LexisNexis 2nd ed. 2005); J Neethling, et al., *Neethling's Law of Personality* (Butterworths 1st ed. 1996).

6.2 Republic of South Africa Constitutional Declarations

The Constitution of the Republic of South Africa[21] is the supreme law of the land and the standard for all national laws and governmental actions. Unlike the US, the constitution provides for clear privacy rights. Chapter 2 covers the Bill of Rights. The SA Bill of Rights applies to private and state actors while the US Bill of Rights generally applies to governmental actions.[22]

Cass Sunstein conducted a comparative study of international constitutions. He determined that the Constitution of SA "is the world's leading example of a transformative constitution."[23] Sunstein found that the Constitution is "the most admirable constitution in the history of the world."[24] The framers analyzed international documents and various national constitutions.[25]

Unlike the preservative traditions in the UK and US, the SA Constitution provides for interpretation rules. Section thirty-nine requires that all courts or tribunals must advance the values of the Constitution while considering foreign and international law.[26]

Section fourteen addresses privacy rights. The text clearly states, "Everyone has the right to privacy, which includes the right not to have (a) their person or

---

[21] Republic of South Africa, *Constitution of the RSA*. (1996), at http://www.info.gov.za/documents/constitution/1996/index.htm (last visited on 19 June 2012). (SA)

[22] Mark S. Kende, Constitutional Rights in Two Worlds: South Africa and the United States, (Cambridge University Press ed. 2009).

[23] Cass R. Sunstein, *Designing Democracy: What Constitutions Do*, (Oxford University Press ed. 2001). p. 224. A transformative Constitution "points(s) toward an ideal future" p. 58. For an analysis of preservative and transformative Constitutions see Lawrence Lessig, *Code and Other Laws of Cyberspace*, (Basic Books ed. 1999). pp. 213-214.

[24] Cass R. Sunstein, *Designing Democracy: What Constitutions Do.* (Oxford University Press ed. 2001). p. 261.

[25] Jeremy Sarkin, The Effect of Constitutional Borrowings on the Drafting of South Africa's Bill of Rights and Interpretation of Human Rights Provisions, 1 *University of Pennsylvania Journal of Constitutional Law* 2, 176 (2008). The framers drew from the Canadian Constitution (which is part of this study) and the German Constitution (which is not a part of this comparison).

[26] Republic of South Africa, *Constitution of the RSA.* (1996), at http://www.info.gov.za/documents/constitution/1996/index.htm (last visited on 24 January 2012). (SA)

home searched; (b) their property searched; (c) their possessions seized; or (d) the privacy of their communications infringed."[27]

Section thirty-two provides for a freedom of information provision for access to any "information held by the government." The section also applies to "any information that is held by another person and that is required for the exercise or protection of any rights" that could be misused. The section declares that "National legislation must be enacted to give effect to this right, and may provide for reasonable measures to alleviate the administrative and financial burden on the state."[28]

Section thirty-six provides for some limitations on the right to privacy. The section declares as follows:

> The rights in the Bill of Rights may be limited only in terms of law of general application to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom, taking into account all relevant factors, including (a) the nature of the right; (b) the importance of the purpose of the limitation; (c) the nature and extent of the limitation; (d) the relation between the limitation and its purpose; and (e) less restrictive means to achieve the purpose. Except as provided in subsection (1) or in any other provision of the Constitution, no law may limit any right entrenched in the Bill of Rights.[29]

The SA Constitutional Court has interpreted the constitutional privacy provisions over the years. In *S v. Jordan*[30] the court, under the 1993 interim Constitution, believed that privacy rights are based on the principles of human dignity. The case affirmed the criminalization of prostitution law and that the law did not violate human dignity or economic rights. The full court ruled that

---

[27] *Id.* at ¶ 14.
[28] *Id.* at ¶ 32.
[29] *Id.* at ¶ 36.
[30] *S v. Jordan* 2002 (6) SA 642 (CC); 2002 (11) B.C.L.R. 1117; 2002 (6) SA 642, at 81. (SA)

although it may be argued that the right to privacy is limited by the Act, the limitation is reasonable and justifiable under section 36(1) of the Constitution.

The Constitutional Court adopted the U.S. reasonable actual or subjective expectation of privacy rule. In *Bernstein v. Bester*[31] Bernstein argued for a privacy right to not produce books, papers, or other records under the Company Act. Justice Ackermann wrote as follows:

> [I]t seems to be a sensible approach to say that the scope of a person's privacy extends *a fortiori* only to those aspects in regard to which a legitimate expectation of privacy can be harbored … A 'legitimate expectation of privacy' has two components a *subjective expectation* of privacy and that the society has recognized that expectation *objectively reasonable.*[32]

The South African Law Reform Commission addressed the issues of Privacy and Data Protection. The Commission found that "A person's right to privacy entails that such a person should have control over his or her personal information and should be able to conduct his or her personal affairs relatively free from unwanted intrusions."[33]

Some DPSIP advocates in SA take the position that information privacy is not an absolute right. They argue that a number of factors must be considered. The commercial interests, including banking, direct marketing, health care, insurance, pharmaceuticals, and travel sectors want special DPSIP considerations. The problem is that many of these commercial sectors are the worst offenders of information privacy principle violations. AU, CA, the UK, and the US have found privacy violations in these sectors.[34] These same commercial advocates argue that consideration must be taken to protect their interests, freedoms, and rights. The classic argument of maintaining law and

---

[31] *Bernstein v Bester* 1996 (2) SA 751 (CC); 1996 (4) BCLR 449. (SA)
[32] *Id.* at 75-76. (emphasis added)
[33] SA Law Reform Commission, *Issue Paper on Privacy and Data Protection*. (2003), at http://www.doj.gov.za/salrc/ipapers.htm (last visited on 6 March 2012), ¶ 1.2.1.
[34] See Chapter 1.4 and Chapter 2.4 of the current work.

order and even governing national social programs is made against acceptance of DPSIP standards.[35] Such issues are not a zero-sum game; nor does the legal principle of proportionality always apply. Clearly written and monitored exceptions can be instituted.

6.3 South African Legislation

At the time of this writing, SA does not have comprehensive DPSIP legislation,[36] although the legislature has enacted some related efforts. Perhaps part of the problem is an unintended consequence of the Constitution granting heightened legal protections to corporations. The experience of AU, CA, and the US certainly shows negative consequences of such a policy. Corporations perceive themselves as above the law, especially when multinational organizations are involved.[37]

In most of the countries involved in the study, there was a time that the Courts and common law were a force for reasoned or enlightened change. Over the past few decades, this pattern has changed. Court decisions are not always impartial and are subject to economic, personal, and political biases. A classic study supporting this view was conducted by Sunstein.[38] Thus, if SA is to join the community of DPSIP nations, legislation is the only alternative. Political interests and power politics must be examined. The most reasoned approach is to benchmark the effort with other countries. SA has the strategic

---

[35] SA Law Reform Commission, *Media Statement by the South African Law Reform Commission: Project 124: Privacy and Data Protection*. (2005), at http://www.nqf.org.za/download_files/nqf-support/Privacy%20and%20Data%20protection%20Paper%2024%20Project%20124.pdf (last visited on 2 May 2012).

[36] A Protection of Personal Information bill has been proposed and is being evaluated at the time of this writing. Analysis of the bill is found in § 6.6 in this chapter.

[37] See Don Tapscott & David Ticoll, *The Naked Corporation: How the Age of Transparency Will Revolutionize Business* (Free Press. 2003); Wade Rowland, *Greed, Inc: Why Corporations Rule Our World* (Arcade Publishing. 2006); Lee Drutman & Charlie Cray, *The People's Business: Controlling Corporations and Restoring Democracy* (Berrett-Koehler Publishers, Inc. 2004); Joel Bakan, *The Corporation: The Pathological Pursuit of Profit and Power* (Free Press. 2004); Katherine Albrecht & Liz Mcintyre, *Spychips: How Major Corporations and Government Plan to Track Your Every Move with RFID* (Nelson Current. 2005).

[38] Cass R. Sunstein, *Why Societies Need Dissent* (Harvard University Press. 2003).

potential to advance the cause rather than play catch-up. By proposing DPSIP legislation, SA has started to move to be aligned with international standards. SA must only be true to itself.

The *Open Democracy Bill*[39] was an early attempt at data protection legislation. The full bill never passed; however, some provisions been incorporated in other legislation. The original bill grants a person the right to have access to one's personal data held by governmental or private bodies. The person may request correction of inaccurate information by amending, deleting, or supplementing the data.[40] When the request is approved, the organization must inform governmental bodies and third parties that had previously received faulty data.[41] If the request is rejected, a note showing the decision is entered into the file. The Bill establishes some basic fair information practices like consent and disclosure.[42] The Bill also establishes some standard exceptions, as noted in other such legislation in AU, CA, the UK, and the US.[43] Thus, the Bill suffers from the same data protection gaps. The data collection provisions of the Bill apply only to governmental agencies. This same error was found in early CA legislation.[44]

In 2000, the *Promotion of Access to Information Act*[45] was enacted. The statute provides that individuals have a legal right to review computer and manual records that contain information regarding a person. The law is similar to provisions found in the laws of the other countries in this study. The law applies to accessing personal data held by governmental agencies and private organizations.[46] The law applies to data held by public and private

---

[39] *Open Democracy Bill* B 67-98 (1999). (SA) at http://www.info.gov.za/view/DownloadFileAction?id=71512 (last visited on 21 April 2012).
[40] *Id.* at B 67-98 ¶¶ 51, 52.
[41] *Id.* at B 67-98 ¶¶ 51(7), 52(9).
[42] *Id.* at B 67-98 ¶ 57.
[43] See chapters 4.3, 5.3, 7.3, 8.3 of this work.
[44] See chapter 4 of this work.
[45] *Promotion of Access to Information Act.* Act 2 of 2000 (2000). (SA) at http://www.info.gov.za/view/DownloadFileAction?id=68186 (last visited on 20 April 2012).
[46] Act 2 of 2000 ss (11) and (50).

bodies.[47] The Act is basically a Freedom of Information Act rather than DPSIP legislation.

The law recognizes the SA Constitutional access to information and privacy rights; however, it actually limits many of these rights.[48] One of the objectives of the Act is to provide reasonable privacy protections and balance the Bill of Rights protections.[49] Chapter Three of the Act does, with restrictions, allow personal access to one's own data and the right to ask for corrections. Consistent with the Constitution, the Act applies to juristic and natural persons.[50] The government has the power to deny a request for information based on its own priorities. A party may apply for an internal review of a governmental agency[51] for an adverse decision, or apply to the courts[52] for review.

The public or private data holder must refuse access to requested data when the release would unreasonably reveal data regarding a third party or a deceased person.[53] Release of data is granted when the person has consented,[54] when the data is publically available,[55] even when the government has or will release the data,[56] when the release is in the best interest of a child,[57] and when a next of kin for a deceased person consents in writing.[58] The Act is monitored by the South African Human Rights Commission.

---

[47] *Id.* at ¶ 12.
[48] Many legislators or parliamentarians have a pattern of writing access or DPSIP legislation using key words; however, the actual Act limits the rights in question.
[49] Act 2 of 2000 ¶¶ 9(b)(i)(ii).
[50] Generally, juristic persons have more economic and political powers than natural persons.
[51] Act 2 of 2000 ¶ 75.
[52] Act 2 of 2000 ¶¶ 78 (1)(2).
[53] *Id.* at ¶¶ 34 and 63.
[54] *Id.* at ¶¶ 34(2)(a), 63(2)(a).
[55] *Id.* at ¶¶ 34(2)(b), 63(2)(b).
[56] *Id.* at ¶¶ 34(2)(c), 63(2)(c).
[57] *Id.* at ¶¶ 34(2)(d), 63(2)(d).
[58] *Id.* at ¶¶ 34(2)(e), 63(2)(e).

In 2002, the *Electronic Communications and Transactions Act* was enacted.[59] Chapter One of the law offers some general definitions of personal information.[60] The law provides for voluntary compliance of data controllers when they electronically collect personal data. Both the data controller and data subject must agree to the terms.[61] The aim is to address public concerns regarding privacy and electronic processing of personal data. The Act applies only to natural persons whose data is electronically processed after the Act was passed. The Act calls for voluntary compliance with all of the stated guidelines; however, the provisions are not legally binding on all data controllers. The Act establishes nine rather common data processing principles.[62] The major impact of the Act is in the credit reporting and

---

[59] *Electronic Communications and Transactions Act.* Act 25 of 2002 (2002). (SA) at http://www.internet.org.za/ect_act.html (last visited on 21 April 2012). (SA)

[60] *Id.* at Chapter 1. The section reads **"personal information**" means information about an identifiable individual, including, but not limited to(a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the individual; (b) information relating to the education or the medical, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved; (c) any identifying number, symbol, or other particular assigned to the individual; (d) the address, fingerprints or blood type of the individual; (e) the personal opinions, views or preferences of the individual, except where they are about another individual or about a proposal for a grant, an award or a prize to be made to another individual; (f) correspondence sent by the individual that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence; (g) the views or opinions of another individual about the individual; (h) the views or opinions of another individual about a proposal for a grant, an award or a prize to be made to the individual, but excluding the name of the other individual where it appears with the views or opinions of the other individual; and (i) the name of the individual where it appears with other personal information relating to the individual or where the disclosure of the name itself would reveal information about the individual, but excludes information about an individual who has been dead for more than 20 years.

[61] *Id.* at Chapter 8, ¶¶ 50-51.

[62] Chapter 8, ¶ 51 defines the principles that include "(1) A data controller must have the express written permission of the data subject for the collection, collation, processing or disclosure of any personal information on that data subject unless he or she is permitted or required to do so by law.
(2) A data controller may not electronically request, collect, collate, process or store personal information on a data subject which is not necessary for the lawful purpose for which the personal information is required.
(3) The data controller must disclose in writing to the data subject the specific purpose for which any personal information is being requested, collected, collated, processed or stored.
(4) The data controller may not use the personal information for any other purpose than the disclosed purpose without the express written permission of the data subject, unless he or she is permitted or required to do so by law.
(5) The data controller must, for as long as the personal information is used and for a

customer relations sectors. In contrast to the private domain registration processes used in the other countries in the current study, the Act shifts the function to a government operated Domain Name Authority. The governmental agency has direct control over domain name registration and related private information. In other countries in the study, this data is accessible only through secondary sources. The government is given the power to declare that some data bases maintain critical data and must be registered with and held accountable to the Minister.[63] However, the operational standards the government applies to determine what qualifies as "critical data bases" are unclear.

The *Regulation of Interception of Communications and Provision of Communication-related Information Act*[64] establishes duties, exceptions, and prohibitions for nearly all forms of personal and technological communications. The act declares: "no person may intentionally intercept or attempt to intercept, or authorize or procure any other person to intercept or to attempt to intercept, at any place in the Republic, any communication in the course of its occurrence or transmission."[65] The act provides for a number of exceptions,[66] some of which make practical sense. These include to prevent bodily harm,[67] emergency locations,[68] and exceptions authorized by other

---

period of at least one year thereafter, keep a record of the personal information and the specific purpose for which the personal information was collected.
(6) A data controller may not disclose any of the personal information held by it to a third party, unless required or permitted by law or specifically authorized to do so in writing by the data subject.
(7) The data controller must, for as long as the personal information is used and for a period of at least one year thereafter, keep a record of any third party to whom the personal information was disclosed and of the date on which and the purpose for which it was disclosed.
(8) The data controller must delete or destroy all personal information which has become obsolete.
(9) A party controlling personal information may use that personal information to compile profiles for statistical purposes and may freely trade with such profiles and statistical data, as long as the profiles or statistical data cannot be linked to any specific data subject by a third party."

[63] *Id.* at Chapter IX.
[64] Regulation of Interception of Communications and Provision of Communication-related Information Act amend. No. 70 of 2002 (2002). (SA)
[65] *Id.* at Chapter 2, part 1.
[66] *Id.* at Chapter 1, part 1.
[67] *Id.* at ¶ 7.
[68] *Id.* at ¶ 8.

acts.[69] Other exceptions allow the application of questionable standards including interception directions,[70] one of the parties intercepts,[71] one of the parties' consents,[72] and selected business indirect communications.[73] A set of law enforcement exception are also included.[74]

Only identified officials may apply for a warrant; moreover, one must show reasonable grounds for access. The grounds are rather expansive and include a serious offense that is actual, potential, or probable. The threat can be related to a wide range of poorly defined issues, including the economic interests of SA, national security, public health, and/or public safety. The data subject does not need to be informed of the monitoring.[75]

The Act has little to do with actual information privacy or data security. The provisions of the Act appear to contradict section fourteen of the Bill of Rights. In contrast to similar UK and US statutes, the SA approach requires a judicial decision to intercept any violations.

The passage of a massive surveillance act prior to establishing sound DPSIP legislation suggests that SA has decided that monitoring is more important than privacy.[76] However, the Act is consistent with the Council of Europe Convention on Cyber crime.[77]

The *National Credit Act*[78] is similar to credit bureau regulation in some other countries. The Act is not as data protective as the AU approach.[79] The provisions establish a confidentiality standard for those who have access to

---

[69] *Id.* at ¶ 9.
[70] *Id.* at ¶ 3.
[71] *Id.* at ¶ 4.
[72] *Id.* at ¶ 5.
[73] *Id.* at ¶ 6.
[74] *Id.* at ¶¶ 4(2), 5(2), 7, 8, 9.
[75] *Id.* at Chapter 3.
[76] Caroline B. Ncube, Watching the Watcher: Recent Developments in Privacy Regulation and Cyber-Surveillance in South Africa, 3 *SCRIPTed - A Journal of Law, Technology & Society* 4, 344 (2006).
[77] CA, SA, and the US are signatories to the Convention.
[78] *National Credit Act* 34 of 2005 (2005). (SA)
[79] See Chapter 4 of this work.

personal credit information. The data must be accurate and maintained for set periods of time. Data that is not allowed to be stored must be eliminated.

The *Consumer Protection Act*[80] establishes an accessible, efficient, fair, responsible, and sustainable legal framework for consumer markets. The purpose of the Act is to help establish fair business practices related to consumer issues. The Act addresses deceptive, fraudulent, improper, misleading, unfair, unjust, and/or unreasonable business conduct and trade practices.[81] The Act establishes a moderate no-fault liability standard for damages related to death, economic losses, injury, and physical damages caused by defective or unsafe products.[82] The provisions apply to all business transactions including franchises, manufacturers, municipalities, non-governmental organizations, professional service providers, retailers, and trade unions.[83] Key principles of the Act must be transferred to any DPSIP legislation.

The Act is intended to enable informed consumer choice and empowerment through awareness and information. The Act establishes a non-adversarial function to resolve consumer transaction disputes by establishing a balance of power for persons who are in a weaker bargaining position. The consensual approach is intended to establish an accessible, consistent, effective, efficient, and harmonized approach to establishing redress for consumer complaints.[84] Although the Act is not a specific DPSIP legislation, the Act does establish a principle of informed consent and the need to protect consumers. Moreover, the Act does establish a consumer's right to privacy and a strict liability standard.[85] The National Consumer Commission is responsible for

---

[80] *Consumer Protection Act* 68 0f 2008 (2008). (SA) The Act came into effect on 1 April 2012 and will be implemented during the next 18 months.

[81] *Id.* at Chapter 2.

[82] *Id.* at ¶ 61.

[83] *Id.* at ¶ 5.

[84] *Id.* at ¶ 69.

[85] *Id.* at Part B ¶ 11(1). The right of every person to privacy includes the right to *(a)* refuse to accept; *(b)* require another person to discontinue; or *(c)* in the case of an approach other than in person, to preemptively block, any approach or communication to that person, if the approach or communication is primarily for the purpose of direct marketing.

administering, applying, and enforcing the Act. Members of the Commission are appointed by the Ministry.[86]

The Act is reasonably consistent with similar consumer protection laws in AU, CA, the UK, and US.[87] As with DPSIP legal and regulatory acts, the business community resisted passage of the Act; instead, businesses labeled the Act as draconian and proclaimed that it would limit business opportunity.[88] As with almost all such claims, the predictions failed to develop and are basically fear-based propaganda.

The *Protection of State Information Bill*[89] is a controversial effort to provide for the free flow of information and protect national security. Critics maintain that the Bill is a modern form of censorship. The Bill actually imposes information restrictions and provides for a maximum criminal penalty of twenty-five years in prison.[90] Critics claim that the Bill represents an abuse of power and is opaque rather than transparent.[91] Opponents claim that the Bill will restrict whistleblower options and allow officials to legally raid houses and offices to search for data without judicial permission or review.[92]

The Bill addresses a number of data security measures.[93] The problem is that the standards are applicable to all governmental agencies and only some

---

[86] *Id.* at ¶¶ 86, 87.
[87] *Id.* at ¶¶¶¶ 4.3, 5.3, 7.3, 8.3 of this work.
[88] Bizcommunity.Com, *Consumer Protection Act Made Easy* (2010, March 15), at http://www.bizcommunity.com/Article/196/307/45701.html (last visited on 24 April 2012).
[89] Protection of Information Bill B6 of 2010 (2010). (SA)
[90] *Id.* at ¶ 32.
[91] Lynley Donnelly, *The Right to Demand Answers*, Mail and Guardian. (2011), at http://mg.co.za/article/2011-04-29-the-right-to-demand-answers (last visited on 4 May 2012).
[92] Freedom Information, *POIB Protestors March in Cape Town; Hearing Set*, Freedom Information. (2010), at http://www.freedominfo.org/2010/10/poib-protestors-march-in-cape-town/ (last visited on 14 October 2012). On 22 November 2011, the Parliament passed the bill. Several steps re needed for the bill to become law.
[93] *Protection of Information Bill* B6 of 2010 (2010). (SA) s 1 information security includes (a) document security measures; (b) physical security measures for the protection of information; (c) information and communication technology security measures; (d) personnel security measures; (e) continuity planning; (f) security screening; (g) technical surveillance counter-measures; (h) dealing with and reporting of information security breaches; (i) investigations into information security breaches;

juristic and natural persons. While proclaiming that the free flow of information is critical to human rights and democracy, the government has the power to control the exchange of valuable information.[94] Furthermore, the definitions have little operational clarity. National interests include such concepts as democracy, economic growth, free trade, justice, security, sound international relations, a stable monetary system, and survival.[95] From an operational perspective, such concepts have little meaning. Commercial information is more protected than personal information. Few checks and balances are provided for review of governmental classification systems except for an internal ten-year review. When the government declassifies certain information, it may be released to the public. Criminal standards can be enforced for espionage, harboring or concealing of persons, hostile activity, as well as interception or interference with classified information.[96] The SA parliamentary committee responsible for the Bill has asked for an extension of time to review controversial provisions.[97]

None of the successful SA legislative actions to date focus on generally acceptable DPSIP standards. No privacy assessments or audits are required. Limited legal attention has been paid to the threat of data mining. There is no requirement for establishing a Chief Information or Security Officer within the government or in the business sector.

An argument can be made that a person's information privacy rights are covered, by analogy, with the moral rights principle in intellectual property law because the data subject creates the data. Section 20 of the *Copyright Act*

---

and (j) administration and organisation of the security function at organs of state to ensure that information is adequately protected.

[94] *Id.*at ¶ 1 valuable information includes *(a)* the information that should be retained for later use or reference; and *(b)* that the alteration, loss or destruction of such information is likely to—(i) impede or frustrate the State in the conduct of its functions; and (ii) deny the public or individuals of a service or benefit to which they are entitled.

[95] *Id.* at ¶ 11.

[96] *Id.* at Chapter 11.

[97] Freedom Information, *South African Committee to Seek Extension of Time*, Freedom Information. (2011), at http://www.freedominfo.org/2011/01/south-african-committee-to-seek-extension-of-time/ (last visited on 28 January 2012).

sets forth some fundamental principles.[98] The data subject "shall be deemed to be the owner of the copyright in question."[99] The data subject "shall have a right to claim authorship of the work and to object to any distortion, mutilation or other modification of it, where such action is or would be prejudicial to the honor or reputation of the author."[100] A key issue in this scenario involves informed consent.

6.4 South African Case Law

Before examining the common or case law determinations on DPSIP legal issues, it is important to examine the power and reality constraints on the highest court in the jurisdiction. A discussion without a common benchmark would be meaningless. A legal declaration without exploring and understanding the de facto influences is narrow-minded. The US Supreme Count was selected as the benchmark for this study because, in theory, it represents the international standard in the rule of law, balance of powers, and political independence analysis. Granted, evidence exists that the benchmark Court has been inconsistent. The SA Court has been influenced by a number of historical lessons; the common law tradition is different from the English common law of the other nations in this analysis.

Table 6.0 Comparison of South African and United States Supreme Court

Factor	**South Africa Constitutional Court**[101]	**US Supreme Court**[102]
Established	1994	1789

[98] Copyright Act 98 of 1978 (1978). (SA)
[99] *Id.* at ¶ 20(2).
[100] *Id.* at ¶ 20(1).
[101] Constitutional Court of South Africa, *Constitutional Court of South Africa*. (2011), at http://www.constitutionalcourt.org.za/site/home.htm (last visited on 29 May 2012).
[102] Kermit L Hall, *The Oxford Companion to the Supreme Court of the United States* (Oxford University Press 2nd. ed. 2005). See also Supreme Court of the United States, *About the Supreme Court*. (2010), at http://www.supremecourt.gov/ (last visited on 5 July 2012).

Power of decisions	Applies to all governmental functions.	Applies to all courts and jurisdictions in the country.
Membership	One Chief Justice, one Deputy Chief Justice, and nine Justices.	One Chief Justice and eight associate justices (currently).
Appointee Background	Leading legal professionals.	Leading appellate courts judges, politicians, and law professors.
Term of Office	Serves non-renewable 12- to 15-year term depending on age at appointment.	Life or until retires.
Jurisdiction	Original and appellate on issues related to Constitutional matters. Can respond to a request based on a parliamentary bill.	Original and appellate.
Role	Error correction, support the Constitution and consider international human rights standards of rulings of other courts in democratic nations.	Error correction.
Operations	Relies on written submissions except in situations when oral evidence is required to clarify issues.	Hears oral arguments but relies heavily on arguments presented in written briefs.
Decisions	Opinion of the majority, written by each justice showing the rationale and decision. Concurring and dissenting opinions are also published.	Opinion of the majority, written by one justice, and concurring and dissenting opinions of other justices.
Judicial Review	Can declare acts of parliament and the President as null and void.	Historic since Marshall.
Appointment	President appoints, based on a Judicial Service Commission report,	President nominates, Senate confirms.

	in conjunction with the Chief Justice and Assembly political leaders.	
Representation	Justices can not be members of the government or political parties.	Recently more political.
Opinions	No advisory opinions.	No advisory opinions.
Case Assignment	Court has discretionary control except when a previously constitutional invalidation must be confirmed.	Court determines what cases it will hear based on writ of certiorari. Since 1925, has discretionary docket control.

The SA Constitutional Court seeks to make decisions based on a consensus to ensure a high-quality decision. Several meetings may be conducted. The US Supreme Court only meets once and assigns opinions based on the majority with dissenting opinions. The Constitutional Court does not limit the time of oral arguments and does not make a transcript, whereas the US Supreme Court only hears oral arguments for a limited time and does make a transcript.[103]

Unlike the other countries in this study, the SA common law is based on Roman-Dutch legal traditions. The SA common law also includes modern SA law and some principles from UK common law. Thus, SA common law recognizes negligence based on foreseeability by a reasonable person and that a causal nexus is essential. The standard is raised when a duty of care exists. Roman law had the means to protect privacy; however, there was no perceived need to address the issue formally.[104]

South African case law does recognize a duty to care and to not act in a negligent manner. While the specific issues of legal concern differ from a DPSIP perspective, a number of cases establish the principle that one can be

[103] Mark S. Kende, *Constitutional Rights in Two Worlds: South Africa and the United States*, (Cambridge University Press ed. 2009).
[104] M. D. Blecher, Aspects of Privacy in the Civil Law, 43 *Tijdschrift voor Rechtsgeschiedenis*, 279 (1975).

held liable for not using standard precautions.[105] The principle is extended to those that borrow, deposit, hire, or lease the property of another.[106]

The law accepts that a breach of trust or confidence is unlawful. Under copyright law, a person has the right to communicate, limit, publish, or restrict what one has prepared or written.[107] A similar case can be made for private facts.[108] A person's privacy rights must be protected from unlawful invasion or unlawful publication.[109]

At times, the SA Court is similar to the current activist conservative court in the US in its ability to practice selective attention. For centuries, in most parts of the world, a medical practitioner[110] has had a duty to protect patient data. The standard is near sacrosanct. When one practitioner refused to supply the government with some requested confidential data, he was criminally charged for violating a statistics act. While he claimed a privacy right, the court found that the statistics act held a higher priority.[111] The court found that there was a higher benefit to the community.[112] Such a finding is counter to thousands of years of medical practice and confidentiality law.

O'Keefe v. Argus Printing & Publishing Co. Ltd[113] establishes that, although much depends on the totality of circumstances in a given case, a person has a legal right to privacy. The case also addresses the importance of requiring consent[114] prior to another using one's information. In this case, a picture was used for commercial purposes. Damages are based on the content, extent of publication, and nature of the publication. All of these standards are outside

---

[105] *Van Tonder v. Alexander*, 1906 E.D.L.D. 186, (1906). (SA) Also see *Hendy v. Oomkens abd Shallies*, 1924 T.P.D. 165, (1924). (SA)
[106] *Madallie & Schieff v. Roux*, 1920 (20) S.C. 438, (1920). (SA)
[107] See *Jeffreys v Boosey*, 1854 (4) HLC 815 862, (1854). (SA)
[108] *National Media Ltd v Jooste*, 1996 (3) SA 262 (A) 271-272, (1996). (SA) See also *O'Keeffe v Argus Printing and Publishing Co Ltd*, 1954 (3) SA 244 (1954). (SA)
[109] *Motor Industry Fund Administrators (Pty) Ltd v Janit*, 1994 (3) SA 56 (W) 60, (1994). (SA)
[110] A medical doctor in the US and CA.
[111] *S v Bailey*, 1981 4 SA 187 (N). (SA)
[112] Such a rationale recalls Dr. Samuel Johnson's April 7, 1775 statement that "Patriotism is the last refuge of a scoundrel."
[113] *O'Keefe v. Argus Printing & Publishing Co. Ltd* 1954 (3) SA 244 (CPD). (SA)
[114] See *Waring & Gillow Ltd v Sherborne*, TS 340, 344 (1904). (SA)

of the control of the data subject. Under the decision, an apology can be considered a mitigating factor in determining damages.[115]

The court modernized relevant Roman law principles by determining that the right to privacy is an independent personality rights. The principle was reaffirmed in *Mhlongo v Bailey*,[116] *Gosschalk v Rossouw*,[117] *S v A*,[118] *Rhodesian Printing and Publishing v Duggan,*[119] and *La Grange v Schoeman.*[120]

The Supreme Court of Appeals[121] has also recognized a right to privacy under SA law. The right is considered a personality right.[122] In *National Media Ltd v Jooste*[123] the Court accepted that privacy is an interest of personality.[124] The legal protection applies only to "ordinary or reasonable sensibilities and not to hypersensitiveness."[125] Information privacy protections are not extended to those who are distressed beyond ordinary feelings and intelligence.[126] The Court also found that eavesdropping on conversations intended to be private is a privacy violation.[127] The individual person has the right to determine what data is private and what is not. However, if the person does not show such a desire to keep information private, the privacy is lacking. Such a standard

---

[115] Kidson v SA Associated Newspapers LTD, 1957 (3) SA 461 (W) at 468. (SA)
[116] *Mhlongo v Bailey*, 1958 (1) SA 370 (C). (SA)
[117] *Gosschalk v Rossouw*, 1966 (2) SA 476, 492 (C). (SA)
[118] *S v A*, 1971 (2) SA 293 (T). (SA)
[119] *Rhodesian Printing and Publishing v Duggan* 1975 (1) SA 590 (R). (SA)
[120] *La Grange v Schoeman*, 1980 (1) SA 885 (E) (SA). See also *Financial Mail v Sage Holdings* 1993 (2) SA 451 (A)(SA); Janit v Motor Industry Fund Administrators 1995 (4) SA 293 (A) (SA); *Jansen van Vuuren v Kruger* 1993 (4) SA 842 (A)(SA); and National Media v Jooste 1996 (3) SA 262 (A). (SA).
[121] Formerly known as the Appellate Division.
[122] *Jansen van Vuuren v Kruger*, 1993 (4) SA 842 (A) (SA); *National Media Ltd v Jooste,* 1996 (3) SA 262 (A) (SA); *Financial Mail (Pty) Ltd v Sage Holdings Ltd,* 1993 (2) SA 451 (A) (SA); and *Janit v Motor Industry Fund Administrators (Pty) Ltd,* 1995 (4) SA 293 (A). (SA)
[123] *National Media Ltd v Jooste*,1996 (3) SA 262 (A) 271-272 (1996) (SA). The Court defined the right to privacy as "The right to privacy encompasses the right to determine the destiny of private facts, which includes the right to decide when and under what conditions private facts may be made public" at 271.
[124] For an explanation of the concept see J Neethling, et al., *Neethling's Law of Personality* (LexisNexis 2nd ed. 2005).
[125] *National Media.* Ibid., at 271.
[126] *Financial Mail (Ply) Ltd v Sage Holdings Ltd,* 1993 2 SA 451 (A). (SA) Such a determination certainly calls for expert psychiatric and/or psychological evidence.
[127] *S v A*, 1971 (2) SA 293 (T). (SA)

places a heavy responsibility on the person to make informed decisions when essential data is absent.

The Court has also determined that one has an interest against unauthorized misuse of personal information.[128] The SA Court has accepted the legal doctrine of increasing protections when there is an expectation of privacy.[129] In *Case v Minister of Safety and Security,* the Court offered a further definition of information privacy.[130]

SA common law recognizes the importance of consent for release of personal information as a legally protected privacy right. However, the consent must be informed. The person must know the benefits and potential harms or risks involved. The person must appreciate, realize, and understand the potential of infringement, the nature of the consent, and the intended purpose of the data. The consent must be voluntary and revocable. The consent must be consistent with public policy.[131]

> In *Mistry v Interim Medical and Dental Council of South Africa*,[132] the Constitutional Court ruled that information privacy could be limited. The limitations include intimate information that was collected in an intrusive manner or was used for a purpose that was not collected for that purpose. Further limitations include when the personal information is given to the press or general public or to persons the applicant could reasonable expect privacy.[133]

---

[128] *Grutter v Lombard*, 2007 (4) SA 89 (SCA). (SA)
[129] See *Bernstein v Bester*, RSA 1996 (2) SA 751 (CC); 4 BCLR 449 (1996) (SA); *Protea Technology v Wainer* [1997] 3 All SA 594 (W) 608; 1997 9 BCLR 1225 (W) 1241). (SA)
[130] *Case v Minister of Safety and Security* 1996 (3) SA 617 (CC) (SA). The Court found that "The right to privacy includes the right to be free from intrusions and interference by the state and others in one's personal life and freedom from unauthorized disclosures of information about one's personal life."
[131] *C v Minister of Correctional Services*, 1996 (4) SA 292, 300-304 (T) (SA); *Castell v De Greef* 1994 (4) SA 408, 420-421 425-426 (T). (SA)
[132] *Ministry v Interim Medical and Dental Council of South Africa*, 1998 (4) SA 1127 (CC). (SA)
[133] *Id.* at 1151-1156.

In 2001, the Constitutional Court recognized the need for the common law to be developed to comply with standards required by the Bill of Rights.[134] The Court has been slow to actually respond; instead, the Court preferred to turn the issue over to the legislature. In theory, in most constitutional governments, the obligation rests with all three branches of government. The issue is to address the spirit and the letter of the law.

The Constitutional Court has accepted a reasonableness standard in determining an informational privacy right. The reasonable expectation of privacy can decrease as the sense of personal space is lowered.[135] The Court later determined that the person must have the ability to determine if facts should be made publically available.[136] A right to privacy exists even in automobiles, on personal mobile phones, and in corporate offices.

The SA courts have accepted the principle that juristic persons have information privacy rights. In *Financial Mail (Pty) Ltd v Sage Holdings Ltd,*[137] the court recognized that corporations can not have feelings such as being offended or outraged. However, legal protections can be imposed in the absence of injured feelings.[138] Corporations have a right to protect confidential oral or written information between stakeholders.[139] Reasonable minds prevailed in recognizing privacy rights for juristic persons. The court found that natural persons have a heightened right to protect human dignity.[140] Under this decision, the interests of juristic persons may vary depending on the nature of the organizations. The level of needed protections of

---

[134] *Carmichele v Minister of Safety and* Security (Centre for Applied Legal Studies Intervening), 2001 (4) SA 938 (CC). (SA)

[135] *Bernstein v Bester*, RSA 1996 (2) SA 751 (CC); 4 BCLR 449 (1996). (SA)

[136] *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Ply) Ltd* 2001 (1) SA 545 (CC). (SA)

[137] *Financial Mail (Pty) Ltd v Sage Holdings Ltd,* 1993 (2) SA 451 (A). (SA)

[138] This reasoning runs counter to the standard established in *National Media Ltd v Jooste.* Why are the standards different for natural persons and corporations?

[139] *Janit v Motor Industry Fund Administrators (Ply) Ltd*, 1995 (4) SA 293 (A). (SA) The Court found that the theft of confidential business meeting recordings and offering the tapes to a third party was a privacy violation. However, the court has denied the same standard to natural persons.

[140] Investigating Directorate: *Serious Economic Offences v Hyundai Motor Distributors* (Pty) Ltd 2001 (1) SA 545 (CC). (SA)

membership organizations, including fraternal, political, religious, or trade unions are different from large for-profit corporations.

6.5 Protection of Personal Information Bill Background

Since 2000,[141] the SA government has been in the process of writing and passing a Protection of Personal Information Bill. The proposed Bill is built on the successes and failures of prior data protection and information privacy laws and regulations in different countries.

In 2000, the South African Law Reform Commission began working on critical DPSIP issues. In 2003, the first discussion paper was issued. A draft bill was circulated in 2005 and 2006; however, it essentially died. Some sources claimed that the Bill could be enacted in 2011; however, progress is slow.

The Bill is not without its critics. Business interests' opposition and some governmental resistance are evident. Opponents claim that the approach will cost too much money, opens litigation options for violations, is unrealistic, and will result in poor compliance.[142] Industry groups that are calling for implementation delays include the Banking Association of SA, Business Unity SA, and South African Insurance Association.

The Commonwealth Human Rights Initiative and South African History Archive have submitted comments of caution related to the Bill.[143] The organizations are concerned that DPSIP legislation in SA will negatively

---

[141] Depending on the standard to be applied, this is a long-term period. After the 9/11 attacks on the World Trade Center, the US Congress took only a few days to pass the previously written Patriot Act to grab unprecedented governmental power. However, health care reform in the US started during the Truman administration and has still to be fully realized, which suggests a comparatively short-term period.

[142] See Audra Mahlong, *High Costs of Privacy Bill: Government will Spend R35 Million to Pilot Systems, But No Further Funding has been Secured,* IT Web Business 3 November 2009. When benchmarked with the experience in other countries, such claims create a state of fear mongering.

[143] See Commonwealth Human Rights Initiative, *Comments Concerning the South Africa Privacy and Data Protection Bill*. (2006), at http://www.humanrightsinitiative.org/programs/ai/rti/international/laws_papers/southafrica/south_africa_privacy_bill_submission_feb06.pdf (last visited on 27 February 2012).

impact the force of the *Promotion of Access to Information Act*. The Archive is also concerned with the right to be forgotten. Critics want private and public sector information to be held to different standards. The proposal is that a regulatory agency be established; however, the agency should report to Parliament. Such an approach questions the independence of the regulators. The Human Rights Initiative is concerned that DPSIP legislation will protect the accountability of public officials. Concerns have also been raised about the public's right to know; however, no safeguards are proposed.

When proper checks and balances are established and enforced, certain organizations have a legitimate need to collect, process, and even store personal information regarding data subjects. Such organizations provide services for the direct benefit of the data subject and the community at large. Given these constraints, the list includes legally established and monitored governmental agencies. Private organizations that also have a regulated need for data subject information include banks, credit reporting agencies,[144] financial institutions, health care providers,[145] insurance companies and regulators, and medical professionals. However, each of these examples includes a standard of duty to care, data subject review, confidentiality, and informed consent.

Although direct marketing companies claim they have a legitimate need to collect and use personal data, and that they meet the exemption provided to those who provide services that benefit the individual and the community, direct marketing *per se* does not meet the above lawful constraints. Almost everyone in developed countries is aware of spam e-mail, junk mail, cookies, and advanced cookie technologies. The direct marketing industry functions for the purpose of greed and company profits. The political problem is that business organizations can join forces to protect the capital interests of all businesses to create a parade of horrible consequences for all. The political power problem in SA is enhanced by the decision to include juristic

[144] AU has the most advanced credit reporting law. See Chapter 4 above.
[145] The US HIPAA legislation is certainly strong. See Chapter 8 below.

organizations as having protections under the Bill of Rights. Such organizations make false arguments regarding costs, expenses, and limitations on free markets, which of course are proposed as a public good.[146]

Beginning in 2000, the South African Law Reform Commission[147] has taken on the herculean task of supporting the enactment of enabling legislation that meets SA Constitutional mandates, reflects the will of the SA people,[148] and helps SA enter into the world of diverse DPSIP nations.

Attempting to review the special interest group responses is similar to the old English warnings of trying to herd domestic cats and watching sausage being made. Special interests groups often want exceptions based on whose ox is being gored.[149] Some groups wanted all household and personal data to be excluded. The Financial Board wanted the legislation to be very broad. IMS Health wanted a distinction between personal and professional data exclusions. Self-interest–based objections were voiced on a number of issues.[150] A consensus was established that the legislation should apply to all data regardless of forum, image, media, sound, or technology format. The definition certainly must cover all technological advances regardless of the whether the data is called "household," "personal," "professional," or something else, and regardless of form or medium.

---

[146] The reality is that modern businesses want to claim the power of the divine rights of Kings. See Wade Rowland, *Greed, Inc: Why Corporations Rule Our World* (Arcade Publishing. 2006) and Joel Bakan, *The Corporation: The Pathological Pursuit of Profit and Power* (Free Press. 2004).

[147] All commission reports starting in 2000 have been reviewed and analyzed. The basis of the current analysis relies on the most recent modifications. See South African Law Reform Commission, *Privacy and Data Protection Report: Project 124* (South African Law Reform Commission. 2009).

[148] See Chapter 2 of the current work.

[149] Groups want their selfish interests protected over what others may need. For example, the SABC did not want to cover the cost of insuring compliance on archival data due to projected costs. Thus, all previously established information would be excluded.

[150] The list includes anonymized/de-identified information (para 3.9); automatic and manual files (para 3.2); critical information (para 3.6); household activity (para 3.8); natural v juristic persons (para 3.4); professional information (including provider information) (para 3.10); public v private sector information (para 3.5); sensitive information (para 3.7); and sound/image information (para 3.3). See South African Law Reform Commission, *Privacy and Data Protection Report: Project 124* (South African Law Reform Commission. 2009) at Chapter 3, p. 2.

Given that SA is embracing DPSIP legal responses relatively late, attention must be focused on the developmental lessons of earlier stages. At first, identifying and protecting critical and sensitive information was essential. Advances in technology, including data mining and RFID, have made such distinctions essentially meaningless.

The South African Law Reform Commission advocates a number of key DPSIP principles. The processing of personal information should be balanced, fair, freely given, lawful, open, and proportional to the aim.[151] SA can learn from the experience of other nations noted in the current study and other national efforts. A basic approach to decisions includes establishing a comprehensive legal approach similar to AU, CA, and the UK. A decision can be made for using the less effective US sectoral approach when laws are enacted to address the latest technology or industry sector problems. The failed model of self-regulation found in the US (and in part in CA) describes the current SA reality. Each organization or industry has the right to develop voluntary standards. In developing a legal approach to DPSIP legal issues, SA can follow the current CA advocacy for including technological solutions.[152] Lee Bygrave and the UN approach suggest a need for a system of regulatory agencies and officials in the private and public sector that is completely impartial, independent, and technically competent.[153]

South Africa is more than an independent nation state. SA is economically and politically an integral part of the interdependent international community of nations. Given that there are DPSIP rogue states, some states (e.g., CA) are EU adequate, and some are not (e.g., AU). SA has the options of

---

[151] See Lee A. Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits* (P. Bernt Hugenholtz ed., Kluwer Law International. 2002).

[152] A preliminary list includes anonymous and pseudonymous browsing, email, re-mailing systems; biometric solutions readers, software etc; cookie managers; platform for Privacy Preferences or P3P; privacy by design; privacy-enhancing technologies; privacy policy generators; and smart cards/public key infrastructures.

[153] Lee A. Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits* (P. Bernt Hugenholtz ed., Kluwer Law International. 2002). This approach is even used in some sector regulations in the US – the FTC and HIPAA. See Chapter 8 of the current work.

meeting current international standards or, like India, pushing the bar higher.[154]

South Africa must make some important DPSIP legal decisions. Will SA adopt a comprehensive legal structure with independent authorities for public and private agencies? Will the law be written to avoid the fraud known as self-regulation? Will the approach be technology neutral and allow for needed adjustments as new technology or approaches are developed? Will the law require the use of technology-based protections prior to granting intellectual property protections? Will enforcement authorities have strong investigation and enforcement powers? Will SA adopt the UK data controller registration approach? Will a DPSIP privacy impact study be required for all related legislation? Will the SA government establish informed consent and the psychologically fairer opt-in standard? Is the SA government able and willing to withstand powerful business and corporate opponents who argue unsubstantiated cost predictions and the related parade-of-horrors? Is the SA government able and willing to withstand current US efforts to eliminate information privacy rights?[155] Will the SA government provide for strict or absolute liability standards for civil DPSIP violations and criminal

---

[154] See Stephanie Overby, *Offshoring: Preparing for India's Proposed Privacy Rules*, PC Advisor. (2011), at http://www.pcadvisor.co.uk/news/security/3279814/offshoring-preparing-for-indias-proposed-privacy-rules/ (last visited on 13 May 2012). The India-proposed standard is stricter than the US or even the EU standards. Not surprisingly, Google and some other US companies object to the entire law including the informed consent clause. Google started a political campaign saying that the law is "harassing," "grossly harmful" or "ethnically objectionable." See Rama Lakshmi, *India Data Privacy Rules May Be Too Strict for Some U.S. Companies*, The Washington Post. (2011), at http://www.washingtonpost.com/business/india-data-privacy-rules-may-be-too-strict-for-some-us-companies/2011/05/18/AF9QJc8G_story.html (last visited on 23 May 2012). Despite economic and political pressure from Google, the law minister declared that "The right to privacy would include the right to confidentiality of communication, confidentiality of private or family life, protection of one's honour and good name, protection from search, detention or exposure of lawful communication between individuals, privacy from surveillance, confidentiality of banking, financial, medical and legal information, protection from identity theft of various kinds, protection of use of a person's photographs, fingerprints, DNA samples and other samples taken at police stations and other places and protection of data relating to individual." Abantika Ghosh, *Right to Privacy May Become Fundamental Right*, The Times of India. (2011), at http://articles.timesofindia.indiatimes.com/2011-06-04/india/29620422_1_privacy-law-ministry-confidentiality (last visited on 4 June 2012) at ¶ 4.

[155] The US refuses to follow EU privacy standards and thus attempts to undermine such efforts. The US supports the less effective APEC approach.

standards?[156] Will the SA approach meet adequate level EU standards for data transfers?

Reinhardt Buys declared that "[T]he longer the Bill's enactment is postponed, the longer the gross violation of data privacy in South Africa will continue. SA already has wholesale commercialization of personal information and databases."[157]

6.6 Protection of Personal Information Bill Provisions

The proposed *Protection of Personal Information Bill*[158] defines personal information[159] and provides a response to national concerns, legal advocacy, and the need to help SA meet international DPSIP standards. The Preamble declares that "the State must respect, protect, promote and fulfill the rights in the Bill of Rights."[160]

The *Protection of Personal Information Bill* attempts to make the constitutional privacy right effective operationally while balancing privacy with other rights. Such rights include the right to access information and allow the free flow of information. The Bill regulates the responsible processing of personal

---

[156] See Anneliese Roos, The Law of Data (Privacy) Protection: A Comparative and Theoretical Study (2003) (LL.D. thesis, UNISA). Chpt 7 ¶ 2.4.2.2.

[157] Leon Englebrecht, *Data Privacy Bill in Suspended Animation*. (2008, February 20), at http://www.itweb.co.za/sections/business/2008/0802201052.asp?S=Legal%20View&A=LEG&O=FRGN (last visited on 21 February 2012), ¶¶ 9-10.

[158] Protection of Personal Information Bill B 9 of 2009 (2009) .(SA)

[159] *Id.* at ¶¶ 7 – 8. The definition includes: "information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to (a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person; (b) information relating to the education or the medical, financial, criminal or employment history of the person; (c) any identifying number, symbol, e-mail address, physical address, telephone number or other particular assignment to the person; (d) the blood type or any other biometric information of the person; (e) the personal opinions, views or preferences of the person; (f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence; (g) the views or opinions of another individual about the person; and (h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.

[160] *Id.* at Preamble.

information to meet EU and related international standards. Data subjects are granted rights and remedies for violations of the data protection standards. Minimum data protection standards are established. The Bill sets compulsory and voluntary standards to enforce, fulfill, and promote DPSIP legal requirements. The Bill establishes an information protection regulator.[161]

The Bill applies to the processing of personal information in SA through automated and non-automated means by private and public bodies.[162] Consistent with other DPSIP approaches noted in the current study, the SA Bill provides for exclusions to the processing of personal information. Some of the SA exclusions make legal and operational sense, like excluding personal and household processing and judicial functions.[163] Based on the negative effect of exclusions in AU, CA, the UK, and the US, and modern technology developments like data mining and RFID, the remaining exclusions are potentially problematic.[164] Checks and balances are needed to discover, prevent, and provide remedies when the government and business organizations abuse their power and manipulate the system.[165]

The Bill establishes eight personal privacy principles. The list includes accountability, processing limitations, purpose specification, further processing limitations, information quality, openness, security safeguards, and data subject participation.[166]

---

[161] *Id.* at Chapter 1, ¶ 2(1).
[162] *Id.* at Chapter 2, ¶ 3.
[163] *Id.* at Chapter 2, ¶ 4(a)(f).
[164] *Id.* at Chapter 2 ¶ 4: *(b)* that has been de-identified to the extent that it cannot be re-identified again; *(c)* by or on behalf of the State and—(i) which involves national security, defence or public safety; or (ii) the purpose of which is the prevention, investigation or proof of offences, the prosecution of offenders or the execution of sentences or security measures, to the extent that adequate safeguards have been established in specific legislation for the protection of such personal information; *(d)* for exclusively journalistic purposes by responsible parties who are subject to, by virtue of office, employment or profession, a code of ethics that provides adequate safeguards for the protection of personal information; *(e)* by Cabinet and its committees, the Executive Council of a province and a Municipal Council of a municipality; *(g)* that has been exempted from the application of the information protection principles in terms of section 34.
[165] See Chapter 2 s 4 of the current thesis.
[166] *Id.* at Chapter 3, part A.

Principle 1: Accountability. All private and public organizations that process personal information must have a responsible person who gives effect to the Bill's principles and certifies compliance.[167]

Principle 2: Processing limitations. Such a principle requires the processing of personal information to be lawful and reasonable. Reasonable is defined as adequate, not excessive, and relevant. Data subject consent and the right to object are established.[168] This section is silent on the issue of informed consent or the opt-in or opt-out issues. The Bill allows for unknown parties to override the consent requirement.[169]

Principle 3: Purpose specification. This principle provides a generally accepted international standard. Data collection must be for a specific

---

[167] *Id.* at Chapter 3, part A, ¶ 7.

[168] *Id.* at Chapter 3, part A, ¶¶ 8, 9, 10 (1)(a).

[169] *Id.* at Chapter 3, part A, ¶¶ 10, 11. Consent, justification and objection 10**.** (1) Personal information may only be processed if— *(b)* processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is party; *(c)* processing complies with an obligation imposed by law on the responsible party; *(d)* processing protects a legitimate interest of the data subject; *(e)* processing is necessary for the proper performance of a public law duty by a public body; or *(f)* processing is necessary for pursuing the legitimate interests of the responsible party or of a third party to whom the information is supplied. (2) A data subject may object, at any time, on reasonable grounds relating to his, her or its particular situation, in the prescribed manner, to the processing of personal information in terms of subsection (1)*(d)* to *(f)*, unless otherwise provided for in national legislation. (3) If a data subject has objected to the processing of personal information in terms of subsection (2), the responsible party may no longer process the personal information. Collection directly from data subject 11. (1) Personal information must be collected directly from the data subject, except as otherwise provided for in subsection (2). (2) It is not necessary to comply with subsection (1) if—*(a)* the information is contained in a public record or has deliberately been made public by the data subject; *(b)* the data subject has consented to the collection of the information from another source; *(c)* collection of the information from another source would not prejudice a legitimate interest of the data subject; *(d)* collection of the information from another source is necessary—(i) to avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution and punishment of offences; (ii) to enforce a law imposing a pecuniary penalty; (iii) to enforce legislation concerning the collection of revenue as defined in section 1 of the South African Revenue Service Act, 1997 (Act No. 34 of 1997); (iv) for the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated; (v) in the legitimate interests of national security; or (vi) to maintain the legitimate interests of the responsible party or of a third party to whom the information is supplied; *(e)* compliance would prejudice a lawful purpose of the collection; or *(f)* compliance is not reasonably practicable in the circumstances of the particular case.

[169] *Id.* at Chapter 3, part A, ¶ 12.

purpose that is legal as well as clearly defined and stated.[170] The data can be retained only for a limited time as defined by law, contract, or data subject's permission.[171] The exact length of time is not clearly defined and is subject to debate as noted in the US.[172]

Principle 4: Further Process Limitation. This principle defines the standards by which the identified responsible person must consider and review data process limitations.[173] The provision also includes an undefined standard for data subject consent, potentially troublesome problems related to public records, public health, public safety, and research that is historical or statistical.[174] The relevant DPSIP issue is who makes such decisions and what are the checks and balances against abuse.

Principle 5: Information Quality. This principle states that the responsible person is obligated to insure that the personal information is accurate, complete, not misleading, and updated.[175] This principle is fairly consistent with international standards. The Bill also provides some major DPSIP legal loopholes. The standards only need to be met when they are necessary. The reasonable person needs to take only the steps that are reasonably practical.[176] The standards do not operationally define key terms. While such an approach may be a full employment act[177] for attorneys and judges,

---

[170] *Id.* at Chapter 3, part A, ¶ 12.
[171] *Id.* at Chapter 3, part A, ¶ 14.
[172] Sam Diaz, *CNET: Justice Dept. to ask Congress for ISP Data Retention Law*, ZDNet. (2011), at http://www.zdnet.com/blog/btl/cnet-justice-dept-to-ask-congress-for-isp-data-retention-law/43969 (last visited on 25 January 2012).
[173] *Id.* at Chapter 3, part A, s 15 (2). *(a)* the relationship between the purpose of the intended further processing and the purpose for which the information has been collected; *(b)* the nature of the information concerned; *(c)* the consequences of the intended further processing for the data subject; *(d)* the manner in which the information has been collected; and *(e)* any contractual rights and obligations between the parties.
[174] *Id.* at Chapter 3, part A, ¶ 15 (3). See Chapter 2 § 4 of the current thesis.
[175] *Id.* at Chapter 3, part A, ¶ 16.
[176] Ibid.
[177] Such a law will probably create considerable paid work for attorneys and judges. Such a law will create considerable litigation.

business and governmental organizations can maximize the value of manipulating the proposed DPSIP system.[178]

Principle 6: Openness. This principle addresses international standards of transparency based on current—but not evolving—DPSIP standards.[179] As noted above, the efforts of the responsible person only need to be reasonable and practical when notifying data subjects of the data processing.[180] The effort does not confront technological advances (e.g., data mining) that make such standards obsolete.

Principle 7: Security Safeguards. This principle addresses current international security standards. The proposed SA security principle is more definite. A responsible person must take due regard and responsibility for the integrity of data in its control or possession and must meet loss standards that are appropriate, as well as organizationally and reasonably technologically competent to prevent security breaches.[181] The standard reinforces that

---

[178] To be fair, from a political perspective such an approach may be a reasonable starting point. A legislative strategy must be made. Sometimes, something is better than nothing. One can always live to battle another day.

[179] *Id.* at Chapter 3, part A, ¶ 17 (2) (3). *(a)* the information being collected; *(b)* the name and address of the responsible party; *(c)* the purpose for which the information is being collected; *(d)* whether or not the supply of the information by that data subject is voluntary or mandatory; *(e)* the consequences of failure to provide the information; *(f)* any particular law authorising or requiring the collection of the information; and *(g)* any further information, such as the—(i) recipient or category of recipients of the information; (ii) nature or category of the information; and (iii) existence of the right of access to and the right to rectify the information collected, which is necessary, having regard to the specific circumstances in which the information is or is not to be processed, to enable processing in respect of the data subject to be reasonable. (3) The steps referred to in subsection (2) must be taken— *(a)* if the personal information is collected directly from the data subject, before the information is collected, unless the data subject is already aware of the information referred to in that subsection; or *(b)* in any other case, before the information is collected or as soon as reasonably practicable after it has been collected.

[180] Ibid.

[181] *Id.* at Chapter 3, part A, ¶ 18. (a) loss of, damage to or unauthorised destruction of personal information; and (b) unlawful access to or processing of personal information. (2) In order to give effect to subsection (1), the responsible party must take reasonable measures to— (a) identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control; (b) establish and maintain appropriate safeguards against the risks identified; (c) regularly verify that the safeguards are effectively implemented; and (d) ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards. (3) The responsible party must have due regard to generally accepted information security practices and procedures which may apply

personal data is confidential and that any extensions must be defined by contract principles. In keeping with the advancement of breach notification principles started in California in the US, the Bill requires breach notification.[182]

Principle 8: Data subject participation. This principle addresses personal information access and correction.[183] With proper identification a data subject can request verification from a responsible party to determine if the party has relevant personal data about the subject. The processing of the request is free. For a non-excessive fee, the data subject can discover the description of any data subject information held by the responsible party. A fee can be charged to determine if any third party or category of parties has or has had access to the information. Requests must be made within a reasonable time; this requirement may be problematic because a data subject may not have had reasonable notice. The responsible party must release the data in a reasonable format and manner that is generally understandable. Such access is subject to some restraints noted in Chapter 4 of the Bill.[184] Under the current Bill, a data subject may contact the responsible party and request a correction or deletion of personal information held by or under the control of the responsible party that is excessive, inaccurate, incomplete, irrelevant, misleading, no longer authorized under the Bill, obtained unlawfully, or is out of date.[185] When the request is determined as valid, the responsible person must correct, delete, or destroy the information. The data subject must be informed and given credible evidence of any actions taken in response to the request. In such a situation, the responsible party must contact any third parties that were provided the information, when reasonable and practical. No operational criteria are provided by the Bill.

Early international DPSIP legislative efforts identified personal information that was considered sensitive. The principles are still part of the laws in the other

---

to it generally or be required in terms of specific industry or professional rules and regulations.

[182] See Chapter 8 of the current thesis and Chapter 3, part A, ¶ 21.
[183] *Id.* at Chapter 3, part A, ¶¶ 22 & 23.
[184] *Id.* at Chapter 3, part A, ¶ 22.
[185] *Id.* at Chapter 3, part A, ¶ 23.

countries noted in this study. Current efforts in CA and the EU have advanced the focus, given more recent technological advances like data mining.[186] The SA Bill prohibits processing of data subject information related to children without parental consent, criminal behavior, ethnic origin, health, philosophical beliefs, political opinions, race, religious beliefs, sexual lifestyle, or trade union membership. An exception is provided for governmental agencies or organizations that maintain that they have a lawful purpose to have such data.[187]

The SA Bill follows the pattern of DPSIP laws in the other study countries by allowing protection exceptions. In SA, the Regulator has the power to grant such exceptions.[188] A set of balancing standards is established that involves a substantial public interest over data subject interests. Such an argument has been made by press organizations in a number of countries. A second standard involves a proclaimed clear benefit to the data subject or a third party that provides a substantial interest that interferes with the privacy of another. Exceptions are allowed for historical, research, or statistical efforts. Under the exceptions, the public interest trumps the protection principles of the Bill. The public interest can reasonably include the criminal justice system, with proper checks and balances, for preventing, detecting, and prosecuting offenses. Exceptions are also allowed for interests that are open to abuse including state security interests and the economic and financial interests of a public body or the State.[189]

The Bill provides a supervision process that is more advanced than the ones in the other countries in the study.[190] A juristic Information Protection Regulator is established.[191] The jurisdiction, independence, and performance

---

[186] See Chapters 3 and 5 of the current study.
[187] *Id.* at Chapter 3, part B, ¶¶ 25-32.
[188] *Id.* at Chapter 4, ¶¶ 33-34.
[189] *Id.* at Chapter 4, ¶ 34.
[190] The one exception is the standards of the US sectoral HIPAA legislation in the US. See Chapter 8 of this work.
[191] *Id.* at Chapter 5, part A ¶ 35.

standards are clearly defined.[192] The regulator does have two masters to serve: the *Protection of Personal Information Bill* and the *Promotion of Access to Information Act*. These purposes may have competing goals and standards. The regulation office includes a full-time chairperson and four part-time ordinary members.[193] The SA President has appointment powers that can be used to stack the regulator; the Parliament can request removal of any of the regulator officers for illness or misconduct.[194] Such powers, without checks and balances, can violate the principle of independence. The Regulator must provide informational reports to Parliament on all investigated matters and present an annual report to the Minister of the Department of Justice and Constitutional Development.[195] The government's Minister is also granted additional powers over the Regulator.[196] Such provisions can impair the stated principle of independence.

The Bill declares a list of regulator duties and powers[197] that is based on problems found in other counties including those in this study. The Bill requires that the regulator must establish and maintain a strategic focus and must respond to changes in DPSIP principles; the regulator must also address potential conflicts with other stakeholder interests, international obligations, and technological changes.[198] However, the provisions require that the regulator must always consider the business and government's interest in the free flow of information.

The Bill requires the appointment of information protection officers in private and public bodies. Specific duties and responsibilities for the officers are

---

192 *Ibid, (a)* has jurisdiction throughout the Republic; *(b)* is independent and is subject only to the Constitution and to the law and must be impartial and perform its functions and exercise its powers without fear, favour or prejudice; and *(c)* must perform its functions and exercise its powers in accordance with this Act and the Promotion of Access to Information Act.

193 *Id.* at ¶ 36.

194 Ibid.

195 *Id.* at ¶ 46.

196 *Id.* at Chapter 12, ¶ 102. *(a)* any matter which this Act requires or permits to be prescribed; *(b)* the monitoring of this Act and the establishment of the Regulator; and *(c)* any other matter which may be necessary for the application of this Act

197 *Id.* at ¶ 43.

198 *Id.* at ¶ 44 (1) (2) (3).

defined.[199] The regulator has the power to issue codes of conduct related to information, classes of information, and practices. The codes can apply to activities in a range of callings, industries, and professions. The regulator has the power to review proposed codes of conduct.[200]

The Bill addresses additional DPSIP principles including unsolicited electronic communications, directories, and automated decision making.[201] The provisions for transnational transfer of personal information require consent or contractual obligation.[202] The transfer standards do not provide any restrictions on where the data is transferred; moreover, the standards do not establish quality control on the processing, and they do not provide any recourse or remedies when violations occur.

In the instant case, the Protection of Personal Information Bill, as proposed, addresses a number of problematic DPSIP issues. The Bill does not address issues related to social networking web sites and the sale of personal information. Companies and individuals who fail to protect data will be legally liable. The original proposal was to include a breach notification requirement and criminal fines, punitive damages, and up to 10 years in prison.[203] The current Bill ignores some key DPSIP protections including privacy by design and independent authority.

6.7 South African Standards and Remedies

To date, the SA judiciary and parliament have failed to respond to established DPSIP legal issues. Sound constitutional protections on privacy have not been operationally established or implemented. Despite decades of international advancements on such issues, SA has struggled with internal

---

[199] *Id.* at Chapter 5, part B ¶¶ 48-49.
[200] *Id.* at Chapter 7, ¶ 57.
[201] *Id.* at Chapter 8.
[202] *Id.* at Chapter 9.
[203] Siyabonga Africa, *Privacy Bill Promises Protection*. (2008, October 8), at http://www.itweb.co.za/sections/internet/2008/0810081040.asp?O=F&A=TELECOMS (last visited on 9 October 2012).

decision-making processes. At present, SA and business interests allow free access to personal information for economic gain and governmental control. Free access to information is the mantra of the power elite. Calls for DPSIP protections have been essentially ignored from a political and judicial perspective.

6.8 South African Implementation System

The SA government has established efforts to help the population become more information technology literate. The government is aware that not all citizens have personal access to computers or the Internet and it has trained community development workers to help assist people with getting acquainted with the Internet. Access for some data purposes is available at multi-purpose community centers and post offices country wide.[204]

None of the DPSIP efforts have been extended to protect the rights of SA citizens under international law. At present, remedy efforts are being explored; however, SA citizens are being exploited without notice or remedy.

6.10 South African Sociolegal Concerns

SA is the most Internet connected country on the African continent. The country is facing the same information privacy, data protection, and security legal problems and issues as AU, CA (one of the ten most connected), EU, UK (one of the ten most connected), and the US (the dominant Internet country).[205]

---

[204] The Center for Democracy and Technology, *Preliminary e-Government Policy, Law and Regulation Survey Report: South Africa* (The Center for Democracy and Technology. 2006).

[205] Caroline B Ncube, Watching the Watcher: Recent Developments in Privacy Regulation and Cyber-Surveillance in South Africa 3 *SCRIPTed – A Journal of Law, Technology & Society* 4, 344 (2006), http://www.law.ed.ac.uk/ahrc/script-ed/vol3-4/ncube.asp (last visited on 23 April 2012).

Research on public concerns regarding data protection and security concerns in SA has occurred over time. A survey conducted in SA revealed that seventy-three percent of those sampled reported concerns about the loss of control over their personal information.[206]

Data protection and security concerns in SA showed that organizational leaders in SA ranked amongst the world's most informed about the need for DPSIP protection and security. Sixty-seven percent reported that such concerns were critical, yet twenty-four percent expressed concerns about the effectiveness of current efforts. The majority noted that governmental policy was motivated by business interests. Forty-two percent of SA respondents reported that initiatives were directed by senior management, compared with twenty percent for the global respondents. Seventy percent of the boards of directors of SA corporations did not receive quarterly reports on DPSIP issues from senior management.[207]

A 2004 survey showed that of the top 100 South African websites, a total of ninety-six percent collected personal information. The same percentage collected personal identifying information, while eighty-four percent reported non-identifying data. The percentages were in line with international standards. Only sixty-eight percent of SA websites posted any type of privacy policy, while ninety-eight percent of the international sites did. Of the few sites that offered some type of user choice, seventeen percent used opt-in while eighty-three percent took the more invasive opt-out option. Fifty-eight percent of the international sample used opt-out options. Of the sites that

---

[206] Jaco Van Der Walt, *Trust and Privacy are the Cornerstones of Successful Relationships between Consumers and Business*. (2003, March 13), http://www.ey.com/GLOBAL/content.nsf/South_Africa/15_May_03_Trust_And_ Privacy (last visited on 5 June 2012).

[207] Ernst & Young, *South African CEOs are Getting More Hands-On with Information Security Issues*, Tech News (2004, November), http://cbr.co.za/article.aspx?pklArticleId=3290&pklCategoryId=378 (last visited on 22 March 2012).

collected personal information, the security procedures in place on those sites were less than international standards.[208]

Table 6.1 Security Claims

Security Claim	South Africa	International
Sites claimed to provide transmission data security from user to the site	43%	60%
Sites claimed to offer site security once data is collected	31%	72%

The research conducted in SA revealed that the majority of people wanted DPSIP legal protections. The data also showed the business organizations in the country were behaving below international standards. The lack of governmental DPSIP laws and regulatory agencies compounded the problem.

Politicians and jurists can and certainly do argue and maneuver around DPSIP issues. Businesses and corporations can and do corrupt the process.[209] The above research shows that the majority of SA citizens want strong DPSIP legislation and regulation.

6.10 South African Critique

Chapter two of the SA Constitution[210] establishes a privacy right that no other Constitution in the study provides. The extension of such rights to juristic persons (corporations) is potentially troublesome given the immense power of national and global corporations. The US has been classified as a corporate

[208] Ibid.

[209] See: Jeffrey D. Clements, *Corporations Are Not People: Why They Have More Rights Than You and What You Can Do About it* (Berrett-Koehler Publishers, Inc ed. 2012). Thom Hartmann, *Unequal Protection: The Rise of Corporate Dominance and the Theft of Human Rights* (Rodale ed. 2002). Robert G. Kaiser, *So Damn Much Money: The Triumph of Lobbying and the Corrosion of American Government*,(Alfred A. Knopf ed. 2009). Lawrence Lessig, *Republic, Lost: How Money Corrupts Congress - and a Plan to Stop It* (Twelve - Hachette Hook Group ed. 2011).

[210] Constitution of the Republic of South Africa 1966 ¶ 2 (1996). (SA)

republic.[211] Corporations can sue for defamation, with no actual damages and privacy violations. The same protections are not often allowed for natural persons. The SA provisions counter the political theory that governments are formed to protect the rights of men and women.

Studies in SA have shown that considerable citizen concerns exist regarding DPSIP issues.[212] The government has done little to execute the will of the people or protect its citizens from the unintended consequences of not properly addressing DPSIP issues. After years of study and review, SA remains the only country in the study that has officially failed to legally respond to DPSIP concerns that its citizens have raised. The US, which has a rather schizoid approach, has at least provided some limited response. To date, the SA approach fails to meet the standards set by AU, CA, UK, and the EU. Despite the recalcitrance of the SA judiciary to establish common law protections and remedies consistent with its international legal peers, despite the resistance of the business community – especially powerful international corporations to any checks and balances on their unlimited greed to make profit on everything – and despite a population that is preoccupied with resolving historic power issues and building a sound modern democracy, a group of dedicated, educated, and socially responsible citizens and professionals has made considerable and somewhat effective efforts to address one of the major issues of the day.

6.11 Summary of South African Literature and Issues Reviewed

The intent of this thesis is to conduct a comparative analysis of DPSIP responses in five different nations. Part of the comparison uses a benchmark approach of key issues. The issues include legal support of DPSIP protections, legal support of corporate privacy and data protection standards, information privacy data protection and security declarations, the use of

---

[211] James K. Galbraith, *Our New Corporate Republic*, Boston Globe. (2001), at http://www.commondreams.org/views01/0107-01.htm (last visited on 20 February 2012).

[212] See Chapter 2 of this work.

regulatory agencies, sectoral legislation, and data controllers. The benchmark standards also include data processor requirements, data subjects, data security destruction, cross-border data flow, exemptions and exceptions, and the current stage of the approach based on evolutionary stages. The following table presents the summary based on the benchmark model.

Table 6.2 Comparative Model of South African Legal Support of DPSIP Models

ISSUE DESCRIPTION	**SA CURRENT RESPONSE**
CM.1: Legal Support of DPSIP Protections	
Signatory, Adheres, and/or Complies with International Human Rights Standards	(See Appendix A)
Signatory, Adheres, and/or Complies with EU DPSIP Standards	No
Signatory, Adheres, and/or Complies with APEC DPSIP Standards	No
Constitutional Law	Yes
Legislative Efforts	Proposed
Common Law	Limited
Province /State Constitutional Law	No
Province / State Legislative Efforts	No
Province /State Common Law	No

CM.2: Legal Support of Corporate Privacy and Data Property Protection Issues	**SA CURRENT RESPONSE**
Copyright Protections	Yes
Database Protection	Yes
Patient Protections	Yes
Service Mark Protections	Yes
Trade Mark Protections	Yes
Trade Secret Protections	Yes
Privacy Impact Audit Required Before Use	No
Privacy Impact Audit Required Before Government Protections Granted	No

Checks and Balances on Corporate Collection, Use, and Transfer of Individual DPSIP Data	No

CM.3: Information Privacy – Data Protection and Security Declarations	**SA CURRENT PROPOSED RESPONSE**
Definitions Provided	Yes
Personal and Sensitive Data Defined	Yes
Definitions Effectively Address Advanced Data Mining Technologies	No
All Holders and Users Held Accountable	No

CM.4: Regulatory Agency	**SA CURRENT PROPOSED RESPONSE**
Independent of Legislative and Executive Branches	Questionable – approach is open to abuse with no checks or balances
Administrative Power	Yes
Investigative Power	Yes
Regulatory Powers	Yes
Education Function	Yes
Enforcement Powers	Yes
Structure	Yes
Responsibilities Defined	Yes
Accountability	Yes
Governmental Chief Privacy Officer/ Commissioner Required	Yes
Governmental Privacy Audits Required as Part of Legislation Passage	Yes
Business Chief Privacy Officer/ Commissioner Required	Yes
Employees are Personally Liable for Violations	No
Business Privacy Audits Required	No
Agency Educational Function	Yes

CM.5: Sectoral DPSIP Legislation	**SA CURRENT PROPOSED RESPONSE**
Credit Reporting Agencies	Yes
Criminal Justice Record Restrictions	Yes

Health Information	Yes
Health Information Exceptions	Yes
Electronic Medical/Health Record Controls	Unclear

CM.6: Data Controllers	**SA CURRENT PROPOSED RESPONSE**
Notice Required	Yes
Opt-in	Unclear
Opt-Out	Unclear
Must Be Lawful and Fair	Yes
System Access Controls	Yes
Data Quality and Integrity	Yes
Accurate	Yes
Complete	Yes
Up to Date	Yes
Limited to Needed Data	In theory
Relevant	Yes
Not Misleading	Yes
Data Retention Limitation	Limited
Data Transfer Controls	Limited
Openness on Information Held	Limited
Breach Disclosures Required	No
Breach Penalties	No

CM.7: Data Processor Requirements	**SA CURRENT PROPOSED RESPONSE**
Informed Consent Required	Unclear
Rationale is Provided	No
Fair Processing	No
Legal Processing	Yes
General Data	No
Sensitive Data	Yes
Accuracy	Yes
Timely	Yes
Duration of Record Keeping Controls	No

CM.8: Data Subjects	**SA CURRENT PROPOSED RESPONSE**
Ownership by the Subject	No
Control Over Access	Limited
Alter, Amend, Correct, and Delete Errors	Yes
Notification Requirement	No

CM.9: Data Security and Destruction	**SA CURRENT PROPOSED RESPONSE**
Security Must be State of the Art	No
Technology Use – Cost of Implementation Not a Defense	No
Tracking	No
Safeguards Required	No
Protects from Alteration	No
Protects Against Disclosure	No
Protects Misuse	No
Protects Against Unauthorized Internal and External Access	No
Unauthorized Access Penalties	No
Timely Notice of Breaches	No
Strong Remedies Provided	No

CM.10: Cross-Border Data Flow	**SA CURRENT PROPOSED RESPONSE**
Individual Informed Consent Required	Yes
Transfer Source Is Accountable	No
Outsource Service Controls	No

CM.11: Exemptions and Exceptions	**SA CURRENT PROPOSED RESPONSE**
Only Permitted Where There Is a Compelling Justification	No
Checks and Balances – Court Order Required	No
Government Agencies	Yes
Intelligence and Defense	Yes
Police Actions	Yes
Small Business Exemption	No

CM.12 DPSIP Evolutional Stages	**SA CURRENT PROPOSED RESPONSE**
DPSIP.0 Limited DPSIP legal Issues	Yes
DPSIP.1.0 Establishes PII; does not fully address security issues; focus on limited legal consent and notice.	Yes
DPISP.2.0 Accepts PII standards; does not fully address security issues; focus on a legally based harm-based analysis.	No
DPSIP.3.0 PII and non-PII data	No

fused; privacy, data protection and security issues are interrelated; legal audits, checks, and balances needed for all personal information stakeholders. New technologies are required to pass privacy audits (e.g., RFID, Internet of Things) and require use of privacy enhancing technologies in all new IP approvals.	

SA has established an advanced constitutional privacy protection clause; however, enabling legislation has yet to be established.[213] The courts have been resistant to establishing DPSIP standards within its Roman-Dutch common law tradition. The focus on establishing DPSIP protections has been left to the legislature. Some sector legislation has been enacted that involves selective DPSIP issues. For more than a decade, the legislative process has been involved in attempting the establishment of a comprehensive DPSIP legal policy, which is needed to meet the data protection demands of the public and the DPSIP legal demands of its major trading partners.

Chapter Seven explores the UK approach to DPSIP legal issues. As a member of the EU, it is accountable to the EU data protection standards. The courts and parliament have established some DPSIP principles; however, the standards do not fully embrace the EU standards. Although some practices have been established, there are actual and potential complications in the UK approach.

[213] A similar legislative problem exists in the US. Some legislators follow the Constitution and the basic principles of human rights and the rule of law. Other legislators follow the dictates and money of the corporate republic.

CHAPTER SEVEN: DATA PROTECTION AND SECURITY LAW:

UNITED KINGDOM LEGAL STANDARDS

> *Parliament has seldom been prepared to legislate specifically to ensure rights to privacy, leaving it to the courts to develop common law and equitable principles. The courts, whilst not altogether shirking this responsibility, have proceeded with extreme, and some would say undue, caution.* David Bainbridge and Graham Pearce[1]

7.0 Overview

The UK is a party to the Council of Europe and a member of the EU. Of the nations addressed in the current study, the UK is the only one that has an obligation to pass legislation conforming with the EU approach to DPSIP legal standards. The UK has instituted some innovative DPSIP approaches. In specified circumstances, EU laws can take precedence over conflicting UK laws.[2] As of August 1, 2010, the EU instructed the UK to strengthen DPSIP laws or face European Court of Justice action.[3] The government has never fully committed to protecting data. Nonetheless, the UK has one of the largest DNA databases in the world. The data base includes eight percent of the entire population of the country. As of 2009, Jill Lawless[4] reported that data from over five million people has been collected. This collection includes DNA from everyone arrested for any reason; moreover, the data is retained no

---

1 David Bainbridge & Graham Pearce, Tilting at Windmills - Has the New Data Protection Law Failed to Make a Significant Contribution to Rights of Privacy, 2000 *Journal of Information, Law and Technology* 2, (2000).

2 See *European Communities Act 1972 (c. 68)* (1972). (UK)

3 Chris Priestly, *United Kingdom: UK Told to Get Tougher on Data Protection Law* Mondaq: Intellectual Property. (2010), at http://www.mondaq.com/article.asp?articleid=106238&email_access=on (last visited on 2 August 2012).

4 Jill Lawless, *Does DNA Database Unfairly Brand the Innocent?*, San Francisco Chronicle(2009), at http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2009/09/12/MNDK19L6BK.DTL.

matter the result of the arrest (e.g., if the charges are eventually dropped or the person is acquitted). When the European Court of Human Rights (ECHR) ruled that this blanket policy was indiscriminate and should be stopped, the UK, in a passive-aggressive response, deleted some records; however, as Lawless[5] reported, the UK also stated that it would keep the records of those cleared of serious crimes for up to twelve years. Alec Jeffreys, the British scientist that discovered the DNA identification factor, criticized the UK response as non-compliant with the spirit of the law.[6]

The UK chapter begins with presenting background on the country. The analysis continues with an examination of the UK Constitutional declarations, UK legislation, and UK case law. The research then focuses on UK constituent governmental declarations, legislation, and case law. An analysis of the UK standards, remedies, and implementation system is reviewed. UK sociolegal concerns are presented. A critique of the UK approach is then addressed. A summary of the UK literature and issues, using the thesis comparative model of the current legal support, is then reviewed and presented.

7.1 Background

The UK is a multi-cultural nation that has historically headed the Commonwealth nations.[7] The majority of the population is of Anglo-Saxon descent, including British, Irish, and Scottish. Based on historic rights to commonwealth nations, additional ethnic groups include West Indians and South Asians.

---

5 *Id.*

6 *Id.*

7 United Kingdom Government, *Government, Citizens and Rights*. (2010), at http://www.direct.gov.uk/en/Governmentcitizensandrights/index.htm (last visited on 5 August 2012). Site contains reference data for this section.

The official name of the UK is the United Kingdom of Great Britain[8] and Northern Ireland.[9] The country is a constitutional monarchy with an unwritten constitution based on common law, practices, statutes, and traditional rights. The UK has the third-largest population in the EU. The executive branch includes the head of state (ie, the monarch) and the head of government (i.e., the prime minister).[10]

The UK legislative structure[11] includes the Parliament of the United Kingdom of Great Britain[12] and Northern Ireland.[13] The Parliament includes the House of Lords,[14] House of Commons,[15] and the monarch. The *Scotland Act of 1998*[16] created the current Scottish Parliament. This body is democratically elected.[17] In 945, the King of Wales codified Welch law. The current National Assembly of Wales has sixty members[18] elected to four year terms. The

---

8 Includes England, Scotland, and Wales. England has been a country since the 10th Century of the common era. In 1707, Scotland formally joined with England and Wales. Starting in 1284 and ending in 1536, Wales joined with England.

9 The union with Ireland occurred in 1801; the Anglo-Irish treaty of 1921 partitioned six Northern Counties into North Ireland.

10 United Kingdom Government, *The Official Site of the Prime Minister's Office*. (2010), at http://www.number10.gov.uk/ (last visited on 5 August 2012).

11 This is not a traditional national legislature; however, it can obligate the courts to follow its statutes. The body includes the House of Commons (651 members) and the House of Lords (26 Bishops, 92 hereditary peers, and 574 life peers). The Sovereign functions as the third part of the legislature. United Kingdom Government, *Parliament*. (2010), at http://www.parliament.uk/ (last visited on 5 August 2012). See

12 Also known as British or Westminster Parliament.

13 The devolved Northern Irish Assembly is unicameral. The 108 Members of the Legislative Assembly are elected in democratic elections. The assembly was created by a 1997 referendum; it was established in 1999.

14 Members are appointed by the monarch with advice from the Prime Minister. The House of Lords includes twenty-six senior bishops of the Church of England and 669 Lords Temporal.

15 Composed of 659 members of Parliament who are democratically elected by constituencies. England has 529 members, Scotland has seventy-two, Northern Ireland has eighteen, and Wales has forty members.

16 The 129 members are democratically elected and are referred to as Members of the Scottish Parliament. The Parliament is unicameral and was created by a 1997 referendum; it was established in 1999. See *Scotland Act 1998 Chapter 46* (1998). (UK)

17 Seventy-three are elected by plurality based on districts and fifty-six by eight regions.

18 Includes forty members elected by plurality and twenty representing five regional sectors.

Government of Wales Act of 2006[19] granted additional powers to the Assembly. Acts can be vetoed by the Parliament of the UK.

DPSIP law in the UK is based on statutory enactments, English common law (judicial decisions), EU legislation,[20] and international treaties. The common law tradition builds on Roman law and current EU actions.

Historically, the highest court of appeal was the House of Lords. The monarch appointed the Lords of Appeal in Ordinary for life. Under the Constitutional Reform Act of 2005, a Supreme Court was established. In October of 2009, the UK opened the Supreme Court[21] with the sitting Law Lords becoming the Court's Justices and the Senior Law Lord becoming the first President. England and Wales have a combined judicial system. Scotland[22] and Northern Ireland[23] each have their own judicial systems based on a common law tradition.

The UK has established a range of civil liberty, civil rights, human rights, and consumer protection standards that relate to DPSIP legal standards. Some standards are proactive, whereas others react to EU standards.

The history of any current constitutional democracy reveals pendulum shifts from supporting civil liberty, civil rights, and human rights priorities to periodically suppressing them in a cyclical pattern. The UK is no exception. The signing of the 1215 Magna Carta remains one of the most important documents in human history. In 1998, the UK government passed a *Human*

---

19 *Government of Wales Act 2006 Chapter 32* (2006). (UK)

20 Includes decisions, directives, and regulations.

21 United Kingdom Government, *The Supreme Court*. (2010), at http://www.supremecourt.gov.uk/index.html (last visited on 5 August 2012).

22 Includes the Scotland's Court of Session and Court of the Justiciary.

23 The supreme courts of England, Northern Ireland, and Wales include Courts of Appeal, the High Courts of Justice, and the Crown Courts.

Rights Act[24] that recognizes rights and freedoms, liberty and security, fair trials, and privacy. The UK is also a *European Convention on Human Rights* signatory.[25]

The UK has established a number of consumer protection acts.[26] As a member of the EU, the UK is mandated to comply with a range of consumer protection directives[27] and determinations of the European Commissioner for Consumer Protection.

7.2 United Kingdom Constitutional Declarations

Given that the UK does not have a written constitution, no clearly established constitutional declaration exists. However, in the UK legal tradition, laws and cases does illustrate a declaration of basic constitutional standards.

7.3 United Kingdom Legislation

The UK DPSIP legal standards are heavily influenced by the findings of the Younger Committee on privacy. The report explains that new electronic, technical, and visual technology is creating imminent and increasing privacy threats. A range of organizations and people, for diverse purposes, are creating "new and menacing" privacy threats.[28]

---

[24] United Kingdom, *Human Rights Act 1998: 1998 Chapter 42*. (1998a), at http://www.opsi.gov.uk/acts/acts1998/ukpga_19980042_en_1 (last visited on 5 June 2012). (UK)

[25] Council of Europe, *Convention for the Protection of Human Rights and Fundamental Freedoms*. (2009), at http://conventions.coe.int/treaty/en/Treaties/Html/005.htm (last visited on 5 August 2012).

[26] The list includes the *Misrepresentations Act of 1967, Consumer Credit Act of 1974, Unfair Contract Terms Act of 1977, Sale of Goods Act of 1979, Consumer Protection Act of 1987, Unfair Terms in Consumer Contracts Regulations of 1999, Consumer Protection (Distance Selling) Regulations of 2000, and Electronic Commerce Regulations of 2002.* The Act establishes a strict liability standard for liability. (UK)

[27] Includes the Unfair Commercial Practices Directive and Directives on Unfair Contract Terms (93/13/EC).

[28] Kenneth Younger, *Report of the Committee on Privacy, Chairman: The Right Hon Kenneth Younger* (Home Office. 1972, July). at 8.

Traditionally, no general privacy right existed in the legal history of the UK. However, in 1984, the government passed the first UK Data Protection Act. The Act regulated the processing of personal information/data, including both sensitive and non-sensitive data. The Act identified some data that was considered sensitive data at the time. While data mining and technological advancements have superseded the approach, the issues remain relevant.[29]

With time, the pattern changed to wider applications of DPSIP principles. Examples include the enactment of the Human Rights Act of 1998 (HRA),[30] the Data Protection Act of 1998 (DPA),[31] and the 2000 Regulation of Investigatory Powers Act (RIPA).[32]

7.3.1 Human Rights Act of 1998

On 2 October 2000, the Human Rights Act went into effect. The Act was in response to the European Convention on Human Rights; in fact, the legislation integrated the majority of the European Convention on Human Rights into UK law. Part One, Article Eight addresses the "Right to respect for private and family life and correspondence."[33] The Act

---

29 United Kingdom Government, *The UK Data Protection Act of 1998*. (1998) (UK), at http://www.hmso.gov.uk/acts/acts1984/1984035.htm (last visited on 17 May 2012). The scheme included alleged or actual offense commission, criminal proceedings, ethnic or racial identity, membership in a trade union, mental or physical condition or health, political opinions, religious or other beliefs, and sexual lifestyle.

30 *Human Rights Act 1998: 1998 Chapter 42*. (1998a), at http://www.opsi.gov.uk/acts/acts1998/ukpga_19980042_en_1 (last visited on 5 June 2012). (UK)

31 *Data Protection Act 1998: 1998 Chapter 29*. (1998b), at http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1 (last visited on 5 June 2012). (UK)

32 *Regulation of Investigatory Powers Act 2000: 2000 Chapter 23*. (2000), at http://www.opsi.gov.uk/acts/acts2000/ukpga_20000023_en_1.htm (last visited on 5 June 2012). (UK)

33 *Human Rights Act 1998. § 8.* (UK) Sect 1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2 There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

prohibits the government from interfering with these rights; however, it includes some exceptions.

As with almost all legislation in the area of DPSIP, the Act provided exceptions which can be very broad, subject to interpretation, and open to questionable judgments. In particular, the meaning of security, safety, economic well being, crime prevention, health, morals, and the rights of others in any given circumstance is broad and open to interpretation. Depending on the interpretation of the exceptions, the stated privacy rights can be voided. The exception clause was consistent with a proportionality test. The Act was limited to actions by public authorities – "It is unlawful for a public authority to act in a way which is incompatible with an EU Convention right."[34] The Act did not apply to business organizations and did not prohibit government from supporting business violations. Thus, the government can use businesses to manage data that would be illegal if the government performed the same task.

The Act required that UK courts and tribunals read and full give effect to the European Convention on Human Rights to all primary and subordinate legislation. The Courts could not render decisions that would violate Convention principles. Courts and tribunals were included in the definition of public authorities and thus must apply the principles of the Act in all legal actions, including interpreting the common law.[35]

7.3.2 Data Protection Act of 1998

The UK addressed data protection issues reluctantly. The first data protection law was passed in 1970 in the German state of Hesse. In the same decade, data controllers in Denmark, France, Germany, and Sweden were also licensed. In 1981, the Council of Europe passed a convention requiring

---

[34] *Id.* at § 6.1.
[35] *Id.* at § 6(3)(a).

member state compliance.[36] In response, the UK passed the 1984 Data Protection Act, which minimally met the Council standards. The 1998 law built on and repealed the 1984 Data Protection Act, which addressed some automated data processing of personal data by any data controller. The focus in this Act shifted from repairing the damages caused by data processing violations to preventing data processing violations.[37]

The 1998 Data Protection Act applies to public and private organizations and includes data controllers, data processors, and data subjects. The Act is intended to comply with the Council of Europe mutual assistance provisions.[38]

The Act required the establishment of a Data Protection Commissioner, which later became the Information Commissioner's Office (ICO).[39] Although the act requires explicit data subject consent, such consent need not be informed,[40] and it does not require breach notification. Moreover, such consent has a number of exemptions including data related to employment, ethnic monitoring, legal proceedings, medical purposes, vital interests, and data in the public domain.[41] The ICO must seek court[42] approval to enter and inspect premises for data-relevant purposes. The ICO has the power to issue enforcement notices, provide educational resources, and encourage the development of codes of best practices. The act further establishes a Data Protection Tribunal to hear appeals of ICO Rulings.

---

36 Council of Europe, *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data: Strasbourg, 28.I.1981*. (1981), at http://conventions.coe.int/Treaty/EN/Treaties/Html/108.htm (last visited on 15 January 2012).

37 The Act provides a framework with the expectation that statutory instruments would follow. The Act consists of seventy-five sections and sixteen schedules.

38 Signatory states must cooperate with one another in relevant laws and judicial actions.

39 The 1984 act used the term Data Protection Registrar. The current term is Information Commissioner's Office (ICO).

40 See Art 2(h) and § 3, ¶ 1.

41 See §§ 3, ¶¶ 2(1), 3(a), 4, 7, 8(1), 9(1).

42 Circuit judge or a sheriff if the issue is in Scotland.

An independent agency is in a better position to address DPSIP standards and innovation than the US approach of placing the responsibility on the individual and industry self-regulations.[43]

Section One, Part One of the 1998 Data Protection Act defines processing of data as "obtaining, recording, or holding the information or data or carrying out any operation or set of operations on the information or data."[44] Personal data refers to data that could identify any living person. The law defines the nature of sensitive data as racial or ethnic, political, religious, concerning union membership, medical conditions, sexual life, legal offense or allegations, or court proceedings.[45]

Part Two of the act provided for legal access to personal data, a right for data corrections, prevention of processing, compensation for failure to comply with certain provisions of the act, and rectification of inaccurate data.[46] Under the Act, individuals have a legal right to personal data that is held about them. Individuals could legally block, erase, and rectify inaccurate data. Individuals could also legally block the processing of certain types of data.

Part Three required that organizations that collect, hold, or transfer data must have a data controller; this controller registers data-processing activities with the ICO.[47] Section Four, Part Four clearly requires that data controllers enforce and follow all data protection and information privacy principles[48] in the Act in a fair and lawful manner.

---

[43] See Chapter 8 § 8.1

[44] *Data Protection Act 1998,* § 1.1 (UK) 1 March 2000, was the effective date.

[45] See Part 1 §2.

[46] See Part 2 §§7-15.

[47] See Part 3 §§17-26. The latest version of the SA POPI rejected this standard.

[48] The eight privacy principles include the following: “personal data being processed fairly and lawfully; shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes; shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed; shall be accurate and, where necessary, kept up to date; data processed for any purpose or purposes shall not be

For data processing to be lawful, the data subject must give consent freely. In contrast, under Canadian law, Article Two Section H consent was defined as "any freely given specific and informed indication of (the data subject's) wishes by which the data subject signifies his agreement to personal data relating to him being processed."[49]

In 2008, the House of Lords passed an amendment that made negligent and deliberate loss of data a criminal offense, subject to a punishment of up to two years in jail. Lord Erroll stated that "Data controllers need to wake up to the importance of personal data, whether in the public or the private sector."[50]

The 2008 amendment, which covered most non-governmental data processors, required processors to pay a £ 35 annual notification filing costs to the ICO. This Act requires that the data controller post notice of several factors.[51]

---

kept for longer than is necessary for that purpose or those purposes; shall be processed in accordance with the rights of data subjects under this Act; appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data; shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data." United Kingdom, *Data Protection Act 1998: 1998 Chapter 29*. (1998), Schedule 1, Part 1, at http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1 (last visited on 5 June 2012).

[49] Canadian Federal Government, *Personal Information Protection and Electronic Document Act*. (2000), at http://laws.justice.gc.ca/en/showtdm/cs/P-8.6 (last visited on 1 November 2012), Art. 2, Sec. H. The notice must include "his name and address, nominated representative, description of the personal data being or to be processed, categories of data subject, description of the purpose(s) of the processing, any recipients for disclosure, and names any non-European Economic Area (EEA) involved in any transfer."

[50] Tom Young, *Lose Data and You Go To Jail*. (2008, May 8), at http://www.computing.co.uk/computing/news/2216073/lose-jail-3989942 (last visited on 10 May 2012), at 4.

[51] United Kingdom Government, *The UK Data Protection Act of 1998*. ch. 29. Part III § 16 (1998), at http://www.hmso.gov.uk/acts/acts1984/1984035.htm (last visited on 17 May 2012).

The importance of DPSIP legislation was further enhanced with the passage of the EU Directive 95/46/EC – the Data Protection Directive.[52] The Directive requires that the UK comply with basic principles through legislation. However, the UK continues a pattern of minimal compliance with the spirit and letter of the Directive. At the time of this writing, the EU is issuing charges of UK non-compliance.

7.3.3 Regulation of Investigatory Powers Act of 2000

The Act was passed to update UK telecommunications laws to account for technological developments and the EU Directive 97/66/EC. Part One, Chapter One criminalized the interception of communications in public and private postal and telecommunication systems. The law made allowance for consent waivers and criminal warrants. "The Act effectively establishes a free standing privacy right by creating a tort of unlawful interception."[53] Section Two, Part Nine allowed for traffic data monitoring; therefore, the impact on e-mail was open to interpretation. Morris[54] argued that in workplace situations, consent waivers must be interpreted as extremely limited. Neo-Conservative regulators interpreted the provisions of the law to balance toward business facilitation. The *fear card* that the businesses might leave the country was played by business special interests groups. Such groups financially supported legislators, and DPSIP legal interests were curtailed.

Whatever the legislative and case law in the UK, the approach is not working well. The Ministry of Defense reports that data on 1.5 million bits of information on 100,000 employees and 600,000 service applicants were

---

52 European Union Directives, *The 95/46/EC Directive*. (1995), at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML (last visited on 4 January 2012).

53 Tas Voutourides, *Privacy Protected by Interception Legalities. Law Society Gazette*. (2000, November 13), at http://www.lawgazette.co.uk/news/privacy-protected-interception-legalities (last visited on 15 May 20aa), at 11.

54 Gillian S. Morris, Fundamental Rights: Exclusion by Agreement? 30 *Industrial Law Journal* 1, 49 (2001).

violated. The numbers did not include the loss of 658 laptops and twenty-six memory sticks containing classified information.[55]

7.4 United Kingdom Case Law

Before examining the UK common or case law determinations on DPSIP legal issues, it is important to examine the power and reality constraints on the highest court in the jurisdiction. A discussion without a common benchmark would be meaningless. A legal declaration without exploring and understanding the de facto influences is myopic. The US Supreme Court was selected as the benchmark for this study because, in theory, it represents the international standard in the rule of law, balance of powers, and political independence analysis. Granted, evidence does exist that the benchmark Court has been inconsistent.[56]

Table 7.0 Comparison of United Kingdom and United States Supreme Court

Factor	**UK Supreme Court[57]**	**US Supreme Court[58]**
Established	2005	1789
Power of decisions	Applies to all courts and jurisdictions in England, Northern Ireland, and Scotland. The High Court of Justiciary addresses criminal issues in Scotland.	Applies to all courts and jurisdictions in the country.
Membership	President of the Court, Deputy President,	One Chief Justice and eight associate justices

55 Elizabeth Stewart, *MoD Loses Hard Drive Holding Military Personnel Data: Portable Drive Holding Private Details of 100,000 Army, Navy and RAF Personnel Belonged to MoD IT Contractor, EDS*. (2008, October 10), at http://www.guardian.co.uk/uk/2008/oct/10/military-defence (last visited on 11 October 2012).

56 See Chapter 8 of the current work.

57 The Supreme Court of the United Kingdom, The Supreme Court. (2010), at http://www.supremecourt.gov.uk/ (last visited on 30 December 2012).

58 Kermit L Hall, *The Oxford Companion to the Supreme Court of the United States* (Oxford University Press 2nd. ed. 2005). See also *Supreme Court of the United States, About the Supreme Court.* (2010), at http://www.supremecourt.gov/ (last visited on 5 July 2012).

	and ten puisne justices. All do not hear the same cases. The president can appoint acting judges.	(currently).
Appointee Background	Leading appellate courts judges and former Law Lords.	Leading appellate courts judges, politicians, and law professors.
Term of Office	Retire at 70 years old if appointed before 1995 or 75 if appointed after.	Life or until retires.
Jurisdiction	Appellate. Can not overturn primary legislation. However, it can overturn secondary legislation.	Original and appellate.
Role	Law—clarification.	Error—correction
Operations	Hears oral arguments and reviews documents.	Hears oral arguments but relies heavily on arguments presented in written briefs.
Decisions	Opinion of the majority, written by one justice, and concurring and dissenting opinions of other justices. Most cases heard by five-person panel.	Opinion of the majority, written by one justice, and concurring and dissenting opinions of other justices.
Judicial Review	Recent.	Historic since Marshall.
Appointment	Selection commission consisting of President and Deputy President of the court, and a member of the Judicial Appointments Commission for England and Wales, Northern Ireland, and Scotland.	President nominates, Senate confirms.
Representation	Tied to the old Law Justice system.	Recently more political.

Opinions	Reference cases - Can render advisory opinions	No advisory opinions.
Case Assignment	Court has discretion on selected cases. The court is responsible for EU and Human Rights cases.	Court determines what cases it will hear based on writ of certiorari. Since 1925, has discretionary docket control.

UK federal case law is tied to the EU case law reviews and its own common law tradition. The Appellate Committee of the British House of Lords has a long history of being legally conservative. Since 1876, the Committee had been Britain's Supreme Court in civil matters. Starting in 1960, the Committee became the *Supreme Court* in criminal matters except for Scotland. As noted earlier, the UK has somewhat reluctantly addressed DPSIP legal issues, but it must also be noted that a number of significant UK court decisions have supported individuals' rights to personal information privacy.

The first case on point was *Pope v. Curl* (1741). The English House of Lords (the highest court at the time) found that an author of a letter had an ownership interest in the letter and that another could not publish it without the author's consent. In essence, the court found that an individual had a property right in maintaining the privacy of personal information to the extent that another could not publish certain letters.[59]

Prince Albert sought an injunction against the publication of a list of etchings and works owned by Queen Victoria. In *Prince Albert v. Strange*, the court granted the injunction. The court found that "The jurisdiction in confidence is based not so much on property or on contract as on a duty of

---

[59] *Pope v. Curl,* 2 Atk. 324, 26 Eng. Rep. 608 (1741), 324. (UK)

good faith." [60] Lord Cottenham declared that in this instance "privacy is the right invaded." The holder of the confidential information has a duty of care and nothing should be done without clear consent.[61]

In *Saltman Engineering Co. Ltd. v. Campbell Engineering Co. Ltd.*,[62] the Court ruled in a case where an agent for the plaintiff delivered materials to the defendant to fill an order with an implied condition of confidence. The defendant violated the confidence for its own gain. The Court ruled that the obligation to protect confidential information does not require a contract between the parties. The confidential information cannot be public knowledge or in the public domain. However, the information does not need to be an absolute secret.

The Data Protection Act of 1984 applied only to electronic records. In *Gaskin v. United Kingdom*,[63] Gaskin wanted access to records related to his treatment care when he was a child. The government stated that it would release the records, provided that all case work writers consented. However, not all case writers could be contacted so the UK refused. The European Court of Human Rights found that the government's actions violated Article 8 of the Convention on Protection of Fundamental Rights and Fundamental Freedoms. Data holders had a "positive obligation" to provide a means of access to the personal data. The Court found no violation under Section Ten.[64]

A tension exists between DPSIP principles and free speech. In 1983, the Lords of Appeal in Ordinary established a right to free speech in

---

60 *Prince Albert v. Strange*, 1 H & Tw 1; 2 De G & SM 293; (1849) 1 Mac & G 25; [1849] EWHC Ch J20, (1849), 293. (UK)

61 *Id.*

62 *Saltman Engineering Co. Ltd. v. Campbell Engineering Co. Ltd*. 65 R.P.C. 203, (1948). (UK)

63 *Gaskin v. United Kingdom*, App. No. 10454/83, 12 Eur. H.R. Rep. 36, (1989). (UK)

64 Section 10 addresses freedom of expression concerns.

Derbyshire County Council v the Times Newspapers Ltd. and Others.[65] The case was a defamation charge brought by a county council. The next year, the Lords of Appeal in Ordinary, struck down sections of a Parliamentary Act for violating EU human rights law in *R v Secretary of State for Employment ex parte Equal Opportunities Commission*.[66] The decision was consistent with the *Regina v Secretary of State for Transport, ex parte Factortame.*[67]

In *R v Brown*[68] Lord Hoffmann wrote that the right of privacy is under technological threat. Massive amounts of intimate data are capable of instantaneous transmission with no notice. A further analysis of the threat is found in Lord Browne-Wilkinson's pronouncement in *Marcel v Metropolitan Police Commissioner.*[69] The judge determined that the currently massive amounts of personal data and data-mining abilities threaten individual freedom. According to the court, such a "dossier of private information is the badge of the totalitarian state."[70]

The Court of Appeals addressed the issue of a person being capable of gaining access to data held by a business under Sections 7 and 8 of the Data Protection Act. In *Durant v. Financial Services Authority*,[71] the court limited the amount of data that must be released. The rationale was that Durant was not the subject of the data. In 1993, Durant had sued Barclay Bank and lost. He wanted to obtain Barclay's records to attempt to re-open his litigation. Since the Financial Services Authority was the financial privacy regulator, he requested data from the Authority. The agency provided computer data about

---

65 *Derbyshire County Council v Times Newspapers Ltd and Others,* [1993] AC 534, [1993] 1 All ER 1011, [1993] 2 WLR 449, 91 LGR 179 House of Lords, (1993). (UK)

66 *R v Secretary of State for Employment ex parte Equal Opportunities Commission*, 2 WLR 409, 1994). (UK)

67 *Regina v Secretary of State for Transport, ex parte Factortame* (No 2) [1991] 1 AC 603, (1991). (UK)

68 *Regina v. Brown*, 1 ALL ER 545 at 555-556, (24 July 1997). (UK)

69 *Marcel v Metropolitan Police Commissioner*, Ch. 225 at 240, (1992). (UK)

70 *Ibid.*

71 *Durant v. Financial Services Authority*, EWCA Civ 1746, (2003). (UK)

him but redacted data about others. The Authority refused to provide all of the information and in the format Durant requested. The court ruled that "Mere mention of the data subject in a document held by a data controller does not necessarily amount to his personal data."[72] The court established a very restricted definition of a "relevant filing system." The definition required that the system must be able to verify that specific personal data can be found and where the file or search criteria can be located. The focus of the data must affect the person's privacy.[73]

Unauthorized photographs taken at the wedding of film stars Michael Douglas and Catherine Zeta-Jones appeared in magazines published in the UK and Europe. The Douglas' sought injunctive relief to no avail. After publication, the Douglas' sought damages under UK legal standards and the Data Protection Act. In *Douglas & Ors v. Hello! Ltd & Ors,* the High Court of Justice (Chancery Division) found for the Douglas' and determined nominal Data Protection Act violations and liability under the law of confidence.[74]

The High Court addressed the issue of a person's right to access data held by a data user. In *Alan Lord v. The Secretary of State for the Home Department,*[75] the court addressed the standards for access denial on the basis that the release would likely be prejudicial to larger interests. The court found that the term "likely" means a significant probability. A risk that the release would be prejudicial—even a real risk—is not enough. A more significant and weighty standard must be applied. According to the court, "The test of necessity is a strict one."[76] The use of a general non-disclosure policy does not satisfy this legal standard. In a victory for individual access to

---

[72] *Id.* at ¶ 28.

[73] *Id.* at ¶¶ 27-28.

[74] *Douglas & Ors v. Hello! Ltd & Ors* [2003] EWHC 786 (Ch) (11 April 2003) [2003] 3 All ER 996, [2003] EMLR 31, [2003] EWHC 786 (Ch), (2003). (UK)

[75] *Alan Lord v. The Secretary of State for the Home Department*, EWHC 2073, (1 September 2003). (UK)

[76] *Id.* at ¶¶ 99-100.

personal data, which a cornerstone DPSIP issue, the court ordered a "full and un-redacted" disclosure.

In 2004, the Financial Services Authority issued an order against the Nationwide Building Society. The case was litigated. The Financial Services Authority[77] issued a final judgment on the Nationwide Building Society. Under Section 206 of the 2000 Financial Services and Markets Act, the largest building society in the country was fined £980,000 because of the theft of a laptop computer that contained massive amounts of customer data.[78]

In *Campbell v. Mirror Group Newspapers Ltd*.[79] the majority of the UK House of Lords decided that even a well-known supermodel had some privacy rights about the publication of personal information. On February 1, 2001, *The Mirror* published an article related to model Naomi Campbell's drug and counseling treatment. After the publication of this information, the model sought legal relief. The magazine went on the attack and published further private information. The majority of the judges determined that the magazine had gone too far.[80]

The case of *X v. British Broadcasting Corporation & Anor*[81] addressed privacy issues in a situation where the BBC was producing a film documentary on the Scottish criminal justice system. Miss X wanted all pictures and references

---

77 Financial Services Authority, *Financial Services Authority v. Nationwide Building Society*. (2007, February 14), at http://www.fsa.gov.uk/pubs/final/nbs.pdf (last visited on 8 September 2012).

78 *Id.* at 2. Nationwide had "failed adequately to assess the risks in relation to the security of its customer information, in relation to information security which failed adequately and effectively to manage the risks … to implement adequate controls to mitigate information security risks… failed to have appropriate procedures in place to deal with an incident involving the loss of customer information.

79 *Campbell v. MGN Ltd* [2004] UKHL 22 (6 May 2004) [2004] UKHRR 648, [2004] 2 AC 457, [2004] EMLR 15, [2004] UKHL 22, 16 BHRC 500, [2004] 2 WLR 1232, [2004] HRLR 24, [2004] 2 All ER 995, (2004). (UK)

80 *Id.*

81 *X v. British Broadcasting Corporation & Anor* [2005] ScotCS CSOH_80 (22 June 2005), ¶ 60. (UK) The court issued an "*interim* interdict against the first defenders to restrain broadcast of those parts of the documentary video relating to the pursuer whether showing her directly or showing others referring to the pursuer thereby identifying her and disclosing personal information about her."

about her deleted. Although Miss X signed a release, she had dyslexia and did not understand the legal document or its implications. Moreover, the producer had orally promised Miss X final approval rights. The court found for the plaintiff.[82] The decision was based on privacy provisions in the European Convention on Human Rights[83] and the 1998 Human Rights Act.[84]

The High Court of Justice decision in *Ash & Anor v. McKennitt & Ors*[85] was appealed to the Supreme Court of Judicature Court of Appeal (Civil Division). The Supreme Court dismissed the appeal of the lower court ruling. The case involved a successful musician who argued that her privacy was being violated by the publication of private facts in a book. Despite her fame, she had a long history of keeping her personal life private. The lower court had enjoined the publication of parts of the book on the basis of privacy concerns.

In the case of *Regina v. Jacqueline Mary Rooney*,[86] the Court of Criminal Appeals reduced the Recovery of Defense Costs Order because of economic hardship. The defendant was a human resource employee of the Stafford Police department who unlawfully accessed personnel records for personal reasons and without consent. The court found that the "unlawful use of the information contained in personal data" is serious.[87]

---

82 *Id.*

83 European Convention of Human Rights and Fundamental Freedoms, *European Convention of Human Rights and Fundamental Freedoms*. (1950), at http://conventions.coe.int/treaty/en/Treaties/Html/005.htm (last visited on 24 September 2012), § 8, 10.

84 European Convention of Human Rights and Fundamental Freedoms, *European Convention of Human Rights and Fundamental Freedoms*. (1950), at http://conventions.coe.int/treaty/en/Treaties/Html/005.htm (last visited on 24 September 2012), § 12.

85 *Ash & Anor v. McKennitt & Ors*. [2006] EWCA Civ 1714 (14 December 2006) [2007] 3 WLR 194, [2007] EMLR 4, [2006] EWCA Civ 1714, [2008] QB 73, [2006] EMLR 178, (2006). (UK)

86 *Regina v. Jacqueline Mary Rooney*. EWCA Criminal 1841 (12 July 2006), ¶ 16. (UK) The court found that "the police are entitled to regard unlawful use of the information contained in personal data on police computers as a serious matter. Based on the verdict of the jury it would appear, sadly, that the appellant did abuse her position and then lied about it both in an interview and in the witness box."

87 *Id.*

On December 17, 2007, Norwick Union Life was fined £1.26 million by the Financial Services Authority.[88] The company failed to develop and implement effective control, risk management, and security processes as required by the Data Protection law. Personal information on 6.8 million customers in the UK was made available. The court found Norwick Union Life liable.

On 13 March 2007, the Information Commissioner's Office for the UK announced the settlement of a Data Protection Act case for improper disposal of customer data. Eleven banks, other financial institutions, and the Immigration Advisory Service were found to be disposing of private data in street trash bins. The Deputy Commissioner declared: "It is unacceptable for banks and other organizations to carelessly discard their customers' information."[89]

Orange Personal Communication Services v. ICO[90] reinforced the principle that data holders must have secure digital access controls. The case followed an ICO investigation of Orange Personal Communication Services. The agency found that employees were sharing names and passwords to access the databases. The ruling was based on the seventh principle of Schedule 1, Part 1 of the Data Protection Act. The principle is that "The sharing of user names and passwords by Customer Service Representatives, to access computer systems, shall not be allowed under any circumstances."[91]

---

88 Financial Services Authority, *Financial Services Authority v. Norwich Union Life aka CGNU Life Assurance Limited, Commercial Union Life Assurance Company Limited, Norwich Union Annuity Limited, Norwich Union Life and Pensions Limited, and Norwich Union Life Services Limited*. (2007, December 17), at http://www.fsa.gov.uk/pubs/final/Norwich_Union_Life.pdf (last visited on 8 September 2012).

89 Information Commissioner's Office, *Banks in Unacceptable Data Protection Breach*. (2007, March 13), at http://www.ico.gov.uk/upload/documents/pressreleases/2007/banks_in_unacceptable_data_protection_breach.pdf (last visited on 17 June 2012), 1.

90 Information Commissioner's Office, *Orange Personal Communication Services v. ICO* UK. (2007 March 21), at http://www.ico.gov.uk/upload/documents/library/data_protection/notices/orange_undertaking.pdf (last visited on 30 September 2012), 2.

91 *Ibid.*

Despite these rulings in favor of individual rights to information privacy, the UK courts are not very supportive of the spirit of DPSIP legislation. A case on point is *Johnson v. Medical Defense Union*.[92] The case addressed the issue of fair processing. Johnson was a consultant orthopedic surgeon. Although a number of complaints were lodged against him, no negligence claims had been made. Medical Defense Union claimed that the number of complaints potentially indicated some risk, and terminated Johnson's membership in their organization. Johnson filed suit that Medical Defense Union unfairly processed his personal data. The court found that because the Medical Defense Union had manually selected the data, it did not constitute an automated processing of the data. Although Johnson argued that the manual selection was unfair because his views and explanations were not taken into account, the Court found that no processing of the data occurred, even though the data was maintained in a computer data base.

From March 2007 through September 2008, the ICO issued a number of court approved enforcement notes of Data Protection Act violations.[93] The list includes business organizations, financial institutions, governmental agencies, and police organizations.[94] At the time of this writing, retailer Marks & Spencer, was appealing the ICO enforcement notice. The charge was that

---

92 *Johnson v. Medical Defense Union*, EWCA Civ 262, (28 March 2007). (UK)

93 Information Commissioner's Office, *Enforcement Notices*. (2008), at http://www.ico.gov.uk/what_we_cover/data_protection/enforcement.aspx (last visited on 29 September 2012), 1. The ICO certainly had more breadth and depth of authority than any agency in the US.

94 *Ibid.* The Business Organizations included Alliance & Leicester, Carphone Warehouse, Cash Generators, Littlewoods Shop Direct Home Shopping Ltd., Marks & Spencer, Orange Personal Communications Services Ltd., Phones4U, Post Office Limited, Royal British Legion Club, and TalkTalk. The **Financial Institutions** included Barclays Bank, Clydesdale Bank, Co-operative Bank, HBOS, FC Bank, Loans.co.uk, Nationwide Building Society, Natwest, Royal Bank of Scotland, Scarborough Building Society, Skipton Financial Services, and United National Bank. The **Governmental Agencies** included the Commonwealth Office, Department of Communities and Local Government, Department of Health, Foreign Office, HM Revenue and Customs, and Ministry of Defence. The **Police Institutions** included the Greater Manchester Police, Humberside Police, Northumbria Police, Staffordshire Police, and West Midlands Police.

the company had lost an unencrypted laptop computer with the pension data on 26,000 persons.[95]

The case of *Murray v. Big Pictures (UK) Ltd*[96] was really a misnomer. The parties were better known as J. K. Rowling (the author of the *Harry Potter* books) and her husband, who is a dentist. Pictures had been taken of their infant without permission. As parents, they sought relief under the privacy protections of Article 8 of the European Convention on Human Rights and the 1998 Data Protection Act. The Supreme Court of Judicature Court of Appeal (Civil Division) referred the case back to the trial court for a full trial of the privacy concerns. The Supreme Court decision suggests the importance of a full trial of privacy concerns. Key issues need to be examined. Do public figures have a right to privacy protections? Can privacy concerns take precedence over press rights? Does a person have a right to limit an invasion of privacy? The case suggests that UK courts are becoming more aware of DPSIP legal issues.

7.4.1 Information Tribunal

The UK Information Tribunal[97] has issued a few relevant DPSIP decisions that favored personal privacy; however, as is often the case, upheld exceptions based on broad and somewhat questionable criteria. The *Community Charge Registration Officer of Rhondda Borough Council v Data Protection Registrar*[98] case involved the collection of date of birth information on a community canvas that the Registrar refused to certify. The Tribunal ruled that the additional data was not necessary or proper. In a related

---

95 Information Commissioner's Office, *Marks & Spencer v. ICO*. (2008, January 23), at http://www.ico.gov.uk/upload/documents/library/data_protection/notices/m_and_s_sanitiseden.pdf (last visited on 29 September 2012). (UK)

96 *Murray v. Big Pictures (UK) Ltd* [2008] EWCA Civ 446 (7 May 2008). (UK)

97 Formally called the Data Protection Tribunal. See Information Tribunal, *Tribunal Service: Information Rights*. (2010), at http://www.informationtribunal.gov.uk/aboutus.htm (last visited on 14 August 2012).

98 *The Community Charge Registration Officer of Rhondda Borough Council v Data Protection Registrar*, Data Protection Tribunal (Case DA/90 25/49/2). (UK)

Community Charge Registration[99] registrar refusal, the Tribunal confirmed that property-type information was personal data. The Registrar argued that the officers violated the fourth personal privacy principle.[100] The Tribunal agreed that a fourth principle violation occurred and that personal information and property information were the same.

In *Equifax Europe Limited v The Data Protection Registrar*,[101] Equifax argued that referencing and processing addresses was not a personal identifier violation. The Tribunal rejected the argument. According to the Tribunal, although the interests of the credit reporting industry should be acknowledged, the interests of the data subjects are critical. The case acknowledges the impact of data mining and the limitation of the personal identifier model.

Infolink Limited, a credit information business, collected data from public records including court records. The Tribunal found that the extracting process was open to unfair practices and revealed information regarding third parties.[102]

In *Innovations (Mail Order) Limited v Data Protection Registrar*,[103] Innovations operated a mail order business requiring the collection of some personal information; however, the data was sold to list brokers with little or late notification to the subject. The Tribunal supported the Registrar's view that the practice was a violation of the 1984 Act. Innovations argued that it had complied with the industry code of practices; however, the court rejected

---

99 *Community Charge Registration Officer of Runnymede Borough Council v Data Protection Registrar (Case Da/90 24/49/3); Community Charge Registration Officer of South Northamptonshire District Council v Data Protection Registrar (Case Da/90 24/49/4); Community Charge Registration Officer of Harrow Borough Council v Data Protection Registrar (Case Da/90 24/49/5).* (UK)

100 Personal data shall be accurate and, when necessary, kept up to date.

101 *Equifax Europe Limited v The Data Protection Registrar*, Data Protection Tribunal (DA/90 25/49/7). (UK)

102 *Infolink Limited v The Data Protection Registrar*, Data Protection Tribunal (DA/90 25/49/6). (UK)

103 *Innovations (Mail Order) Limited v Data Protection Registrar*, Data Protection Tribunal Case DA/92 31/49/1). (UK)

the argument because the Registrar had qualified the acceptability of the code.

The *Linguaphone Institute Limited v Data Protection Registrar*[104] case involves a similar fact pattern as the Innovation case. After the Registrar noted the unlawful practice and before the case was appealed to the Tribunal, the company added an opt-out tab in small print at the end of the order form. The Tribunal found both practices violated the law.

Midlands Electricity used its customer database to send a marketing-oriented magazine with advertisements from other companies to customers without the consent of the customers. No effective opt-in or opt-out option was provided. The Registrar and the Tribunal found that the practice represented unfair data processing.[105]

In *Norman Baker v. Secretary of State for the Home Department*,[106] the Information Tribunal - National Security Appeals Panel addressed the power of the national security data protection exemption. Baker, a Liberal Democrat Member of Parliament, wanted access to his data held by the security services. The service claimed that it had staff administration, building security, and commercial agreements. However, any personal data is exempt and is not accessible. The Tribunal found that while blanket exception standards exist, the court must determine each exception on a case-by-case basis. In the instant case, the security certificate was quashed. In subsequent cases,[107] the Tribunal found for an alternative appeal process; however, the result was the same. The Tribunal supported the security exception decision. The Tribunal appeal alternatives provide procedural relief

---

104 *Linguaphone Institute Limited v Data Protection Registrar*, Data Protection Tribunal (Case DA/94 31/49/1). (UK)

105 *Midlands Electricity PLC v. The Data Protection Registrar*, Data Protection Registrar (DA/ 99). (UK)

106 *Norman Baker v. Secretary of State for the Home Department*, UKHRR 1275, (2001). (UK)

107 *Peter Hitchens v. Secretary of State for the Home Department*, UKHRR 1275, (10 December 2001) (UK). See also *Tony Gosling v. Secretary of State for the Home Department*, UKHRR 1275, (10 December 2001). (UK)

but no substantive change. The UK approach appears to provide few checks and balances on DPSIP exceptions. Exceptions provide a means to circumvent the spirit of DPSIP laws. Such an approach supports an argument that the end justifies the means.

7.5 European Union Case Law

The European Court of Justice and the European Court of Human Rights essentially function as the final appellate courts for member states. The principle was certainly true in the UK, and generally these European courts were more supportive of personal privacy than courts in the UK and other member states. From 1959 to 1989, The Human Rights Commission heard more cases from the UK than any other signatory nation. The experience had a significant impact on the UK focus, and by 2007, the number of UK cases was significantly reduced. At that point in time, the largest percentage of cases focused on Turkey, Russia, Poland, and the Ukraine, which accounted for forty-nine percent of all judgments.[108]

The Lords of Appeal in Ordinary became more responsive to considering Commission principles and language in responding to DPSIP issues.[109] In 1966, the Lords ruled that it could overrule its own decisions.[110] For example, the Lords issued a reversal of its *London Street Tramways v. London County Council* Case.[111]

---

[108] European Court of Human Rights, *Annual Surveys of Activity*. (2008), at http://www.echr.coe.int/ECHR/EN/Header/Reports+and+Statistics/Reports/Annual+surveys+of+activity/ (last visited on 24 August 2012).

[109] N. Bratza, *The Treatment and Interpretation of the European Convention on Human Rights: Aspects of Incorporation*, *in* European Convention on Human Rights: Aspects of Incorporation (J. P. Gardner ed. 1992).

[110] House of Lords, Practice Statement 119661 1, 58 *Weekly Law Reports,* 1234 (1966).

[111] See UK: *London Street Tramways v London County Council,* [1898] AC 375, (1898).

The 1992 case of *Niemietz v. Germany*[112] contrasted the US position of protecting privacy at home but not in the workplace. The European Court of Human Rights declared that privacy is not directly tied to place. The reasoning was that private life can not exclude business or professional relationships or places.[113]

In 1998, the European Court ruled that individuals have a legal right to access personal information relating to them. In *Gaskin v. the United Kingdom*,[114] the court found that no procedures were available for the data subject to gain access to the personal information held by the government. The Court ruled that the UK had a positive obligation to protect private data and respect a person's right to access his or her data.[115]

On January 11, 2000, the European Commission started violation litigations against Germany, France, Luxembourg, and the Netherlands. By 2001, every country but the Netherlands were found to be noncompliant with the Directive.[116]

In 2001, the UK was a party in a European Court of Human Rights case. The case of *Hatton and Others v. the United Kingdom*[117] found "a positive duty on the State to take reasonable and appropriate measures to secure the applicants' rights under Article 8 § 1 of the Convention" on the Protection of Fundamental Rights and Fundamental Freedoms.[118] The case involved privacy rights of those living next to the Heathrow airport. The majority of the Court found an Article 8 violation and an Article 13 violation of the EU Convention. Article 13 declares that "Everyone whose rights and freedoms as set forth in this Convention are violated shall have an effective remedy before

---

112 *Niemietz v. Germany*, E.C.H.R. 12/16/1992, (1992). (EU)
113 *Id.*
114 *Gaskin v. the United Kingdom*. July 7, 1989, Series A, No 160, (1998). (UK)
115 *Id.*
116 Joel R. Reidenberg, E-commerce and Trans-Atlantic Privacy, 38 *Houston Law Review,* 717-749 (2001-2002), at 733.
117 *Hatton v. United Kingdom,* ECHR 565, (2002) 34 EHRR 1, (2001), § 95. (EU)
118 *Id.*

a national authority notwithstanding that the violation has been committed by persons acting in an official capacity."[119] On appeal, the Grand Chamber reversed the decision on the violations. The Court refused to ignore the dictum of a positive duty to protect.

In an earlier case, *Leander v. Sweden,*[120] the Court found a privacy duty under Article 8(1) of the Convention on the Protection of Fundamental Rights and Fundamental Freedoms but did not find that Sweden had violated Section 8(2). The case involved the personnel records of Leander, who applied for and was rejected for a high governmental position as a security risk. The Court found an Article 8(1) breach. The breach was founded upon the fact that "both the storing and release of such information… were coupled with a refusal to allow Mr. Leander an opportunity to refute it."[121] A similar ruling was found in *Chavenee Jullien v. France.*[122] The petitioner wanted her name removed from a list of people with psychiatric diagnoses. The Court found the list retention was a violation of Article 8(1) but that the government had a Section 8(2) justification.

In the case of *Amann v. Switzerland*,[123] the court further found that storing and retaining private information is an Article 8(1) violation. Business and professional justifications do not trump the legal protection provided by the law.[124] The European Court of Human Rights found that rights, freedom, and privacy apply to the identified or identifiable person.

---

119 *Id.* at § 108.

120 *Leander v. Sweden*, 26 March 1987, 9 EHRR 433, (1987). (EU)

121 *Id.* at ¶ 48.

122 *Chavenee Jullien v. France*, Appl 14461/88, 71 DR 141, (1991). (EU)

123 *Amann v. Switzerland*, ECHR 27798/95, (2000),¶ 65 EU). The purpose is to secure in the territory of each Party for every individual ... respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him" (Article 1), such personal data being defined as "any information relating to an identified or identifiable individual (Article 2).

124 *Id.*

The Court expanded on the legal principle in *Rotaru v. Romania*.[125] The case involved an applicant that wanted access to Romanian Secret Police records to correct possible errors. The Court ruled that Article 8 was violated by collection, storage, access refusal, non-disclosure, and confidentiality standards. The Court found that state parties have both a negative and positive obligation in protecting personal privacy. The negative obligation is not to breach the existing legal rights. The positive obligation is to respect that the rights exist.

In *Peck v. The United Kingdom*,[126] the European Court of Human Rights found for Peck, who was depressed and suicidal. The Brentwood Borough Council's closed-circuit television (CCTV) taped him while slitting his wrists and then released the data to public television. Peck found no relief in the UK courts. The EU Court unanimously found that the government violated Articles 8 and 13 of the Convention for the Protection of Human Rights and Fundamental Freedoms. The UK was required to pay 11,600 Euros in non-pecuniary damages and 18,075 Euros, plus value-added taxes for costs and expenses.

The Court of Justice of the European Communities (including Court of First Instance Decisions)[127] ruled on the Lindqvist (Approximation of Laws) case. Mrs. Lindqvist set up a web page at home on her personal computer to post information on parishioners who were preparing for confirmation. She requested and was granted a link to the web site of the Swedish Churches.

---

125 *Rotaru v. Romania* ECHR 28341/95; 8 BHRC 449, (2000), ¶ 5). (EU) The Court noted that "no provision of domestic law laid down any limits on the exercise of those powers. Thus, for instance, domestic law did not define the kind of information that could be recorded, the categories of people against whom surveillance measures such as gathering and keeping information could be taken, the circumstances in which such measures could be taken or the procedure to be followed. Similarly, the Law did not lay down limits on the age of information held or the length of time for which it could be kept (Article 8)."

126 *Peck v. the United Kingdom* (application no. 44647/98), (2003). (EU)

127 Court of Justice of The European Communities (Including Court Of First Instance Decisions), *Lindquist (Approximation of laws) [2003] EUECJ C-101/01 (06 November 2003) [2004] QB 1014, C-101/01, [2003] EUECJ C-101/01, [2004] All ER (EC) 561 (*(2004), at http://www.bailii.org/eu/cases/EUECJ/2003/C10101.html (last visited on 28 September 2012).

The site included information on the webmaster and eighteen colleagues in the parish. The data included full names, first names, jobs, telephone numbers, and even medical conditions. The colleagues and the supervisory data protection authorities were not told about the site. When the colleagues formally complained and instituted legal recourse, she removed the web page.

The court ruled that the Internet page violated Article 3(1) of the Directive 95/46 of the European Parliament. The activities on the site amounted to a processing of personal data, and there was not an Article 3(2) exemption available. Article 8(1) was violated with the note that one colleague was working part-time because of an injured foot - which amounted to the processing of sensitive personal medical data. The court found that the Directive 95/46 supports the freedoms and rights of the European Convention for the Protection of Human Rights and Fundamental Freedoms.

In *P.G. and J.H. v. United Kingdom,*[128] the European Court of Human Rights distinguished the European and US judicial views on *reasonable expectation of privacy*. The US courts considered the expectation as sacrosanct. The European Court determined that the reasonable expectation principle may be significant but not necessarily conclusive. The Court determined that it was clear that a violation of one's private life may occur even in a public place. A private life includes but is not limited to gender identification, name, right of personal development, right to develop interpersonal relationships, right to identify, and right to choose a sexual lifestyle. The scope of private life may include personal interactions, even in a public context.

The European Court of Human Rights ruled that Article 8 of the European Convention of Human Rights applied in the Case of *Copland v. The United Kingdom*.[129] The case involved management officials accessing the e-mail and Internet usage of a colleague employee, without obtaining the

---

[128] *P.G. & J.H. v. United Kingdom*, E.C.H.R., 9/25/2001, (2001). (EU)

[129] *Case of Copland v. The United Kingdom*, Application no. 62617/00 (3 April 2007) (ECHR, (2007), ¶ 48. (EU)

person's consent. The Court declared the following: "The Court would not exclude that the monitoring of an employee's use of a telephone, e-mail or internet at the place of work may be considered 'necessary in a democratic society' in certain situations in pursuit of a legitimate aim."[130]

The European Court of Justice, on January 29, 2008, issued a decision in *Productores de Música de España (Promusicae) v. Telefónica de España SA.*[131] The case involved Internet access providers. The providers were required to keep data for a set period of time. A group of copyright holders wanted access to determine if any intellectual property right violations had occurred. The Court observed that "This case illustrates that the storage of data for specified purposes creates the desire to use those data more extensively."[132] The court found that EU members are not required to transfer or allow access to personal information in a civil litigation related to copyright protections.

In 1999, The Spanish Data Protection Authority started investigating Microsoft's subsidiary in Spain for improperly handling and storing personal data. This was the first time that an American company was brought to account under the EU Data Privacy Directive. The company was found guilty and fined fifty million pesetas; however, this amount was later reduced to 10 million pesetas ($250,000 to $50,000 USD).[133] Gregory Shaffer noted that the Europeans consider privacy as a human right—not an issue that can be bargained away.[134] Not even Microsoft could violate a privacy human right for profit.

---

130 *Id.*

131 *Productores de Música de España (Promusicae) v. Telefónica de España SAU*, Case C-275/06, (2008), ¶ 1. (EU)

132 *Id.*

133 Christopher Kuner, Beyond Safe Harbor: European Data Protection Law and Electronic Commerce, 35 *International Lawyer* 79 (2001)

134 Gregory Shaffer, Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards, 25 *Yale Journal of International Law 1* (2000).

The European system encounters difficulties when the standards do not match standards in other parts of the world. A case in point was the length of time that search engines can store data. The European standard is six months. The mega search engine, ixquic.com, follows the European standard and even eliminates all traces of individual searches within 48 hours. The practice may make the service operate at a small competitive disadvantage to other firms. The firm has established a major marketing strategy for its privacy compliance. The US firm Google kept data for 9 months while Microsoft and Yahoo kept data for 13 months. EU data protection officials were attempting enforcement compliance against non-compliant firms. The effort met with considerable resistance. Officials were threatening anti-trust actions if the three firms did not start to comply. French official Alex Türk proclaimed, "If Google and others continue to ignore EU law and gain an unfair advantage over companies based in the EU which follow the law, then one could argue that that is a competition issue."[135]

The EU is the international gold standard for DPSIP legal concerns. The EU is more dedicated to the Directives than UK legislators and jurists. The UK has resisted following EU standards and has been called for improvements.

7.6 Constituent Government Constitutional Declarations

Northern Ireland, Scotland, and Wales do not have separate written constitutions. Each country must comply with UK legal standards. Each must comply with all applicable delegation powers acts. The standards are also with applicable EU directives. The system is similar in practice to the relationships between state and federal law and treaties in the US.

---

135 Kevin J. O'Brien, *European Standoff Over Search Engine Data*. (2008, October 5), at http://www.iht.com/articles/2008/10/05/business/privacy06.php?page=1 (last visited on 6 November 2012), ¶ 3.

7.7 Constituent Government Legislation

Northern Ireland and Wales do not have enabling DPSIP laws. Both are subject to UK legislation.[136] Scotland is also subject to UK and EU law related to DPSIP issues. The Scottish Executive and Parliament has endorsed the provisions of the 1998 Data Protection Act.[137] A call has been made for Scotland to pass a privacy law. The position is that it can not wait for England and Wales to find a significant case to establish a common law principle. The law could either mirror the UK approach or establish sound differences.[138]

The *Scottish Regulation of Investigatory Powers Act*[139] addresses some privacy concerns. The Act addresses various surveillance issues, including the appointment of a Chief Surveillance Commissioner and provides some checks and balances for potential privacy violations.

England and Wales have proposed a new British bill of human rights. Scotland and Northern Ireland have promised to veto the move. Northern Ireland maintains that the move is a violation of the Good Friday peace agreement. Scotland maintains that the issues are addressed under the Scotland Act.[140] UK efforts at addressing DPSIP legal concerns are

---

136 See § 7.3 United Kingdom Federal Legislation above.

137 Scottish Executive, Data Protection Act 1998 Explanatory Guidance. (1998), at http://www.scotland.gov.uk/Resource/Doc/1066/0006064.pdf (last visited on 19 August 2012). See also Scottish Parliament, The Data Protection Act 1998 and Subject Access Requests. (1998), at http://www.scottish.parliament.uk/corporate/foi/sar/ (last visited on 19 August 2012).

138 Suzie May, *A Picture's Worth a Thousand Words*, The Journal Online: The Member's Magazine of the Law Society of Scotland. (2010), at http://www.journalonline.co.uk/Magazine/55-7/1008393.aspx (last visited on 19 July 2012).

139 *Regulation of Investigatory Powers (Scotland) Act 2000 asp 11* (2000). (UK)

140 Afua Hirsch, *Scotland and N Ireland Could Reject Bill of Rights: Proposals to Change the Human Rights Act Could Become a 'Legal and Political Nightmare,' Experts Have Said*, guardian.co.uk. (2010), at http://www.guardian.co.uk/uk/2010/feb/07/northern-ireland-bill-of-rights (last visited on 10 August 2012).

hampered by divisions within England and the rest of the country. Perhaps the DPSIP effort needs to be removed from the UK views on human rights.

7.8 Constituent Government Case Law

The case law of Northern Ireland, Scotland, and Wales is generally subject to UK and EU case law.[141] Conflicting case decisions are subject to appeal to the UK Supreme Court and the EU courts.

7.9 United Kingdom Standards and Remedies

DPSIP legal protections are evolving in the UK. The UK is not as advanced as the standards in CA and in some ways AU. Barrington Moore argues that historically there have been information privacy rights in England.[142] Victorian England provided for political freedom and privacy. The view was that the individual was the basic unit of society and that the interests of businesses, groups of people, and the government are subservient.

7.10 United Kingdom Implementation System

The UK requires that data holders and processors register[143] and pay an operating fee[144] that provides an added level of control and revenues. The approach is similar to laws that regulate professionals whose practices involve

---

[141] See § 7.4 United Kingdom Case Law and § 7.4.1 European Union Case law above.

[142] Barrington Moore, Jr, *Privacy: Studies in Social and Cultural History* (M.E. Sharpe, Incorporated. 1984).

[143] The registration is similar to a license under US law. One can not function if not registered.

[144] The fee ccurrently ranges from £35 a year to £500 for large organizations. See Chris Williams, *Data Watchdog Jacks Up Charges: Privacy Costs After All*, The Register. (2009), at http://www.theregister.co.uk/2009/10/01/ico_charges/ (last visited on 5 October 2012). The process saves companies £15.5 million in losses. Operational costs are about £53 million but the figure does not address revenue factors. See Chris Greenwood, *Data Protection Act Costs Country £53m Every Year*, The Independent. (2010), at http://www.independent.co.uk/news/uk/politics/data-protection-act-costs-country-pound53m-every-year-2019747.html (last visited on 6 July 2012).

consumer protection.[145] Failure to register is a criminal offense and can be punished by monetary fines. The potential loss of such a license provides an incentive to comply with the DPSIP laws, or the organization could be forced out of business. The approach also shifts the cost of DPSIP from potential taxpayers; however, registration funding also limits the enforcement resources that a tax payer approach could provide. Ian Lloyd[146] argues that in the UK, the approach is a governmental abdication of a DPSIP responsibility that establishes an "outdated and bureaucratic system."

Perhaps there is a better approach that involves a formal licensing requirement with fees related to regulatory costs, as well as governmental funding for an independent agency[147] that protects the common good. Thus, licensing and related fees increase the power of the DPSIP law and regulators, and nudges compliance to relevant DPSIP laws. Compliance is thus directly related to data protection and security. Given that DPSIP legal issues are essential to protecting the social contract,[148] a fully funded independent regulatory agency relieves DPSIP legal regulation from economic and political pressures. The approach would provide checks and balances while protecting against special interests power plays.

This approach runs counter to a policy perspective that supports a corporate republic. The corporate policy perspective is that one person one vote is antiquated. Not only do corporations have human rights, they can use unlimited funding to establish self serving policy agendas. Corporations want to privatize profits while socializing risks. The view is that the ability of companies to make profits should not be constrained. However, the government and the people should cover any and all risks. The basic

---

145 Examples include attorneys, mental health professionals, and physicians. The list also includes barbers, contractors, and even realtors.

146 Ian J. Lloyd, *Information Technology Law,* 33 (Oxford University Press 5th. ed. 2008).

147 An independent agency is one that does not have to report or be held accountable to parliament or the executive. Examples include the Federal Trade Commission or the Federal Reserve in the US.

148 Jean Jacques Rousseau and John Locke argued that individuals make an expressed or implied agreement or contract for mutual protection. The protections include freedom from abuses of power by corporations and the government.

calculus is flawed. Profits and risks are interconnected, and all stakeholders' interests must be protected. This perspective has negatively countered DPSIP legal efforts in the UK, AU, and the US.

The UK does, at times, take heed of the findings of the EU Article 29 Working Party. In addressing RFID technology and privacy concerns, the group reinforced the need for clear consent of the person. The use of RFID technology must adhere to standards of access to examining the data. Controls are needed to identify the purpose of collection and any other uses of the data. Any one of these factors can lead to a DPSIP finding when they are used to identify, learn, or record individual data.[149]

The Advertising Standards Authority of Britain (ASAB)[150] has the power to monitor the majority of advertising practices. The authority addresses Internet advertisements like banners and sponsored links. Recently the organization announced that the standards also apply to blogs, non-traditional digital marketing, mobile applications, organizational web sites, and social media. The ASAB authority has an agreement with Google, which controls eighty percent of the UK web searches, to block paid searches to offending marketers. The agreement came after years of delaying any attempt to address behavioral targeting activities or responses.[151]

Starting 6 April 2010, the ICO increased the agency's powers to fine organizations that experience a data breach. Previously, the maximum fine was £ 5,000 pounds. A new fine limit of £ 500,000 pounds is possible for

---

149 Article 29 Data Protection Working Party, Working Document on Data Protection Issues Related to RFID Technology (10107/05/EN-WP 105). (2005), at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp105_en.pdf (last visited on 29 August 2012).

150 A private self-regulatory organization that sets voluntary standards to avoid governmental regulation.

151 Eric Pfanner, *British Advertising Regulator Making Itself Felt Online*, The New York Times. (2010), at http://www.nytimes.com/2010/09/06/business/media/06cach.html (last visited on 5 September 2012).

serious breaches based on negligence. The new policy also provides for compulsory audit notices.[152]

7.11 United Kingdom Sociolegal Concerns

In 2003, sixty percent of Europeans reported strong concerns related to privacy protection. Seventy percent reported that awareness of violations was low in their home country. Only forty-two percent were aware of data protection laws and responsibilities. In 2007, sixty-four percent wanted protection from breach violations.[153]

Almost seventy-five percent of Europeans reported that they were worried about their lack of control of personal information. While more than fifty percent trusted employers, financial institutions, local governments, medical services, police, social security, and tax authorities to follow data protection and security standards. Less than half trusted credit card agencies, credit reference agencies, mail order companies, marketing companies, nonprofit organizations, opinion research companies, and travel businesses. The loss of personal data for 25 million persons by the UK Government was a strong area of concern.[154] The Angus Reid[155] data showed that fifty-nine percent were concerned about new technology being used to violate personal privacy standards.

---

152 Information Commissioner Office, Information Commissioner's Guidance About the Issue of Monetary Penalties Prepared and Issued Under Section 55C (1) of the Data Protection Act 1998, Author. (2010), at http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/ico_guidance_monetary_penalties.pdf (last visited on 12 September 2012).

153 Wik-Consult/Rand Europe/Clip/Crid/Glocom, *Comparison of Privacy and Trust Policies in the Area of Electronic Communications: Final Report* (Authors 2007).

154 Aoife White, *EU Poll Shows Three Out of Four Europeans Worried about Personal Data Online* (22 January 2008), http://news.theage.com.au/technology/eu-poll-shows-three-out-of-four-europeans-worried-about-personal-data-online-20080122-1nba.html (last visited on 22 April 2012).

155 Angus Reid Global Monitor, *Five Countries Review Privacy, Technology* (2006), http://www.angus-reid.com/polls/view/11915 (last visited on 31 March 2012).

A study by the European Commission found that eighty percent of the youths studied were concerned about governments and businesses using their personal data without permission and sharing it with third parties. The sample also thought the governmental regulation was necessary and that few use current protection technology.[156]

The issue of data security in business organizations was addressed in a study of 107 international security officials from fifteen countries including the UK. The study reinforced security concerns. Ninety-six percent argued for legal regulation of breaches and fifty-nine percent supported compensation for breach victims. Seventy-nine percent thought the data security pressure was increasing. Chief Executive Officers and Boards of Directors were thought responsible by ninety-five percent – up from seventy-four percent the year before, and survey respondents thought the appropriate response should be jail sentences. Seventy-six percent thought that business organizations were being reactive to the issue.[157]

Politicians and jurists can and certainly do argue and maneuver around DPSIP issues. Businesses and corporations can and do corrupt the process.[158] The above research shows that the majority of UK citizens want strong DPSIP legislation and regulation.

---

156 Judith Crosbie, *Commission Seeks External Advice on Internet Privacy* (2009, April 28), http://www.europeanvoice.com/article/2009/04/commission-seeks-external-advice-on-internet-privacy/64717.aspx (last visited on 29 April 2012).

157 CSO The Source For Security Executives, *e-Crime Congress Survey Reveals Jail Sentence for CEO a Fitting Punishment for Data Breach* (9 April 2009), http://www.cso.com.au/article/211736/e-crime_congress_survey_reveals_jail_sentence_ceo_fitting_punishment_data_breach (last visited on 29 April 2012).

158 See: Jeffrey D. Clements, *Corporations Are Not People: Why They Have More Rights Than You and What You Can Do About it* (Berrett-Koehler Publishers, Inc ed. 2012). Thom Hartmann, *Unequal Protection: The Rise of Corporate Dominance and the Theft of Human Rights* (Rodale ed. 2002). Robert G. Kaiser, *So Damn Much Money: The Triumph of Lobbying and the Corrosion of American Government* (Alfred A. Knopf ed. 2009). Lawrence Lessig, *Republic, Lost: How Money Corrupts Congress - and a Plan to Stop It* (Twelve - Hachette Hook Group ed. 2011).

7.12 United Kingdom Critique

The legal system access structure in the UK is different from that in CA, AU, and the US. The UK has a "loser pays" rule in trial and appellate cases. Under this rule, the losing party pays the attorney's fees for the side that wins. Therefore, those parties that have limited resources were less likely to pursue legal recourse against more powerful forces. Those with financial resources are not discouraged from litigating for more power. The system raises the cost of litigation for everyone.[159] The UK system makes it much harder for individuals to litigate for DPSIP rights.

The UK approach to DPSIP legal issues shares some strength of the EU Directives. The UK law shares some basic operational definitions and standards for dealing with sensitive information. The approach, despite some parliamentary and judicial evasion, has improved awareness of DPSIP concerns and interests in the UK. The approach provides a measure of good—if not best—practices. The standards provide some flexibility and are technologically neutral. In theory, the UK approach makes it easier to transfer data within the EU community. International data transfers are limited by EU, economic, and political factors outside of the UK powerbase.[160] The approach provides a registration income stream to help cover administrative costs. The system provides for a strict liability standard for subject access.[161]

While the UK has passed some privacy and data protection legislation with some regulatory controls, the population is concerned about the effectiveness of the current system. The latest research data was compiled in 2008 by the

---

[159] Barrington Moore, Jr*, Privacy: Studies in Social and Cultural History* (M.E. Sharpe, Incorporated. 1984); Herbert M. Kritzer, *Loser Pays Doesn't*, Legal Affairs. (2005, November), at http://www.polisci.wisc.edu/~kritzer/Research/Law_misc/LegalAffairs2005.pdf (last visited on 20 August 2012).

[160] Research approach support can be found at Neil Robinson, et al., *Review of the European Data Protection Directive*, (Rand Europe ed. 2009).

[161] See David Bainbridge & Graham Pearce, Tilting at Windmills - Has the New Data Protection Law Failed to Make a Significant Contribution to Rights of Privacy, 2000 *Journal of Information, Law and Technology* 2, (2000).

Information Commission Office.[162] The data revealed a number of concerns regarding how data is handled by governmental and private bodies. These concerns will be illustrated by means of a table.

Table 7.1 Concern with Regard to Organizations using Personal Information

Concerns	2005	2006[163]	2007	2008[164]
Passing or selling information on to other organizations without your permission	85%	95%	94%	95%
Not keeping the information securely so it is at risk of being stolen or getting into the wrong hands	85%	94%	94%	96%
Passing your information on to other countries without adequate data protection	85%	93%	94%	95%
Not collecting information in a secure way	83%	93%	94%	95%
Using information for purposes other than that for which is intended	84%	92%	n/a	n/a
Requesting too much personal information	77%	88%	88%	89%
Holding inaccurate or out-of-date information	74%	88%	87%	89%
Requesting inappropriate information that is not relevant	72%	83%	83%	83%
Holding information for longer than is required	69%	83%	84%	84%
n/a = question not asked based on regrettable researcher's decision in not addressing the issue in later studies				

---

162 Social and Market Strategic Research, *Report on Information Commissioner's Office Annual Track*, (Author ed. 2006). See also Peter Bradwell, *Private Lives: A People's Inquiry Into Personal Information,* Demos. (2010), at http://www.demos.co.uk/files/Private_Lives_-_web.pdf?1269213706 (last visited on 5 September 2012).

163 *Id.* at § 4.2.22, p. 17.

164 Social and Market Strategic Research, *Report on Information Commissioner's Office Annual Track*, (Author ed. 2008), 18.

The above data, provided by an independent research organization funded by the Information Commissioner's Office, reveals two progressive trends and interpretations. The first trend is that UK subjects are showing increased DPSIP concerns. The second interpretation suggests that the current set of UK laws and regulations is not meeting citizens' expectations and concerns. With the exception of "Requesting inappropriate information that is not relevant," which has held at eighty-three percent, all of the areas of concern are increasing over time. Bruce Schneier, the British Telecom's Chief Security Technology Officer, clearly identified the risks of not addressing DPSIP issues.[165] The risks are related to the individual who is an organizational stakeholder and included abuse of personal information, damage, loss of data controls, and misuse. The organizational costs include monetary costs due to compensation claims and regulator enforcement actions. The organization can be seen as a privacy threat, experience a loss of good will, and suffer economic losses.

The UK current privacy acts fail to adequately address the complex DPSIP issues related to the media exception. To be fair, the Data Protection Act of 1998 was written prior to the widespread use of current computer technology; the law has not kept pace with technology. However, the act does provide for special exceptions for artistic, journalistic, and literary purposes. The provisions make it difficult for data subjects to seek redress for violations. The act provides a major difference between wider public interests and a mere public interest story, the later is subject to more DPSIP controls. The law allows data controllers to claim a special purpose, even when the claim has no justification or merit. In *Campbell v. MGN, Ltd.*[166] Lord Phillips referred to Justice Moreland's comment in finding for Campbell. Lord Phillips wrote, "He (Morelad) described his path to this conclusion as weaving his way through a

---

[165] Bruce Schneier, *The Tech Lab: Bruce Schneier* BBC News. (2009), at http://news.bbc.co.uk/2/hi/technology/7897892.stm (last visited on 26 February 2012).

[166] *Campbell v. MGN Ltd.*, [2004] UKHL 22 (6 May 2004) [2004] UKHRR 648, [2004] 2 AC 457, [2004] EMLR 15, [2004] UKHL 22, 16 BHRC 500, [2004] 2 WLR 1232, [2004] HRLR 24, [2004] 2 All ER 995, (2004) at 72. (UK)

thicket, and the Act is certainly a cumbersome and inelegant piece of legislation."[167]

The UK system is difficult to change and keep updated, even when other nations are changing DPSIP legal standards and technology is advancing. The UK system makes it difficult to reasonably address evolving issues like breach notification, control of cookies, data mining, length of data retention, and opt-out versus opt-in standards. The structure makes it difficult to confront such issues. Industry codes of conduct are voluntary and are not allowed to be used as a standard in litigations. The ICO has worked to advance the concept of Privacy Impact Assessments (PIA). The office has published a valuable handbook on the issues and the standards of processing DPSIP issues.[168] The standards include initial assessment, full-scale PIA, small-scale PIA, privacy law compliance checks, and data protection checks. As part of an education and compliance program the office has also published privacy notice codes of practice.[169]

The UK adoption of PIA standards has been slow. Advocates are just starting to suggest following the CA PIA advocacy along with CA privacy by design efforts. The government and the private sector have chosen to ignore a classic international study on PIA effectiveness.[170] Few private or public PIA reports have reached the public domain. The UK system does not require any formal review by an independent source for private or public organizations. The UK PIA system is inconsistent in technical process, reporting, and result publications.[171]

---

167 *Ibid.*

168 Information Commissioner Office, *Privacy Impact Assessment Handbook*. (2009), at http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/html/0-advice.html (last visited on 6 October 2012).

169 Information Commissioner Office, *Privacy Notices Code of Practice.* (2009), at http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/privacy_notices_cop_final.pdf (last visited on 6 July 2012).

170 Adam Warren, et al., Privacy Impact Assessments: International Experience as a Basis for UK Guidance, 24 *Computer Law & Security Report* 3, 233 (2008).

171 *Ibid.*

The UK government, much like the US federal government, has not been compliant with international DPSIP standards. CA, many members of the EU, and some states in the US are advancing DPSIP legal and regulatory protection standards. The UK government did not establish an independent regulatory body;[172] therefore, it passively established the limited role and reporting structure of the commission.

The UK government did not want to pay the cost for a DPSIP legal and regulatory agency; therefore, it established a system of registration fees. Some have criticized the approach as bureaucratic.[173] The approach does require those that are in the information industry and potential violators help to pay regulatory costs. From an economic perspective, this makes some sense; however, it is inconsistent with other areas of legal risk. For example, intellectual property holders do not pay an ongoing fee to protect their rights. Given that the commission has little enforcement powers, the approach is limited. Those that refuse to register have few economic or legal disincentives. The database of registered holders must be carefully protected or the entire scheme becomes a major breach potential—similar to breaches during WW II in Europe and the US.[174]

Provided that such an approach was truly independent and the commission had true enforcement powers, the approach would create a valuable property right in that it would require compliance to the Data Protection Act to maintain the right to continue in the industry. A violation that would suspend the required registration or proposed license would be an incentive to maintain high-level practices and standards. From a social contract and corporate social responsibility perspective, the approach makes sense. From an economic checks and balances perspective, the approach makes sense. From a legal perspective, since those that create an attractive nuisance or

---

[172] The ICO is accountable to the Parliament and is subject to political control. Even if the ICO is made accountable to the home office or attorney general, it would still be subject to political pressures.

[173] Ian J. Lloyd, *Information Technology Law,* 33 (Oxford University Press 5th. ed. 2008).

[174] See Chapter 8 for a full an analysis.

those that fail to comply with legal standards must cover the risk, it makes sense. From an interdisciplinary behavioral, economic, and legal perspective, the approach also makes sense.[175]

The UK government, like the US policy approach, prefers self-regulation and industry codes of practice. When such systems fail, the government must impose statutory standards. The legal policy problem is how long data is stored and what form the standards will take. The issue of behavioral advertising including opt-in or opt-out options continues to be an issue. The All Party Parliamentary Communications Group has recommended an opt-in approach.[176] The group also advocates that the current laws are a hodgepodge of complex and unclear directions. There is no clear, consistent, and effective privacy protection standard.

Compliance standards are low in practice - even twelve high-ranking ministers, including departmental secretaries, have been notified that they are not complying with the Data Protection Act, and that they may be prosecuted if the pattern of non-compliance does not cease.[177] The Home Office has also been found to have breached DPSIP laws. The incidence and costs of such breaches is increasing in the public and private sectors.[178] The UK law does not require automatic breach notification to subjects even for significant legal and regulatory reasons.

---

[175] See Richard H. Thaler & Cass R. Sunstein, *Nudge: Improving Decisions about Health, Wealth, and Happiness* (Yale University Press ed. 2008).

[176] All Party Parliamentary Communications Group, *Can we keep our hands off the net? Report of an Inquiry by the All Party Parliamentary Communications Group.* (2009), at http://www.apcomms.org.uk/uploads/apComms_Final_Report.pdf (last visited on 19 October 2012). The group is an open and independent organization of MPs and Lords from all political parties. The group encourages stakeholders to present evidence and testimony on communication issues. The stakeholders include the Government, Parliamentarians, industry, and consumer groups.

[177] Information Commissioner's Office, *Ministers breach Data Protection Act, Contractor UK*. (2008), at http://www.contractoruk.com/news/004075.html (last visited on 18 November 2012).

[178] Ponemon Institute, *United Kingdom 2009 Annual Study: Cost of a Data Breach.* (2010), at www.encryptionreports.com/download/Ponemon_COB_2009_UK.pdf (last visited on 7 February 2012).

Under color of authority, police officers have illegally violated Section 53 of the Data Protection Act for personal reasons. The fines ranged from £750 to £1,200 for violations. Christopher Graham, the Information Commissioner, argues that the low fines are not a deterrent. He argues for a two-year jail term for such behavior. He maintains that the shift is critical "if the law is to provide an effective deterrent against the illegal trade in personal data," which was "widespread and organized."[179]

Historically, the UK has acquiesced to business pressure brought about by special interest groups to establish and maintain opt-out provisions for DPSIP legal issues. The All Party Group[180] argument for a shift to an opt-in approach has had some results. The historic opt-out provisions of the Article 5(3) of the e-Privacy Directive for cookies changed focus. On 19 December 2009, the provision was amended for a consent and opt-in provision.[181] The UK has not fully complied. The shift adds to the DPSIP debate. The shift is a positive sign that the UK may start addressing current DPSIP concerns.

Retrospective analysis of innovative responses to DPSIP legal and technological policies is inherently flawed. Legal, policy, social, and technological changes do impact DPSIP approaches. While the past can not be compared to the present, the data does provide insights into what is working and what is not.

While the focus on personally identifiable information (PII) was once innovative, the concept is now outdated, simplistic, and static. Many of the

---

179 Leo King, *Call for Data Jail Sentences after Police Wrongly Hand Over Sensitive Information: Information Commissioner Says Fines are not Effective as a Deterrent,* ComputerworldUK. (2009), at http://www.computerworlduk.com/news/it-business/17776/call-for-data-jail-sentences-after-police-wrongly-hand-over-sensitive-information/ (last visited on 30 November 2012).

180 The All Party Group is a UK group composed of all parties. See All Party Parliamentary Communications Group, *Can we keep our hands off the net? Report of an Inquiry by the All Party Parliamentary Communications Group*(2009), at http://www.apcomms.org.uk/uploads/apComms_Final_Report.pdf.

181 Chris Pulham, *United Kingdom: Prior Consent for Cookies - Amendments to the e-Privacy Directive, Mondaq: IT and Telecoms.* (2010), at http://www.mondaq.com/article.asp?articleid=104548 (last visited on 5 July 2012).

DPSIP legal standards are cumbersome, inconsistent, ineffective, and outmoded. The proportionality of business and governmental interests on the one hand versus consumer civil liberties - human rights and consumer protection on the other hand remains unclear. The UK government's response to DPSIP issues refused to grant the Information Commissioner's Office accountability, enforcement, and independent powers.[182] The approach is based on a technologically antiquated view of the real DPSIP issues. The ICO's lack of power is a major issue in the disagreement with the EU. EU pressure may force the UK to comply.

In contrast to CA, the UK is not taking an active role in business and technology privacy by design policies. The UK does not require the use of Privacy Enhancing Technologies (PET).[183] Thus, organizations do not purchase or use such technology. Since there is no clear market, developers do not actively research and develop enhanced – state-of-the-art technology. Large corporations (including Google, HP, Microsoft, and Oracle) lobby for less DPSIP regulation. However, the HP research lab in the UK has developed the HP Privacy Advisor software that encrypts cloud computing data.[184]

In the public and private sectors, the UK does not require the appointment of a Chief Privacy Officer. Where such an officer is appointed, the official does not have statutory personal responsibility and criminal liability for DPSIP violations. The abdication of such a responsibility strategy has no legal viability. The lack of a responsible officer weakens a checks and balances approach.

---

[182] See Neil Robinson, et al., *Review of the European Data Protection Directive*, (Rand Europe ed. 2009).

[183] The PET approach involves shifting DPSIP issues to include the principles of privacy by design.

[184] Kevin J. O'Brien, *Cloud Computing Hits Snag in Europe,* The New York Times. (2010), at http://www.nytimes.com/2010/09/20/technology/20cloud.html?_r=1 (last visited on 19 September 2012).

In determining the levy of DPSIP violation fines, the UK Financial Authority uses a standard set of principles. The authority considers prior compliance problems, disciplinary history, post-breach behavior, and the impact, nature, and seriousness of the breach.[185] The approach ignores the level of egregiousness of the behavior, number of persons affected, and the costs to stakeholders. The standards are not compressive, nor balanced.

Amy Barzdukas, Microsoft's Internet Explorer and Consumer Security Manager, reports that companies profit from consumer ignorance of privacy concerns. Firms are not clear or honest about how the data will be used. Business goals trump the law.[186] The UK must implement stronger DPSIP laws and implementation systems to address business behaviors. The UK Internet Advertising Bureau has established a number of protective Good Practices principles; however, the standards are self-regulating.[187]

The ICO is well aware of the above-noted problems. The Office issued an online code of practice to address some of the issues.[188] However, given the systemic constraints on the Office, the document does not reflect robust enforcement of laws or protections. The ICO reports that the Office is hampered by a systemic lack of support by the courts and parliament. The government rejects the concept of checks and balances by deferring to the special interests of businesses and newspapers. The unintended consequence is a reversal of historic legal protections and principles.[189]

---

185 UK Financial Services Authority, *Decision Procedure and Penalties Manual Release 070 Section 6.2* (2007), at http://www.fsa.gov.uk/pubs/hb-releases/rel70/rel70depp.pdf (last visited on 7 September 2012).

186 Phil Muncaster, *IE boss calls for more honesty about privacy,* V3.co.uk: All the latest UK technology news, reviews and analysis. (2009), at http://www.v3.co.uk/v3/news/2251656/ie-boss-calls-greater-honesty (last visited on 20 October 2012).

187 Internet Advertising Bureau, *IAB UK Unveils Good Practice Principles for Online Behavioural Advertising.* (2009), at http://www.iabuk.net/en/1/behaviouralbestpractice030309.html (last visited on 4 March 2012).

188 Information Commissioner's Office, *Personal Information Online: Code of Practice*, (Author ed. 2010).

189 Caroline Davies & James Robinson*, Information Commissioner's Office 'Let Down' Over Illegal Snooping, guardian.co.uk* (2009), at

The Joseph Rowntree Reform Trust issued a report noting several key issues with the DPSIP conditions in the UK.[190] Several months later, the government issued a response.[191] The government rejected the Trust report and argued that the current structure provides needed data protections and informed consent. The ministry rejected a recommendation that ECHR litigants should not have to pay court costs. The government maintains that there is no need to review or perform audits on the protection system. The ministry also rejected a recommendation for consent and database limitations. The government claimed that the report was confusing. A right to anonymous access to public services was seen as impractical. The ministry rejected a recommendation that the Chief Information Officer should be a permanent secretary reporting to the Chancellor of the Exchequer or Deputy Prime Minister.

The Chief Information Officer reports that the limited fines for data breaches currently in effect are insufficient. He cites police officers, private investigators, and governmental agencies who commit severe violations and receive low fines when detected. Commissioner Christopher Graham argues that the standard should be a maximum of two years in jail for violations.[192]

The UK approach does not provide adequate consent requirements and enforcement mechanisms. The national DPSIP authority is not legally and politically independent. Rather than intervening with any unlawful

---

http://www.guardian.co.uk/media/2009/sep/02/information-commission-illegal-phone-hacking (last visited on 2 September 2012).

190 Ross Anderson, et al., *Database State: A Report Commissioned by the Joseph Roundtree Reform Trust Ltd*. (2009), at http://www.jrrt.org.uk/uploads/Database%20State.pdf (last visited on 23 March 2012).

191 UK Ministry Of Justice, *Government Response to the Joseph Rowntree Reform Trust Report: 'Database State'*. (2009), at http://www.justice.gov.uk/publications/docs/government-response-rowntree-illegal-databases-report.pdf (last visited on 9 December 2012).

192 Leo King, *Call for Data Jail Sentences after Police Wrongly Hand Over Sensitive Information: Information Commissioner Says Fines are Not Effective as a Deterrent*, Computerworld UK (2009), at http://www.computerworlduk.com/news/it-business/17776/call-for-data-jail-sentences-after-police-wrongly-hand-over-sensitive-information/ (last visited on 27 November 2012).

interception, the UK approach only addresses intentional interceptions. The consent requirement in the UK is not based on an informed, freely given basis, and does not include a specific purpose standard.[193]

The ICO has attempted to increase enforcement with little results. Attempts at increasing the deterrence effect of increased enforcement have been ignored. Limited powers to audit private firms are ignored because there are no consequences.[194] The ICO published a Code of Practice but it is basically advisory.[195] When British Telecom was caught illegally using tracking software without notice of the practice or clear consumer consent, there was no consequence. The company said that it would stop the practice.[196] Perhaps the European Court of Justice can force the UK into compliance.

The current approach can not effectively respond to threats to data that is endlessly amended, collected, enriched, exchanged, and reused. The approach ignores the reality that personal information is the currency and focus in the information and Internet economy.[197]

The UK must strengthen its DPSIP approach. A privacy impact assessment should be required for all legislation, legal protections, and technological developments. Current legislation must be refined. Data subjects should

---

193 Pinsent Masons, *Commission Takes UK to Court Over Alleged Privacy Law Failings, Out-Law.com.* (2010), at http://www.out-law.com/page-11409 (last visited on 30 September 2012). See also Europa, *Digital Agenda: Commission Refers UK to Court Over Privacy and Personal Data Protection*. (2010), at http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/1215&format=HTML&aged=0&language=EN&guiLanguage=en (last visited on 30 September 2012).

194 Dan Worth, *ICO Wants Power to Bang Up Data Protection Offenders: Privacy Watchdog Also Wants Greater Authority to Investigate Company Procedures,* V3.co.uk. (2010), at http://www.v3.co.uk/v3/news/2271081/ico-outlines-desire-increased (last visited on 6 October 2012).

195 Information Commissioner's Office, *Personal Information Online: Code of Practice*, (Author ed. 2010).

196 Pinsent Masons, *Commission Takes UK to Court Over Alleged Privacy Law Failings,* Out-Law.com. (2010), at http://www.out-law.com/page-11409 (last visited on 30 September 2012).

197 Angel Gurría, *Closing Remarks by Angel Gurría, OECD Ministerial Meeting on the Future of the Internet Economy*. (2008), at http://www.oecd.org/document/8/0,3343,en_2649_34487_40863240_1_1_1_1,00.html (last visited on 7 September 2012).

have control over their personal data. Ownership should not automatically transfer to others since such data is an extension of the data subjects. People must know what personal data is held and used by commercial and governmental sources. Data subjects should have remedies when data is leaked, lost, or misused.[198] Any damage, emotional distress, or loss of reputation, or costs incurred by the data subject should be recoverable.[199] The approach should follow the mandatory breach notification process established by several states in the US.[200]

The UK approach to DPSIP legal issues is caught between the proverbial rock and a hard place.[201] The UK is being pressured, and a case has been submitted to the European Court of Justice for non-compliance to EU standards. On the other hand, a group of businesses wants profits and complete control at any cost, and many parliamentarians do not want to offend backers. The judiciary is recalcitrant and does not accept DPSIP legal principles as a consumer and human right, despite international agreements. The ICO is not independent and is essentially ineffectual; however, attempts to meet international standards while dealing with antiquated and non-compliant EU legal standards are laudable.

Although some may argue that language is a technicality, part of a legal analysis does relate to language and definitions. At the time, bifurcating sensitive and non-sensitive data made sense. The distinction is no longer viable as having non-sensitive data can lead to sensitive data on almost any data subject. Modern technology can address the letter of the law but not the

---

198 See Henry Porter, *My Ideal Queen's Speech,* guardian.co.uk. (2010), at http://www.guardian.co.uk/commentisfree/henryporter/2010/may/05/ideal-queens-speech-manifesto-club (last visited on 5 May 2012).

199 Warwick Ashford, *Mandatory Data Breach Notifications: An Opportunity For Change,* Computer Weekly. (2010), at http://www.computerweekly.com/Articles/2010/07/21/242043/Mandatory-data-breach-notifications-an-opportunity-for.htm (last visited on 20 July 2012).

200 California established the first breach notification law. The statute requires that when an organization experiences a data breach, it must notify all stakeholders including data subjects. Failure to comply is an infraction.

201 A slang term for being damned if you and damned if you do not. Both the rock and hard place provide considerable pressure.

spirit. Current data mining techniques can meet the legal standard and subvert the spirit of the law. Personal data must be viewed in context. DPSIP laws must not only address current technological practices but must also protect against future developments and practices. The current definition of personal data is inadequate and conflicts with EU standards. Case law and technological developments make old definitions unhelpful and inefficient. A lack of clarity creates a burden for all stakeholders. The law must address new forms of identification and technology-related behavior.[202]

The ICO filed a response to a request for evidence issued by the Ministry of Justice. The report shows that the collection and use of personal information is increasing faster than ever before; breaches and misuse are increasing; DPSIP legislation and regulation are more needed and relevant than ever, and more effective approaches are needed.[203]

The ICO's recommendation is that a new approach must meet a number of standards. The legal standards must be clear and address new forms of identification; they must protect individual freedoms and rights; and individuals must have clear, effective, and simple rights. The process must be cost-effective with clearly defined and accessible procedures that provide protection and vehicles of redress. The standards for processing must cover the entire information life cycle ensuring accountability and responsibility. Obligations must focus on risks rather than categories. Protections must focus on direct and indirect identification methods. Consent standards must be improved. Exceptions need checks and balances. The government must establish privacy by design principles for manufacturers and service providers that are enforced. Governments should not grant intellectual property protections for goods and services that are inherently privacy violations. The

---

202 Pinsent Masons, *ICO Urges Clarity on Definition of Personal Data,* OUT-LAW News. (2010), at http://out-law.com/page-11422 (last visited on 6 October 2012).

203 Information Commissioner Office, *The Information Commissioner's Response to the Ministry of Justice's Call for Evidence on the Current Data Protection Legislative Framework.* (2010), at http://www.ico.gov.uk/upload/documents/library/data_protection/notices/response_to_moj_dpframework.pdf (last visited on 6 October 2012).

historic distinction between data controllers and data processors fails to address current collaborative efforts. The current journalism and artistic exception cannot relate to individual Internet behavior. DPSIP legislation and regulation must address potential adverse effects, damages, discrimination based on data, and distress risks. Privacy protections are needed for behavioral advertising and electronic health records violations. Contrary to some claims, DPSIP laws and regulations are not in place to burden business. Only seven percent of businesses studied adopted a contrary view.[204]

The concept of consent and informed consent must be clear and include a description of the lawful and specified purpose of data collection with a contractual guarantee that the purposes are adequate, not excessive, and relevant. The Act needs to support the DPSIP principle of informational self-determination.

7.13 Summary of United Kingdom Literature and Issues Reviewed

The intent of this thesis is to conduct a comparative analysis of DPSIP responses in five different nations. Part of the comparison uses a benchmark approach of key issues. The issues include legal support of DPSIP protections, legal support of corporate privacy and data protection standards, information privacy data protection and security declarations, the use of regulatory agencies, sectoral legislation, and data controllers. The benchmark standards also include data processor requirements, data subjects, data security destruction, cross-border data flow, exemptions and exceptions, and the current stage of the approach based on evolutionary stages. The following table presents the summary based on the benchmark model.

---

[204] *Ibid.*

Table 7.2 Comparative Model of United Kingdom Legal Support of DPSIP Models

ISSUE DESCRIPTION	UK CURRENT RESPONSE
CM.1: Legal Support of DPSIP Protections	
Signatory, Adheres, and/or Complies with International Human Rights Standards	(See Appendix A)
Signatory, Adheres, and/or Complies with EU DPSIP Standards	Yes
Signatory, Adheres, and/or Complies with APEC DPSIP Standards	No
Federal Constitutional Law	No
Federal Legislative Efforts	Yes
Federal Common Law	Limited
Province / State Constitutional Law	No
Province / State Legislative Efforts	Limited
Province /State Common Law	Some

CM.2: Legal Support of Corporate Privacy and Data Property Protection Issues	**UK CURRENT RESPONSE**
Copyright Protections	Yes
Database Protection	Yes
Patient Protections	Yes
Service Mark Protections	Yes
Trade Mark Protections	Yes
Trade Secret Protections	Yes
Privacy Impact Audit Required Before Use	No
Privacy Impact Audit Required Before Government Protections Granted	No
Checks and Balances on Corporate Collection, Use, and Transfer of Individual DPSIP Data	Yes

CM.3: Information Privacy – Data Protection and Security Declarations	**UK CURRENT RESPONSE**
Definitions Provided	Yes
Personal and Sensitive Data	Yes

Defined	
Definitions Effectively Address Advanced Data Mining Technologies	No
All Holders and Users Held Accountable	No

CM.4: Regulatory Agency	UK CURRENT RESPONSE
Independent of Legislative and Executive Branches	No
Administrative Power	Yes
Investigative Power	Limited
Regulatory Powers	Limited
Education Function	Yes
Enforcement Powers	Limited
Structure	Yes
Responsibilities Defined	Yes
Accountability	Yes
Governmental Chief Privacy Officer/ Commissioner Required	Yes
Governmental Privacy Audits Required as Part of Legislation Passage	Limited
Business Chief Privacy Officer/ Commissioner Required	Suggested
Employees are Personally Liable for Violations	Limited
Business Privacy Audits Required	No
Agency Educational Function	Yes

CM.5: Sectoral DPSIP Legislation	UK CURRENT RESPONSE
Credit Reporting Agencies	Yes
Criminal Justice Record Restrictions	No
Health Information	Some
Health Information Exceptions	Some
Electronic Medical/Health Record Controls	Some

CM.6: Data Controllers	UK CURRENT RESPONSE
Notice Required	Limited
Opt-in	No
Opt-Out	Generally

Must Be Lawful and Fair	In theory
System Access Controls	In theory
Data Quality and Integrity	In theory
Accurate	In theory
Complete	In theory
Up to Date	In theory
Limited to Needed Data	In theory
Relevant	In theory
Not Misleading	In theory
Data Retention Limitation	Limited
Data Transfer Controls	Yes
Openness on Information Held	Limited
Breach Disclosures Required	No
Breach Penalties	Limited

CM.7: Data Processor Requirements	**UK CURRENT RESPONSE**
Informed Consent Required	In theory
Rationale is Provided	Yes
Fair Processing	Yes
Legal Processing	Yes
General Data	Yes
Sensitive Data	Yes
Accuracy	Yes
Timely	Yes
Duration of Record Keeping Controls	Limited

CM.8: Data Subjects	**UK CURRENT RESPONSE**
Ownership by the Subject	Limited
Control Over Access	Limited
Alter, Amend, Correct, and Delete Errors	Limited
Notification Requirement	Limited

CM.9: Data Security and Destruction	**UK CURRENT RESPONSE**
Security Must be State of the Art	Generally
Technology Use – Cost of Implementation Not a Defense	No
Tracking	Not once merged
Safeguards Required	Adequate encryption
Protects From Alteration	Yes
Protects Against Disclosure	Yes
Protects Misuse	Yes
Protects Against Unauthorized	Yes

Internal and External Access	
Unauthorized Access Penalties	Yes
Timely Notice of Breaches	Limited
Strong Remedies Provided	Limited

CM.10: Cross-Border Data Flow	**UK CURRENT RESPONSE**
Individual Informed Consent Required	Yes
Transfer Source Is Accountable	Limited
Outsource Service Controls	Limited

CM.11: Exemptions and Exceptions	**UK CURRENT RESPONSE**
Only Permitted Where Compelling Justification Exists	Yes
Checks and Balances – Court Order Required	Limited
Government Agencies	Yes
Intelligence and Defense	Yes
Police Actions	Yes
Small Business Exemption	No

CM.12 DPSIP Evolutional Stages	**UK CURRENT RESPONSE**
DPSIP.0 Limited DPSIP legal Issues	Yes
DPSIP.1.0 Establishes PII; does not fully address security issues; focus on limited legal consent and notice.	Yes
DPISP.2.0 Accepts PII standards; does not fully address security issues; focus on a legally based harm based analysis.	Yes
DPSIP.3.0 PII and non-PII data fused; privacy, data protection and security issues are interrelated; legal audits, checks, and balances needed for all personal information stakeholders. New technologies are required to pass privacy audits (example – RFID, Internet of Things) and require use of privacy enhancing technologies in all new IP approvals.	No

Chapter Eight addresses the actual and potential US approach options to DPSIP legal issues. The US has advanced some basic principles of DPSIP, civil rights, and human rights; however, it has failed to raise these principles to the current international level of concern. Although the US claims to be and is often seen as a leader of the Western World (including in technology development), in terms of DPSIP legal issues, it is a recalcitrant follower. The approach in the US reflects its shift from a representative republic to a corporate republic that favors business interests over individual interests throughout a range of DPSIP legal issues. As of 2012, the US is considering adopting more DPSIP protections that are closer to the EU approach. The proposed shift has powerful critics.

CHAPTER EIGHT: DATA PROTECTION AND SECURITY LAW:

UNITED STATES OF AMERICA LEGAL STANDARDS

> *The real danger is the gradual erosion of individual liberties through the automation, integration, and interconnection of many small, separate record-keeping systems, each of which alone may seem innocuous, even benevolent, and wholly justifiable.* US Privacy Protection Study Commission[1]

8.0 Overview

Legal protection of data security and informational privacy in the US is a patchwork of administrative rules, laws, and cases. The culture highly values privacy; however, it also values the free flow of information, freedom of speech, independence, minimal laws and regulation, and transparency. More recently, free market and security rhetoric has played a major role in how the US is handling DPSIP legal issues.

Information privacy was not a significant issue during the early years of the US and the agricultural era, because of open lands and a lack of potentially intrusive information technology. Privacy was perceived as the right to protect one's home and land from searches and seizures. Privacy concerns increased with industrialization and the urbanization of the country. The amount of open spaces diminished and information privacy became a more prominent concern. The advent of computer technology raised the information privacy stakes higher. "Technological change precipitated a gap

[1] United States Privacy Protection Study Commission, *Personal Privacy in an Information Society* (U.S. Privacy Protection Study Commission. 1977), at 533.

in existing laws,"[2] and in the US, information privacy law developed in a haphazard manner.

Due to the enactment of the Bill of Rights, the US has a long history of protecting civil liberties. However, during some periods of fear and war, some human rights principles have been ignored. More recently, the US Federal Trade Commission (FTC) has advocated for privacy rights under strong consumer protection legislation. Despite the general push for consumer advocacy, the business community has not always acquiesced and more recently mounted a major political battle.

The US chapter begins with presenting background on the country. The analysis continues with an examination of the US Constitutional declarations. US federal legislation and case law is examined. The research then focuses on US State Constitutional declarations, state legislation, and case law. An analysis of the US standards and remedies, and implementation system is reviewed. US sociolegal concerns are presented. A critique of the US approach is then addressed. A summary of the US literature and issues, using the thesis comparative model of the current legal support is then reviewed and presented.

8.1 Background

The US is a constitutional republic.[3] The governmental model includes the executive, legislative, and judicial branches. The structure applies to the federal government and the fifty state governments. The federal executive branch is headed by the President, who is elected to a maximum of two terms consisting of four years each. The President is the Head of State, top federal government official, and commander-in-chief of the military. The President and Vice President are elected by the Electoral College based on public

---

[2] Priscilla M. Regan, Ideas or Interests: Privacy in Electronic Communications, 21 *Policy Studies Journal,* 3, 450 (1993), at 450.

[3] United States of America, *Find Government Agencies*. (2010), at http://www.usa.gov/ (last visited on 5 August 2012). Site contains reference data for this section.

elections. The chief executive for each state is publically elected as a Governor. The executive branch includes a number of departments and some independent agencies.[4]

The federal legislative branch includes the Senate[5] and House of Representatives.[6] The Senate provides advice and consent for presidential appointments and ratifies treaties. The House is responsible for revenue issues. Senators are elected for a six-year term; members of the House are elected for two-year terms. Once both bodies pass a bill, that piece of legislation is then sent to the President for signature or veto. All states, with the exception of Nebraska,[7] have a similar structure.

The federal judiciary is headed by the Supreme Court,[8] Federal Courts of Appeal, and Federal District Courts. The states follow the same pattern. The US Supreme Court is the highest court in the country. All federal judges are appointed to a lifelong term. The US judiciary generally follows the British common law tradition.

James Katz and Annette Tassone[9] studied privacy protection concerns in the US. The data showed that privacy was a strong cultural value; however, some people shared data without considering the consequences. This finding was consistent with psychological research on decision-making errors. The data demonstrated a strong possibility that privacy would be a greater issue in

---

4 United States of America, *The Executive Branch*. (2010), at http://www.whitehouse.gov/our-government/executive-branch (last visited on 5 August 2012).

5 United States of America, *United States Senate*. (2010), at http://www.senate.gov/ (last visited on 5 August 2012). Senators are elected for staggered six-year terms with two elected from each of the fifty states.

6 United States of America, *United States House of Representatives*. (2010), at http://www.house.gov/ (last visited on 5 August 2012). The House has 435 members who are elected for two-year terms. The number of members from each state is based on the census. A state must have at least one representative.

7 Nebraska has a unicameral legislature. The bi-cameral states have a Senate and Assembly.

8 United States of America, *Supreme Court of the United States*. (2010), at http://www.supremecourt.gov/ (last visited on 5 August 2012).

9 James E. Katz & Annette R. Tassone, Public Opinion Trends: Privacy and Information Technology, 54 *Public Opinion Quarterly* 1, 125 (1990).

the future. Although some subjects provided data to the requesting sources, they were often reluctant and not happy with the request or requirement. Many of the subjects thought that privacy protection issues were ignored. The data showed that eighteen percent of the subjects had been victims of privacy invasions. These levels of concern were higher than the earlier Louis Harris and Allen Westin[10] reported concerns.

Leading advocates of privacy rights existed even in the colonial period. Colonial courts established information privacy rights. The privacy-related issues included limiting defamation communications, government searches and seizures, and physical intrusions. The courts required hearings, protected privileged communications, and outlawed trespass of person and property.[11] While Benjamin Franklin was the Postmaster General, he established an information privacy policy. All postmasters had to swear that they would not "wittingly, willingly, or knowingly open or cause, procure, permit, or suffer to be opened . . . any letter or letters which shall come into their hands."[12]

John Adams, a signer of the Declaration of Independence and the second president wrote about the need for privacy rights and duties in his diary. He wrote that privacy must be maintained to "protect one from their enemies or indiscreet friends to do so is only wise."[13]

In 1890, Samuel D. Warren and the future Justice Louis D. Brandeis, published a major work on privacy in the US. They wrote that inventions and business models invade "the sacred precincts of private and domestic life."[14]

---

10 Louis Harris & Allen F. Westin, *The Dimensions of Privacy* (Sentry Insurance. 1979).

11 David H. Flaherty, *Privacy in Colonial New England* (University of Virginia Press. 1972), 248.

12 *Id.* at 121.

13 *Id.* at 5.

14 Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, 4 *Harvard Law Review* 5, 193 (1890) at 195.

The authors argued that freedom of the press did not exist without limitations.[15]

Warren and Brandeis also suggested remedies for right to privacy violations. The remedies included "1. An action of tort for damages in all cases. Even in the absence of special damages, substantial compensation could be allowed for injury to feelings as in the action of slander and libel. 2. An injunction, in perhaps a very limited class of cases."[16]

Years later, President Gerald R. Ford presented himself as a strong DPSIP leader. He was instrumental in enacting the 1974 Privacy Act which limited sources of violations used during the Nixon years. However, President Ford rejected the part of the original Act that established a national data-protection-commission.[17] Ford used a classic political move to kill the proposal by getting Congress to agree to a Study Commission.[18] In his October 9, 1974, statement regarding the Privacy Act, he declared that executive and legislative actions are needed to improve the levels of confidentiality and privacy rights, especially related to criminal justice records, income tax records, and other identified privacy concerns. However, the right to privacy committee achieved minimal accomplishments.[19]

The DPSIP standards in the US are a complicated and often conflicting set of various state and federal laws and related Court decisions. The standards, much like anti-trust enforcement, depend on which administration and court appointees are in power. Although public opinion polls in the US consistently

---

15 *Id.* at 196-197.

16 *Id.* at 197.

17 David H. Flaherty, *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States* (University of North Carolina Press. 1989), 305.

18 Under Robert's Rules of Order, if one wants to stop a legislative action, one refers it to a committee for study.

19 Ford Library Museum, *President Gerald R. Ford's Statement on Privacy Legislation*. (2001), at http://www.fordlibrarymuseum.gov/library/speeches/740125.htm (last visited on 31 July 2012), at 7.

favor privacy protections, special interests groups[20] have passed legislation in favor of self-regulation. Generally, recent conservative governments wanted to limit the enforcement of laws and regulations to increase corporate power. Business interests wanted to be free to make more money, no matter what legal and policy interests existed. Starting with President Clinton, the official US privacy policy has been self-regulation. "Americans treasure privacy, linking it to our concept of personal freedom and well-being."[21] The Clinton administration wanted consumer-friendly fair information practices. However, the Administration chose not to involve the government in the effort.[22]

8.2 United States of America Constitutional Declarations

The Constitution of the US[23] does not specifically delineate a privacy right. At the time of the original writing, privacy was taken for granted and was not a major issue due to geography, population, and self-evident truths. The constitutional basis for DPSIP concerns came in the twentieth century and was based on a number of provisions of the Bill of Rights.

The First Amendment proclaims that the government cannot interfere with the "right of the people peaceably to assemble."[24] In 1958, the US Supreme Court identified the First Amendment as the basis of the relationship between speech and privacy. Alabama wanted access to the private membership list of the state NAACP organization. In *NAACP v. Alabama,*[25] Justice Harlan found that the Court "has recognized the vital relationship between

---

20 On both sides of the political spectrum – including conservatives to progressive.

21 William J. Clinton & Albert Gore, *A Framework for Global Electronic Commerce*. (1997, July 1), at http://www.w3.org/TR/NOTE-framework-970706.html (last visited on 1 August 2012), § 5 ¶ 1.

22 *Id.* at ¶ 10.

23 United States Constitution, *United States Constitution.* (1788), at http://www.kearney.net/~tclayton/The%20Constitution%20of%20the%20United%20States.htm (last visited on 4 July 2012). (US)

24 *Id.* at amend. I.

25 *NAACP v. Alabama*, 357 U.S. 449, 462, 78 S. Ct. 1163, 2 L. Ed. 2d 1488, (1958), 462. (US)

freedom to associate and privacy in one's association particularly where a group espouses dissident beliefs."[26]

The Supreme Court then ruled as unconstitutional another state of Alabama law on privacy grounds using the First Amendment. The law required that all public school teachers release private information related to group memberships and organizations that the teachers supported.[27] These cases show the danger of individuals losing control over their personal information and that the general public does not always have a right to know or even have a realistic public interest.

In *Griswold v. Connecticut*,[28] US Supreme Court Justice William O. Douglas, writing for the majority, found a constitutional right of privacy – a "penumbra" of rights associated with the First, Third, Fifth, Ninth, and Fourteenth Amendments. The case involved a statute that outlawed the use of contraceptives. The Court ruled that the Amendments created a "zone of privacy created by several fundamental constitutional guarantees."[29]

The Third Amendment prohibits the government from having soldiers "quartered in any house, without the consent of the owner."[30] The Fourth Amendment declares that "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated."[31]

In *Olmstead v. United States*, [32] Justice Brandeis argued in dissent, that "the right to be let alone was the most comprehensive constitutional right."[33] In

---

[26] *Ibid.*
[27] *Shelton v. Tucker*, 364 U.S. 479, (1960). (US)
[28] *Griswold v. Connecticut,* 38 1 U.S. 479, 85 S.Ct. 1678, 14 L.Ed.2d 510, (1965). (US)
[29] *Id.* at 500.
[30] U.S. Const. amend III.
[31] U.S. Const. amend IV.
[32] *Olmstead v. U.S.,* 277 U.S. 438, 478 S. Ct. 564. 66 ALR 376, 72 L.Ed. 944, (1928), 475-478. (US)
[33] *Ibid.*

Goldman v. United States,[34] a case on telephonic privacy invasion, Justice Murphy warned that modern technology had developed means of privacy invasions not foreseen by the Constitution under the Fourth Amendment. The Supreme Court thought so much of the need for privacy protection that it found constitutional protections. In *Mapp v. Ohio*,[35] the Supreme Court established the exclusionary rule, which made unlawful searches inadmissible. The Court determined that privacy cannot be an "empty promise."

The Fifth Amendment declares that no person shall be "deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation."[36] The Ninth Amendment further declares that "The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people."[37]

In *Griswold v. Connecticut,*[38] US Supreme Court Justice Arthur Goldberg, with Chief Justice Warren and Justice Brennan joining and concurring argued that privacy was an un-enumerated right under the Ninth Amendment. To determine if such a right exists, Justice Goldberg argued that one "must look to the tradition and conscience of our people . . .the totality of the constitutional scheme under which we live."[39]

The Tenth Amendment, and last of the Bill of Rights, declares that legal protections are not limited by the text. The Amendment declares that *"The powers not delegated* to the United States by the Constitution, nor prohibited by it to the states, *are reserved* to the states respectively, *or to the people."*[40]

---

[34] *Goldman v. United States*, 316 U.S. 129, 138, (1942), 138. (US)
[35] *Mapp v. Ohio*, 367 U.S. 644, (1961), 644. (US)
[36] U.S. Const. amend V.
[37] U.S. Const. amend IX.
[38] *Griswold v. Connecticut*, 494. (US)
[39] *Ibid.* (emphasis added)
[40] U.S. Const. amend X.

The Fourteenth Amendment guarantees that the federal bill of rights provisions applied to the states. The Amendment declares, "*nor shall any state deprive any person of life, liberty, or property, without due process of law."*[41]

The finding for a right to privacy in the Constitution was not always a partisan effort. Republican President Richard Nixon appointed Chief Justice Warren Burger in 1969. In *Richmond Newspapers v. Virginia,*[42] Chief Justice Burger ruled that the Constitution does provide for privacy protections as unarticulated, implicit, enumerated, and indispensably guaranteed.

While the US Constitution did not specifically identify a clearly defined DPSIP legal right, the document did provide a legal basis for protections. The Supreme Court has used the above Amendments as the basis for DPSIP cases.

8.3 United States of America Federal Legislation[43]

Over the years, the Federal government enacted a number of Acts that addressed selected DPSIP problems. Some state governments have followed the same pattern. In some situations, the states have been more innovative at privacy problem resolutions. This section reviews a number of laws and some related court decisions. In general, the materials are in chronological order in order to clarify the developmental aspects of the issues. The US has a long history of passing legislation to meet immediate challenges. When situations change, the legislation is then repealed, changed, ignored, or not funded. DPSIP issues are no exception.

---

41 U.S. Const. amend XIV. (emphasis added)

42 *Richmond Newspapers v. Virginia*, 448 U.S. 555, (1980), 578. (US)

43 The legislation includes all of the sections noted in this 8.3 section.

8.3.1 Federal Trade Commission Act of 1914

The Federal Trade Commission Act, signed by President Woodrow Wilson, established the trade commission and granted it power to investigate and enforce actions against "unfair or deceptive acts or practices in or affecting commerce."[44] The commission was empowered to issue cease-and-desist orders and levy fines for violating the Act. The power of the commission was expanded to include commercial e-mail, competition, consumer protection, the Internet, privacy, and spam. The FTC was slow to enforce the expansion.[45]

8.3.2 The Federal Wiretap Act of 1968

In 1968, the federal Congress passed Title III of the Omnibus Crime Control and Safe Street Act of 1968 (Wiretap Act).[46] The Act applied only to contents of telephone communications, hidden microphones, and did not control the use of pen registers for tracking contacts. The statute did require law enforcement to obtain a judge-issued warrant, based on probable cause, to wiretap phone conversations. The Act set standards of probable cause for issuing a warrant.[47] The Act and subsequent court actions established three principles of exception for telephone companies and their employees. Telephone companies do not need subscriber's consent to monitor. Companies can monitor for measuring rendition of services and to protect company rights and property.[48] The Act allows for a private right of action and allows for liquidated damages.[49] The Act allows for criminal penalties,

---

44 *Federal Trade Commission Act*, 15 U.S.C. § 41 (1914), § 45(a)(1). (US)

45 See § 8.4.1 in this document.

46 *Omnibus Crime Control and Safe Streets Act of 1968*, Pub. L. No. 90-350, 82 Stat. 197 (codified as amended at 18 U.S.C. § 2511-2520) (1968). (US) AKA Federal Wiretap Act of 1968

47 *Id.* at § 1.

48 *Id.* at § 2511(2)(a).

49 A private right of action allows an individual to litigate. Statutes with liquidated damages do not require proof of actual damages.

punitive damages, and equitable remedies. The Act does not preempt state laws.[50]

In *United States v Auler*,[51] the Federal Court of Appeals found that a telephone company was recording the content of conversations under the pretense of investigating service theft issues. The issue before the Court was one of monitoring content information. The Court determined that restricted monitoring of non-content information, by the phone company, might fit within the exception to the need to protect consumers' right to privacy.

In *Deal v Spears,*[52] the Court of Appeals again ruled on the issue of consent under the Act. Under the ruling, consent that is implied is not a legal violation of the "reasonable expectation of privacy test (or) a test of constructive consent."[53] In response, the states of California, Connecticut, Florida, Illinois, Maryland, Massachusetts, Michigan, Montana, Nevada, New Hampshire, Pennsylvania, and Washington passed laws requiring that all parties must formerly consent. The state laws voided the *Deal* ruling in these states.

8.3.3 The Fair Credit Reporting Act of 1970

Beginning during the Second World War, US merchants started collecting and sharing data on consumers' purchases and payments. Over the next twenty-plus years, the data became valuable and had a major impact on individual purchasing power.[54] Part of the problem was that the data was often incorrect. In 1970, the Fair Credit Reporting Act was enacted to require that collected data should be accurate and accessible, and to provide data

---

50 Preemption in a federal statute requires all states to follow the same way. The principle is used for the sake of uniformity and to limit state laws that might have a higher standard.

51 *United States v. Auler*, 539 F.2d 642 (7th Cir. 1976). (US)

52 *Deal v. Spears*, 980 F.2d 1153, 1157-58 (8th Cir. 1992), 1153. (US)

53 *Ibid.*

54 Federal Trade Commission, *The Fair Credit Reporting Act*. (2004), at http://www.ftc.gov/os/statutes/031224fcra.pdf p. 3. (last visited on 11 June 2012).

correction procedures. Business interest groups objected to passage of the Act and even recent enhancements.[55] The Act was to be administered by the Federal Trade Commission and State Attorney Generals.[56] The collected personal data could be used only for the legally established permitted purpose.[57] When organizations violated the law, private rights of action were also established by the Act. Civil and criminal penalties also applied.[58] Over and above actual damages, statutory damages also included fines for willful violations.[59]

The Act covered all entities that compiled consumer credit reports and entities that used these reports. Historically, a report included the consumers' name, address, social security number, credit worthiness, credit standing, credit capacity, and payment records. The original purpose of credit reporting was to serve consumers in establishing eligibility for credit. Over the past ten years, reporting companies have added character, general reputation, mode of living, and personal characteristics in investigative consumer reports. The credit bureaus justified the change in focus for the purposes of employment, insurance, or other business desires. The expansion was based on mutual market demand; however, the Act does provide some limitations and consumer recourse.[60] The US approach is far less protective than that used in AU.[61]

The Act required that when an adverse credit decision was made on the basis of one of the reporting agencies' data, the consumer must be informed. The

---

55 Emily Flitter, *Consumer Protection Debate Pits Theory Against Record*, American Banker. (2009), at http://www.americanbanker.com/issues/174_124/-383336-1.html (last visited on 23 June 2012).

56 *Fair Credit Reporting Act (FCRA), Public Law No. 91-508*. (1970), at http://www.ftc.gov/os/statutes/031224fcra.pdf (last visited on 3 July 2012). (US)

57 *Ibid.*

58 *Ibid.*

59 *Ibid*

60 *Id.* at § 1681.

61 See Chapter 4 § 4.3 of this study.

responsibility for correction was placed on the consumer.[62] Consumers had the legal right to request correction of any errors or dispute any data.[63] The data collector had a legal standard, but not a per se requirement to insure that the data collected was accurate, complete, and current. Business interests found a legislative way to circumvent strong DPSIP legal principles.

8.3.4 The Family Educational Rights and Privacy Act of 1974

The Family Educational Rights and Privacy Act of 1974 (FERPA)[64] was passed during the Nixon Watergate period because Congress determined a need for colleges and universities to maintain the privacy of student educational records. Senator James L. Buckley proclaimed that "the protection of individual privacy is essential to the continued existence of a free society. There has been clear evidence of frequent, even systematic violations of the privacy."[65]

The protected student records include personally identifying information, transcripts, disciplinary, and complaint data.[66] Prior to release of records, the student or parent must provide written permission.[67] The only exceptions include legitimate educational interests, regulatory audits, financial aid issues, accrediting agencies, judicial orders, lawful subpoenas, health or safety emergencies, and some directories.[68] The Act is enforced by potential withdrawal of all federal funds to the educational institution.[69] Campus law enforcement records were not considered to be educational records. Campus data on criminal

---

62 *Fair Credit Reporting Act (FCRA) at* § 1681(g).

63 *Ibid.*

64 *Family Educational Rights and Privacy Act (FERPA)* amend. 20 U.S.C. § 1232g; 34 CFR Part 99 (1974). (US)

65 James L. Buckley, *Joint Statement in Explanation of Buckley/Pell Amendment*, 120, Congressional Record, Record 13991, December 13, 1974 (1974), 13991.

66 *Family Educational Rights and Privacy Act (FERPA)* § 1232. (US)

67 *Id.* at § 1232g(b).

68 *Id.* at § 1232g(a).

69 *Id.* at § 1232g(f).

activities must be publicly released on an annual basis.[70] The act does not allow a private right of action or criminal penalties.

The federal courts have ruled that student disciplinary records, that include personally identifying information, were educational records and could not be released. Student disciplinary proceedings were not seen as criminal because the proceedings applied related only to students and their educational institutions.[71]

An issue in any DPSIP law is the willingness to enforce the standards. The FERPA standards are very clear; however, violations still occur. In Manassas Virginia, the City of Manassas School Board, the City, and the Police Department joined forces to use data mining programs and openly shared the data.[72] Although the Manassas decision was based on discrimination rather than privacy standards, the case does establish a concern regarding the use data mining procedures.

8.3.5 The Freedom of Information Act of 1974

The Freedom of Information Act[73] was passed to require the release of governmentally held information to private persons and organizations upon filing a request. Although the focus of the Act was on governmental transparency, the Act nevertheless provided for exceptions to accommodate internationally established data privacy issues. Section Six protected the release of medical, personnel, and related records. Section Seven protected

---

70 *Higher Education Amendments of 1992* amend. Public Law No. 102-325, § 1555(a), 106 Stat. 448, 840 (1992), 840. (US)

71 *United States v. Miami University*, 91 F.Supp.2d 1132, 1147 (S.D. Ohio 2000), 1157. (US)

72 Brigid Schulte, *Student Privacy Spotlighted in VA: Manassas School Board, City Pay in Discrimination Suit; Policies Tightened*. (2008, September 27), at http://www.washingtonpost.com/wp-dyn/content/article/2008/09/26/AR2008092603641.html?sid=ST2008092700733&s_pos= (last visited on 27 September 2012), B01.

73 *Freedom of Information Act*, amend. 5 U.S.C. sec. 552(b)(6)(7) (1974); see also U.S., *The Freedom of Information Act, 5 U.S.C. § 552*. (1966), at http://www.usdoj.gov/oip/foia_guide07/text_foia.pdf (last visited on 1 July 2012); U.S. *Freedom of Information Act of 2005*, 5 USC, 552 (2005). (US)

the release of criminal history records. Section Four protected private business information obtained through legal duties.

8.3.6 The Privacy Act of 1974

The US Privacy Act of 1974 was passed to protect individual private data from governmental misuse. The impetus for its passage was the events that occurred during the Nixon presidency.[74] The preface to the act declares that "the opportunities for an individual to secure employment, insurance, and credit, and his right to due process, and other protections are endangered by the misuse of certain information systems."[75]

The Privacy Act was classified as an "omnibus code of fair information practices" and was tied to the 1966 Freedom of Information Act. At the time of passage, considerable concerns existed related to governmental misuse of citizen data in computerized databases during the Nixon years.[76] The Act applied to how the Federal Government, federal entities, and contractors deal with information privacy issues.[77] Under the Act, most individuals could seek access to any federal agencies' records related to themselves.[78] The Act stated that information must be "accurate, complete, relevant, and timely" and allowed for accuracy challenges.[79] The Act required that information

---

[74] Nixon was the first US President to resign in lieu of impeachment. His resignation was prompted by advice by the Republican senate members that he would be impeached and found guilty of *high crimes and misdemeanors.* Nixon would have been found guilty for using governmental powers to physically break in and steal private information that today could be stolen by hacking; using the taxing authority to punish so called enemies, establishing surveillance of a governmental hit list of enemies; obstruction of justice, abuse of power; and contempt of Congress. All of the charges violated DPSIP principles.

[75] *Privacy Act of 1974*. 5 U.S.C. § 552(a)(4) (1974). (US)

[76] The issues are fully documented in Frank Church, Senate Select Committee to Study Government Operations with Respect to Intelligence Activities, 94th Congress, Final Report on Intelligence Activities and the Rights of Americans (United State Printing Office. 1976, April 26).

[77] *Privacy Act of 1974*. 5 U.S.C. § 552(a)(4) (1974), (US)

[78] *Id.* at § 552a(b).

[79] *Id.* at § 552a(d)(2)(B).

collected for one purpose could not be used for another.[80] The Department of Justice criticized the Act for "imprecise language, outdated regulatory guidelines," unpublished court decisions, and related unsettled issues.[81]

The Act required that governmental agencies and contractors could only compile data that was relevant and necessary. Any new governmental system of records must be publically announced. The right to individual data access must be respected by the government. The law provided for a private right of action.[82] Civil and criminal penalties were applicable for federal agencies and employees.[83]

During the political discussions between Congress and the newly appointed president, Gerald Ford, who succeeded Nixon, the enforcement of the Act was moved to the Office of Management and Budget (OMB), which was under the Executive branch's control. The intent of the Act was to report to Congress on Executive privacy protection dysfunction. The OMB prepared guidelines but never performed any enforcement actions.[84] The Privacy Protection Study Commission found that no agency or individual did anything to enforce the Act on the part of anyone.[85]

Despite the lack of enforcement, the Act had some laudatory basic goals:

> "(1) data is kept accurate, complete, up-to-date, and open to review and correction by the people concerned;

---

80 *Id.* at § 552a(e)(3)(B).

81 See U.S. Department of Justice, *Overview of the Privacy Act of 1974*. (2010), at http://www.justice.gov/opcl/1974intro.htm (last visited on 4 January 2012).; U.S. Congress Joint Committee on Governmental Operations, *Legislative History of the Privacy Act of 1974: Source Book on Privacy*. (1976), at http://www.loc.gov/rr/frd/Military_Law/pdf/LH_privacy_act-1974.pdf (last visited on 2 January 2012).

82 *Privacy Act of 1974*. 5 U.S.C. § 552(a)(4) (1974), (US)

83 *Id.* at § 552a(g)(1)(D).

84 House Committee on Government Operations, *Who Cares About Privacy? Congressional Report Number 455 of the 98th Congress* (Government Printing Office. 1983).

85 Privacy Protection Study Commission, *Personal Privacy in an Information Society*. (1977), at http://www.epic.org/privacy/ppsc1977report/ (last visited on 29 July 2012).

> (2) the uses of filed data must proceed according to rules of due process that data subjects can know and, if necessary, invoke; and
> (3) the organizations collecting and using personal data can do so only as is necessary to attain their appropriate organizational goals."[86]

Unfortunately, under the Act, information privacy data collection and use actually increased. The government instituted surveillance initiatives such as Carnivore, Clipper Chip, and Echelon[87] to circumvent the spirit and letter of the Privacy Act law.

The conservatives in Congress and the administration furthered their attack on information privacy with the rushed passage of the post 9/11, 2001 Patriot Act.[88] The Act essentially overturned all prior privacy legislation in the US. The traditional rule of law principles of checks and balances were gone. Sections 904 and 905 of the Patriot Act allowed US spy agencies and executive police to do what they want with no accountability to Congress or the courts.[89]

8.3.7 Privacy Protection Act of 1980

The Privacy Protection Act of 1980[90] protected computer information systems and journalists from the police wanting to have access to any work-product,[91] even before it was made public. The Act was passed in reaction to the

---

86 James Rule, et al., *Preserving Individual Autonomy in an Information-Oriented Society*, *in* Computers, Ethics, and Social Values (Deborah G. Johnson & Helen Nissenbaum eds., 1995), at 321.

87 Governmental policies and technology intended to create massive surveillance databases and mine individual data rejected by the public when presented with transparency options.

88 U.S. Patriot Act, *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act: Public Law 107-56, 2001 H.R. 3162 (2001).* (2001), at http://leahy.senate.gov/press/200110/102401a.html (last visited on 15 June 2012).

89 *Id.* at §§ 904-905.

90 *Privacy Protection Act*. 42 U.S.C. § 2000(a)(a) *et seq* (1980). (US)

91 Includes contact information, notes, research, and writings.

Zurcher v. Stanford Daily[92] case wherein the Burger Court ruled that the police could search newspaper offices even if no one was suspected of a crime.

The Act prohibited any search and seizure by law enforcement agencies of any "work product materials possessed by a person reasonably believed to have a purpose to disseminate to the public in a newspaper, book, broadcast, or other similar form of public communication, in or affecting interstate or foreign commerce."[93] The exceptions included a probable cause to suspect that the person has committed a crime or "there is reason to believe that the immediate seizure of such materials is necessary to prevent the death of, or serious bodily injury to, a human being."[94] The Act does allow for a private right of action, allows for liquidated damages, and does not allow criminal penalties.[95] The Act preempts state statutes.[96]

8.3.8 Electronic Communications Privacy Act of 1986

The Electronic Communication Privacy Act[97] expanded the Federal Wiretap 1968 statute to include interstate and stored electronic mail.[98] The Act established that when a person participates in online activities, such behavior did not waive all privacy rights. The Act provided criminal penalties for unauthorized electronic data access, including using the Internet. Section 2703 required that law enforcement must obtain a valid search warrant or subpoena to access stored data. A major exception was that Act only applied to intentional actions; however, accidental or unintentional acts were not

---

92 *Zurcher v. Stanford Daily.* 436 U.S. 457, 98 S. Ct. 1970, 56 L. Ed. 2d 525, (1978). (US)

93 *Privacy Protection Act*. 42 U.S.C. § 2000(a)(a) *et seq* (1980). (US)

94 *Id.* at § 2000(a)(2).

95 *Id.* at § 2000(aa)(6).

96 *Id.* at § 2000(aa)(6)(d).

97 *Electronic Communications Privacy Act of 1986* amend. (ECPA Title I) 18 U.S.C.A. §§ 2510-2521 (1986) (US). Note that in the US, any Act that uses *Privacy* in the tile probably limits privacy rights.

98 Intra-state behaviour would be a state action.

covered.[99] System operators were limited to authorized business functions and required not to disclose any information.[100]

In *Steve Jackson Games, Inc. v United States Secret Service,*[101] the Court found for Jackson, an Internet Bulletin Board operator, and ordered the Secret Service to pay $303,040 in damages plus attorney fees and costs for violating the Electronic Communication Privacy Act. While the Secret Service had a limited warrant, it took all of Jackson's computers and kept them for several months. The Court found that the Secret Service had exceeded its authority under the warrant and that the computers contained Bulletin Board e-mails and Jackson's simulation games.

In *McVeigh v. Cohen,*[102] the US Navy accessed a seventeen-year-old's Naval Veterans' America Online ISP website with the help of the Internet Service Provider. The Navy's action was conducted by deceit and taken before confronting McVeigh, obtaining a court order, subpoena, or warrant. McVeigh sued under the 1986 Electronic Communication Privacy Act. The court found for McVeigh and issued a preliminary injunction on any further Naval actions against him. The court declared that McVeigh's Internet Service Provider broke the law with the encouragement of the Navy. The court held that information privacy violations of the Electronic Communication Privacy Act must be protected by a standard strictly observed.[103]

In *Planned Parenthood v. ACLA*,[104] the Supreme Court determined that information privacy cyber threats are the same as unlawful physical threats.[105] Some federal anti-spam laws even protected against unwanted

---

99 *Id.* at 2701(a).

100 *Id.* at 2510(5)(a).

101 *Steve Jackson Games, Inc. v. United States Secret Service*, 816 F. Supp. 432 (W.D. Tex. 1993), *aff'd*, 36 F.3d 457 (5th Cir. 1994). (US)

102 *McVeigh v. Cohen*, 983 F. Supp 215 (D.D.C.)(1998). (US)

103 *Id.* at §, 1.

104 *Planned Parenthood v. ACLA*, 41 F.Supp 2d 1130, D. Or. 1999). *Planned Parenthood v. ACLA*, (41 F.Supp 2d 1130, D. Or. 1999). (US)

105 *Id.*

spam e-mail.[106] The Court formally established privacy as information privacy control in *Kyllo v. United States.*[107] The case found that warrantless searches, using modern technology, were a Fourth Amendment violation. The Supreme Court was concerned about legal protections and new technology that can "discern all human activities."[108]

In *re Pharmatrak, Inc. Privacy Litigation*[109] the District Court focused on the meaning of consent. Pharmatrak used cookies to collect data on its website. The site collected names, addresses, phone numbers, e-mail addresses, date of birth, and other personal information. The corporation claimed that the viewers had consented to the collection. The court ruled that consent must be actual rather than constructive and cannot be inferred from the mere purchase of an information service. A registration form is not consent to release personal information. The court also ruled:

> We think, at least for the consent exception under the ECPA in civil cases, that it makes more sense to place the burden of showing consent on the party seeking the benefit of the exception, and so hold. That party is more likely to have evidence pertinent to the issue of consent.[110]

A major problem with the Electronic Communication Privacy Act and related restrictive legislation was found in *re Northwest Airlines Privacy Litigation*.[111] Northwest Airlines disclosed passenger records to the National Aeronautical and Space Agency (NASA) in violation of its privacy policy and the Electronic Communications Privacy Act and other similar Acts. The customer's suit was

---

106 Jan Fernback & Zizi Papacharissi, Online Privacy as Legal Safeguard: The Relationship Among Consumer, Online Portal, and Privacy Policies, 9 *New Media & Society* 5, 715 (2007).

107 533 U.S. 27, 121 S.Ct. 2038, 150 L.Ed.2d 94, (2001). (US)

108 *Ibid.*

109 In re *Pharmatrak, Inc. Privacy Litigation,* 329 F.3d 9 (1st Cir. 2003), 19. (US)

110 *Ibid.*

111 *In re Northwest Airlines Privacy Litigation*, 2004 U.S. Dist. LEXIS 10580 (D. Minn., 2004). (US)

dismissed because Northwest was not an electronic communications service provider.[112]

Congress passed the Pen Register Act of 1984,[113] which declared that "no person may install or use a pen register or a trap and trace device without first obtaining a court order." Section (b) provided exceptions for providers that include "operation, maintenance, and testing of a wire or electronic communication service … protection of the rights or property of such provider, or to the protection of users of that service from abuse of service or unlawful use of service."[114] The Act did not require an informed consent from data subjects.[115] The Pen Register Act does not allow a private right of action; however, it does provide for criminal penalties.[116] The Act does not preempt state statues.

8.3.9 Computer Matching and Privacy Protection Act of 1988

The US Congress continued its concern about data collection, storage, mining, and sharing. In 1988, Congress passed the Computer Matching and Privacy Protection Act.[117] In theory, the law limited sharing of computer privacy data between federal agencies. The law did not pass the test of time or governmental practices. US governmental standards changed with the Bush administration and the 9/11 attacks.

---

112 *Ibid.*

113 *Pen Register and Trap and Trace Device* Use amend. 18 U.S.C. II, 206, § 3121, § a-b (1984), (US)

114 *Ibid.*

115 *Id.* at § 3121(b)(3).

116 *Id.* at § 3123(d).

117 *Computer Matching and Privacy Protection Act* amend. 5 USC 552a (1988). (US)

8.3.10 Health Insurance Portability and Accountability Act of 1996

The Federal government passed the Health Insurance Portability and Accountability Act of 1996 (HIPAA)[118] to ease the transfer of health insurance policies, to advance electronic acceptance of medical data, and to codify some privacy principles. The Act was intended to protect the privacy of patient data. Most of the privacy principles were not new; however, additional administrative and legal penalties were established. Protected health information (PHI) included all health data that was transmitted or maintained in any form. All covered entities were restricted from using or disclosing any protected health information except as permitted or required by the privacy and security regulations of the Act. The Act does not preempt state statutes.

The Department of Health and Human Services is the regulatory agency charged with enforcing HIPAA.[119] Two departments monitor the self-regulation of patient privacy. The Office of Civil Rights addresses privacy issues while the Office of E-Health Standards and Services addresses security issues. Each Office can impose civil penalties; however, the Department of Justice has criminal oversight. The Department of Justice has determined that organizations and selected individuals can be prosecuted for violations of the law.[120] The Department of Health and Human Services has taken the position that the Act and its agencies should seek only voluntary compliance and self-regulation. Through 2007, the Office of Civil Rights has received over 20,000 complaints about violations; however, only one has been referred for trial.[121] The HIPAA case study shows that even when the

---

118 *HIPAA. Health Insurance Portability and Accountability Act of 1996* amend. 42 U.S.C. § 1320 (1996) (US).

119 U.S. Department of Health and Human Services, *Health Information Policy*, Author. (2011), at http://www.hhs.gov/ocr/privacy/ (last visited on 14 July 2012).

120 American Medical Association (A.M.A.), *HIPAA Violations and Enforcement*, Author. (2011), at http://www.ama-assn.org/ama/pub/physician-resources/solutions-managing-your-practice/coding-billing-insurance/hipaahealth-insurance-portability-accountability-act/hipaa-violations-enforcement.page (last visited on 14 June 2012).

121 Sheera Rosenfeld, et al., *Privacy, Security, and the Regional Health Information Organization (*California Health Care Foundation. 2007), 24.

legislature passes clear laws, regulatory agencies that support self-regulation will ignore the law and the self-regulation process will again fail.

The Attorney General's Office in the various states also has enforcement powers. The Act did not pre-empt any stronger state laws, but rather functions as a privacy "floor" by establishing minimal standards. Many states enacted stronger health care privacy laws than HIPAA.

The Department of Health and Human Services did not start enforcing 1996 HIPAA standards for some time. The first investigative action took place in 2007 and involved the Piedmont Hospital in Atlanta, Georgia.[122] The action involved the loss of 386,000 Providence patients' data. The final agreement was not reached until July 15, 2008, when an administrative resolution agreement was signed. Providence paid $100,000 US Dollars (USD) in fines and agreed to a corrective plan. The plan required that the organization revise policies and procedures; train workers; do annual policy updates; establish a risk assessment plan; and conduct reviews.[123]

Margret Amatayakul and Michael R. Cohen reported on a number of HIPAA compliance studies.[124] The Act has only a sixty percent compliance record. From 500 to 600 privacy violation complaints are received per month. From seventy to eighty-six percent of sample subjects voiced concerns about the privacy of their personal medical records under the HIPAA act. HIPAA enforcement has been less than acceptable. The non-response pattern is related to violator resistance and the fact that the fines are less than the cost of compliance. Federal regulators have followed a classic non-response

---

122 Amanda Sounart, *CMS Hires PricewaterhouseCoopers to Monitor HIPAA Violations*. (2008), at http://www.amnhealthcare.com/News.aspx?ID=17342 (last visited on 5 June 2012).

123 *Ibid.*

124 Margret Amatayakul & Michael R. Cohen, *Is HIPAA Now Spelled Apathy?* (2008), at http://health-care-it.advanceweb.com/editorial/content/editorial.aspx?CC=89534%20 (last visited on 24 July 2011), 3 & 6 .

regulation pattern.[125] The general lack of concern from the legal community has resulted in little HIPAA enforcement.

The compliance situation became so bad that California enacted the Health Insurance Portability and Accountability Implementation Act of 2001.[126] The new legislation used HIPAA standards as a floor rather than a ceiling for privacy standards. The new California legislation increased fines, penalties, and new breach-disclosure standards and created a new Office of Health Information Integrity. The new legislation instituted fines up to $250,000 USD for data release violations and a $100.00-a-day fine for non-disclosure of any breaches.[127]

8.3.11 Children's Online Privacy Protection Act of 1998

In 1998, the Children's Online Privacy Protection Act (COPPA)[128] was passed to regulate the collection and use of personal information related to children under the age of thirteen years by commercial websites. In most circumstances, verifiable parent consent is required before website operators can collect such information.[129] Children's personal information that must be protected includes name, physical address, e-mail address, telephone number, social security number, any means to contact the child or parent, and any identifiable information.[130] Violators could be sued for damages.[131] The Act is enforced by the Federal Trade Commission and state attorney generals. The Act does not provide for a private right of action or provide for criminal penalties.

---

125 See Stephen G. Breyer, *Regulation and its Reform* (Harvard University Press. 1982).
126 *California Health and Safety Code* § 130200-130203 (US).
127 *Ibid.*
128 *Children's Online Privacy Protection Act of 1998 (COPPA),* 15 U.S.C. §§ 6501-6506 (1998) (US).
129 *Id.* at § 6502(b)(1)(A)(i).
130 *Id.* at § 6501(8).
131 *Id.* at § 6504.

In August 2012, the FTC proposed rules that would strengthen enforcement standards for requiring parental consent for mobile phone apps and tablets. Voice applications, location tracking, and behavioral advertising were included.[132] Direct marking associations and large service providers opposed the change and effectively got the FTC to modify the rules. In December 2012, the FTC exempted app stores like Apple. The FTC also exempted Facebook and Google.[133]

8.3.12 Gramm-Leach-Bliley Act of 1999

In 1999, the conservatives in the US Congress passed the Gramm-Leach-Bliley Act[134] that was formally titled the Financial Services Modernization Act. The Act effectively repealed most of the banking legislation established during the Great Depression to combat significant banking industry abuses. Industry leaders had long disliked the financial restrictions placed on them by President Franklin Delano Roosevelt's New Deal.[135] The Act covers domestic financial institutions, meaning "any entity that significantly engages in financial activities."[136] Under the Act, financial institutions can again behave in a pre-depression pattern; however, the Act did establish a financial sector standard for information privacy and data protection.

---

[132] Natasha Singer, *New Online Privacy Rules for Children*. (2012), at http://www.nytimes.com/2012/12/20/technology/ftc-broadens-rules-for-online-privacy-of-children.html?_r=0&adxnnl=1&adxnnlx=1356472268-p+IWhdnIfSnfwJY3miX9tA (last visited on 19 December 2012).

[133] Anton Troianovski & Danny Yadron, *U.S. Expands Child Online Privacy Law to Cover Apps, Social Networks.* Wall Street Journal. (2012), at http://online.wsj.com/article/SB10001424127887323777204578189430101877770.html (last visited on 19 December 2012).

[134] *Gramm-Leach-Bliley Act aka Financial Services Modernization Act. Pub. L. No. 106-102, 113 Stat. 1338*. (1999), at http://banking.senate.gov/conf/ (last visited on 22 June 2012) (US).

[135] Paul J. Polking & Scott A. Cammarn, *Overview of the Gramm-Leach-Bliley Act*, 4 North Carolina Banking Institute, 1 (2000); Lissa L. Broome & Jerry W. Markham, Banking and Insurance: Before and after the Gramm-Leach-Bliley Act, 25 *Journal of Corporation Law* 4, 723 (2000).

[136] *Id*. at § 103.

The privacy provisions of the Act require that all covered financial institutions must provide privacy and security practices-notices to consumers (yearly) and customers (automatically) on an opt-out basis. The Act applies to all US financial institutions and holders of personal financial information.[137] In the US, banks are regulated by the Federal Deposit Insurance Corporation (FDIC).[138] The Department of Commerce has no jurisdiction over FDIC-regulated institutions. Thus, such institutions have no Safe Harbor provisions.[139] The Act requires that the FTC and the FDIC develop and enforce privacy and safeguard rules.[140] Some states (e.g., California) have much stricter legislation.[141] There is no private action right for violations; however, criminal penalties can be applied.[142]

Under the Act, financial institutions must provide safeguard security administration standards.[143] The institution must always conduct due diligence, do periodic risk assessments, maintain vendor oversight, manage workforce risks, and provide employee training. The institution must provide technical security over access controls, applications, computer systems, and networks. Although acceptable encryption is not required, it is recommended; moreover, proper disposal rules are set. The data must be "burned,

---

137 *Gramm-Leach-Bliley* § 6827 (4)(B). The list includes auto dealers, banks, credit card companies, financial advisors, insurance firms, landlords, merchants that issue credit cards, mortgage brokers, real estate agents, security firms, thrift shops, and universities. See also Federal Trade Commission, *FTC Consumer Alert*. (2005, June), at http://www.ftc.gov/bcp/conline/pubs/alerts/disposalalrt.shtm (last visited on 2 September 2012).

138 Federal Deposit Insurance Corporation, *FDIC*. (2007), at http://www.fdic.gov/ (last visited on 30 August 2012).

139 See § 8.9.2 of this work.

140 *Gramm-Leach-Bliley Act* at § 6822(a)(b).

141 See *California Financial Information Privacy Act* amend. California Finance Code §§ 4050-4060 (2003) (US). The federal law does not pre-empt state laws with stronger privacy protections. See 15 U.S.C. § 6807(b).

142 *Gramm-Leach-Bliley Act* at Sec 523.

143 *Gramm-Leach-Bliley Act* at Sec 501(b).

pulverized, or shredded." Electronic files or media must be fully "erased or destroyed." Due diligence is required to supervise the destruction process.[144]

8.3.13 Patriot Act of 2001

As early as 1988, twenty Deans and 590 law professors from 147 law schools submitted a petition to Congress to stop governmental practices violating privacy rights and the First Amendment. Over 120,000 citizens also signed the petition.[145] The government's response was to intimidate and harass those involved.[146] Minimal corrective legislative actions followed until 2001, when the concerns were rejected.[147]

The Uniting and Strengthening America by Providing Appropriate Tools Required to Obstruct Terrorism (Patriot) Act of 2001 was euphemistically called the US Patriot Act. The Neo-Conservative forces in the US had been trying but had failed for years to enact legislation for more police powers and fewer civil liberties. The September 11, 2001, attack on the World Trade Center in New York City was the crisis that allowed passage. The bill had already been written and was passed in record time; few legislators even read the bill. Such actions are common in US history, followed by an awareness of remorse and understanding that the action was folly.[148] The Patriot Act increased governmental and police surveillance powers and allowed authorities to ignore prior privacy protections, including the Pen Registration

---

144 Federal Trade Commission, *FTC Consumer Alert*. (2005, June), at http://www.ftc.gov/bcp/conline/pubs/alerts/disposalalrt.shtm (last visited on 2 September 2012), ¶ 6.

145 David Cole & James X. Dempsey, *Terrorism and the Constitution: Sacrificing Civil Liberties in the Name of National Security* (The New Press 2nd ed. 2002), 189-201.

146 *Ibid.*

147 *Ibid.*

148 Frederic Block, Civil Liberties During National Emergencies: The Interactions Between the Three Branches of Government in Coping with Past and Current Threats to the Nation's Security, 29 *New York University Review of Law and Social Change* 3, 459 (2005).

Act[149] and protections regarding financial privacy; it also limited court review of governmental privacy related actions.

The Act and the public relations efforts that helped to get the Act passed certainly ignored Benjamin Franklin's November 11, 1755, declaration that "Those who would give up essential liberty, to purchase a little temporary safety, deserve neither liberty nor safety."[150] David Cole documented that the Patriot Act was an example of a trade-off of safety for liberty. David Cole and James Dempsey argued that the government used a double standard that is constitutionally wrong, is normatively counterproductive, and is "likely to pave the way for future incursions on citizens' rights."[151] The Act gave tremendous power to government while ignoring constitutional powers. The law essentially revoked the majority of prior DPSIP laws. Under the new legislation, federal agents now had the authority to seize personal documents (e.g., book store sales, business files, e-mails, library files, medical records, phone bills, video rentals) and place wire-taps without court approval.[152]

The legal, professional, and scientific fields adopted a different view. David Cole and James Dempsey[153] showed that the Act was repeating prior governmental crimes and mistakes. Christopher Raab[154] showed that the Act was overbroad and needed careful review. Stephen Schulhofer[155] argued

---

149 *Pen Register and Trap and Trace Device* Use amend. 18 U.S.C. II, 206, § 3121, § a-b (1984), (US).

150 Benjamin Franklin, *Pennsylvania Assembly: Reply to the Governor; Votes and Proceedings of the House of Representatives, 1755-1756* (Pennsylvania Assembly. 1756), 19–21, ¶ 7.

151 David Cole & James X. Dempsey, *Terrorism and the Constitution: Sacrificing Civil Liberties in the Name of National Security* (The New Press 2nd ed. 2002).

152 Kevin Bankston & Megan E. Gray, Government Surveillance and Data Privacy Issues: Foundations and Developments, 3 *The Privacy & Information Law Reporter* 8, 1 (2003).

153 David Cole & James X. Dempsey, 2002,

154 Christopher Patrick Raab, Fighting Terrorism in an Electronic Age: Does the Patriot Act Unduly Compromise Our Civil Liberties? 2006 *Duke Law and Technology Review* 3, 26 (2006).

155 Stephen J. Schulhofer, *Rethinking the Patriot Act: Keeping America Safe and Free* (The Century Foundation. 2005).

that the Act provided little to no transparency. Schulhofer[156] explored many of the areas of lack of accountability within the Act. Moreover, the Act contains no viable checks and balances. John Whitehead and Steven Aden argued that the Act was fundamentally unconstitutional. The authors argued that the attacks on the World Trade Center were not attacks on America as much as an "Attack on America as America … If the American people accept a form of police state in the name of a promise of personal security, that would be the greatest defeat imaginable."[157] Su Herman clearly established that the authors of the Act and the current administration ignored fundamental checks and balances.[158] Therefore, not only is DPSIP at stake; the basic rule of law is under attack.

8.3.14 Fair and Accurate Credit Transactions Act of 2003

In December 2003, the Fair Credit Reporting Act[159] was amended by the Fair and Accurate Credit Transaction Act.[160] The Act required that credit and debit card receipts printed by machines could no longer display the expiration date; moreover, only the last four numbers of the card could be displayed. Plaintiffs could recover small actual damages and limited punitive damages.[161]

A number of class action suits have been litigated under the credit and debit card receipts provisions of the Act. One concern was that potential damages might be more than the net worth of the defendant. In *Safeco Insurance*

---

156 Stephen J. Schulhofer, The New World of Foreign Intelligence Surveillance, 17 *Stanford Law & Policy Review* 531, 538 (2006).

157 John W. Whitehead & Steven H. Aden, Forfeiting "Enduring Freedom" for "Homeland Security": A Constitutional Analysis of the U.S. PATRIOT Act and the Justice Department's Anti-Terrorism Initiatives, 61 *American University Law Review* 6, 1081 - 1133 (2002), 1133.

158 Su.S. N N. Herman, The U.S. Patriot Act and the submajoritarian Fourth Amendment, 41 *Harvard Civil Rights - Civil Liberties Law Review* 1, 67 (2006).

159 *Fair Credit Reporting Act (FCRA), Public Law No. 91-508*. (1970), at http://www.ftc.gov/os/statutes/031224fcra.pdf (last visited on 3 July 2012) (US).

160 *Fair and Accurate Credit Transaction Act*, amend. 15 U.S.C.A. § 1681 (2003) (US).

161 *Id.* at §616, (a)(1)a).

Company of America v. Burr,[162] the Court established a principle of an "objectively unreasonable" standard for such cases. The holding of this case was that an insurance company may subjectively believe that its practices did not violate the law or consumer rights. When the companies' interpretation of the law is highly unreasonable, the company should have known that the practices were unacceptable. Thus, consumers do not need to establish that the company had knowledge of its legal violations.

A Federal District Judge refused to certify class action litigation under the Act because the damages to the company would be too high. The Seventh Circuit ruled that the "district judge sought to curtail the aggregate damages for violations he deemed trivial. Yet it is not appropriate to use procedural devices to undermine laws of which a judge disapproves."[163] The courts determined that a class action case should be certified and if necessary that an analysis to determine if the behavior is constitutionally excessive be applied. The US credit protections are far less stringent than the law in AU.[164]

8.3.15 Health Information Technology for Economic and Clinical Health Act of 2009

At least in terms of HIPAA standards, the Obama administration has taken a more proactive stand on DPSIP issues. The Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH) strengthened standards on the handling of PHI.[165] The Act also provided economic stimulation funding under the American Recovery and Reinvestment Act. The

---

[162] *Safeco Insurance Company of America v. Burr,* 551 U.S. 1, 127 S. Ct. 2201, 2213 (June 4, 2007), b. (US).

[163] *Murray v. GMAC Mortgage Corporation*, 434 F. 3d 948 (7th Cir. 2006), 7. (US).

[164] See Chapter 4 § 4.3 of the current work.

[165] U.S. Department of Health & Human Services, *HITECH Act Enforcement Interim Final Rule*. (2009), at http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/hitechenforcementifr.html (last visited on 27 December 2012).

Act increased the violation penalties for HIPAA violations and provided funds for health care agencies and professionals to adopt Electronic Medical Record (EMR)[166] technologies. The Act fails to address the DPSIP risks of EMR practices.

The major change in the law is that HITECH standards for HIPAA compliance was expanded to provider's business associates and required data breach notification to patients. The ACT does provide a patient's right to restrict information transfer to insurance companies for services directly paid by the patient. Providers must provide an audit trail of all PHI transfers. Criminal penalties apply to covered employees who access and disclose PHI. Civil penalties for such violations can reach $1.5 million USD a year.[167]

8.4 United States of America Federal Cases

Before examining the federal case law determinations on DPSIP legal issues, it is important to examine the power and reality constraints on the highest court in the jurisdiction. At various times the Court has maintained its purpose to be independent. At other times, the Court is blatantly political. Evidence does exist that the Court has been inconsistent.[168]

---

166 Some agencies and authors use the term Electronic Health Records (EHR).

167 *Ibid*.

168 See John W. Dean, *Broken Government: How Republican Rule Destroyed the Legislative, Executive, and Judicial Branches* (Viking. 2007); Jay M. Feinman, *Un-Making Law: The Conservative Campaign to Roll Back the Common Law* (Beacon Press. 2004); Jan Crawford Greenburg, *Supreme Court: The Inside Story of the Struggle For Control of the United States Supreme Court* (The Penguin Press. 2007); Jeffrey Rosen, *The Supreme Court: The Personalities and Rivalries that Defined America* (Times Books Henry Holt and Company. 2006); Cass R. Sunstein, *Why Societies Need Dissent* (Harvard University Press. 2003); Cass R. Sunstein, et al., *Are Judges Political? An Empirical Analysis of the Federal Judiciary* (Brookings Institution Press. 2006).

Table 8.0 United States Supreme Court

Factor	**US Supreme Court**[169]
Established	1789
Power of decisions	Applies to all courts and jurisdictions in the country
Membership	One Chief Justice and eight associate justices (currently)
Appointee Background	Leading appellate courts judges, politicians, and law professors
Term of Office	Life or until retirement
Jurisdiction	Original and appellate
Role	Error-correction
Operations	Hears oral arguments but relies heavily on arguments presented in written briefs
Decisions	Opinion of the majority, written by one justice, and concurring and dissenting opinions of other justices
Judicial Review	Historic since Justice Marshall established the principle of judicial review in US law.
Appointment	President nominates, Senate confirms
Representation	Recently more political
Opinions	No advisory opinions
Case Assignment	Court determines what cases it will hear based on writ of certiorari. Since 1925, the Court has had discretionary docket control.

The early American privacy law and the bill of rights were influenced by *Pope v. Curl.*[170] *Pope* was a UK case that found a property-based privacy right in one's own productions, writings, and letters.

The US federal case law includes decisions established by the Federal Trade Commission rulings and successful litigations. The federal case law also includes decisions made by the US federal court system.

---

169 Kermit L Hall, *The Oxford Companion to the Supreme Court of the United States* (Oxford University Press 2nd. ed. 2005). See also Supreme Court of the United States, *About the Supreme Court*. (2010), at http://www.supremecourt.gov/ (last visited on 5 July 2012).

170 *Pope v. Curl*, 2 Atk. 324, 26 Eng. Rep. 608 (1741). (UK)

8.4.1 United States Federal Trade Commission Case Law

The Federal Trade Commission Act of 1914 created the Federal Trade Commission (FTC) as an independent regulatory agency. The FTC is not under the direction of nor does it report to the Executive, Judicial, or Legislative branches of government. Such a structure is unique when compared to the AU, CA, SA, and UK regulatory systems. Appointments to the commission are made by the Executive and approved by the Senate. The commission is headed by five commissioners, each of whom serves a seven year term. No more than three commissioners can be appointed from the same political party.[171] In theory, political interests can control appointments and can essentially influence the commission's focus. The FTC can self-institute an investigation or respond to a complaint. The goal is to reach an agreement of consent with penalties when warranted. When the parties can not agree, the FTC can institute federal litigation to have the courts enforce the FTC's decision.

The Commission has jurisdiction over a number of information privacy and data security related laws.[172] The Commission investigates, negotiates, litigates, and monitors compliance. Historically, fines have been small. The typical violation required corrective actions and third party audits and periodic reports. FTC case decisions have the force of case law. The sampled decisions explored in the current study include cases related to how businesses provide checks and controls on how information data is handled, data security, and misrepresentation cases that involve privacy concerns. In all of the following cases, corporations made promises to protect privacy concerns, follow the applicable FTC related law, and were caught violating their own promises and the FTC administered law. The analysis includes some major US and international businesses. The selected FTC cases address issues of checks and controls, data security, and misrepresentation

---

171 *Federal Trade Commission Act, 15 U.S.C. § 41* (1914) (US).

172 Including the Children's Online Privacy Act, Federal Trade Commission Act, Fair Credit Reporting Act, and the Gramm-Leach-Bililey Act.

or false statement violations. In each case, the company was found to have violated FTC controlled laws, fined, and required to submit to a third-party monitoring of continuing practices.[173]

The Superior Mortgage Corporation was subject to the 2002 Gramm-Leach-Bililey Act (GLBA) Safeguard Rule.[174] The corporate websites had a privacy and security statement that promised protections and security, including data encryption.[175] The truth was that data held by the corporation was not encrypted.[176] The FTC ruling was that the corporation had failed to establish reasonable data security and failed to comply with the GLBA safeguard rules. The corporation made false and misleading statements regarding its privacy and security procedures. The corporation failed to assess data risks, institute appropriate password policies, follow control access practices, protect sensitive customer information, and deal with DPSIP risks in a timely fashion. However, only monitored reporting was ordered.[177]

DSW, Inc. (Designer Shoe Warehouse) used an unprotected wireless computer network in its stores to request and authorize check, credit card, and debit card purchases. A breach compromised "approximately 1,438,281 credit and debit cards (but not the personal identification numbers associated with the debit cards), along with 96,385 checking accounts and driver's license numbers."[178] The FTC found that the corporation failed in its DPSIP legal responsibilities.[179] The corporation was required to use state of the art

---

173 The author's review of the cases reveals a progression from passive to more activist enforcement.

174 *Gramm-Leach-Bliley Act aka Financial Services Modernization Act. Pub. L. No. 106-102, 113 Stat. 1338*. (1999), at http://banking.senate.gov/conf/ (last visited on 22 June 2012) (US).

175 Federal Trade Commission, *Superior Mortgage Corporation (Docket C-4153)*. (2005, December 16), at http://www.ftc.gov/os/caselist/0523136/051216comp0523136.pdf (last visited on 2 August 2012).

176 *Id.* at § 13.

177 *Id.* at § 6.

178 Federal Trade Commission, *DSW, Inc. (DOCKET NO. C-4157)*. (2006, March 7), at http://www.ftc.gov/os/caselist/0523096/0523096c4157DSWComplaint.pdf (last visited on 23 July 2012), 2. (US)

179 *Ibid.*

security protections and submit to third party audits for twenty years. The company was liable for up to $11,000 civil fines for each violation.

Choice Point, Inc. collected and sold consumer data and credit reports to businesses, government agencies, legally established organizations, and professionals for consumer reporting, risk management, and other purposes. The corporation had privacy policies posted on its annual reports, contracts, website, and other documents that promised that it allowed access only under the rules of the Fair Reporting Credit Act.[180] In early 2006, it was discovered that the personal data of 163,000 consumers was disclosed to people who had no permissible justification. The corporation, despite being alerted, continued to authorize the release of data by failing to monitor and identify unauthorized activity.[181] Choice Point was fined $10 million plus an additional $5 million set aside for consumer redress.[182] Choice Point was the first case that involved a significant economic sanction.

The Hershey Food Corporation operated over 30 websites aimed at age 13 and under children. Contests were run on the sites, and contest winners' names and home states were published on the website with no parental consent.[183] The FTC found that sufficient notice was not given and the disclosure practices were unlawful.[184] The corporation was fined $85,000 and placed on a 20-year reporting regimen.[185]

Mrs. Fields' Original Cookies, Inc., and its wholly owned subsidiaries offered websites with a birthday club for children 12 years and under. The club offered a birthday card and a cookie or pretzel coupon. Club members had to

---

180 Federal Trade Commission, *ChoicePoint Inc.* (2006 December 6), at http://www.ftc.gov/os/caselist/choicepoint/0523069complaint.pdf (last visited on 1 August 2012). (US)

181 *Ibid.*

182 *Ibid.*

183 Federal Trade Commission, *Hersey Food Corporation*. (2003, February 27a), at http://www.ftc.gov/os/2003/02/hersheycmp.htm (last visited on 26 July 2012), at19. (US)

184 *Id*. at 21.

185 *Id*. at 25-28.

provide personal information. The corporation did not notify or obtain verifiable parental consent nor was there a means for parents to delete or review the information posted by the children. The corporations were fined $100,000 for the COPPA violations.[186]

Bonzi Software developed utilities and a free desktop download aimed at young children. Access to the programs required providing personal information that included address, age, e-mail address, name, and stated personal interests. No parental consent or notice was provided. The Bonzi practices were a violation of the Children's Online Privacy and Protection Act[187] and the Federal Trade Commission Act.[188] The corporation was only issued a $75,000 fine.[189]

Starting in 2004, Facebook, a social networking site, had grown to 900 million members worldwide. In 2009, the annual income was 777.2 million USD. Members set up pages that can include personal information, photos, and other information. [190]

Starting in November of 2009, Facebook established a Central Privacy Page. Members could make the information public; restrict access to only friends, or to friends of friends. The company failed to notify members that despite the privacy settings, selected third parties could access the data. Starting in December 2009, Facebook overrode members' privacy settings and no notice was posted. Facebook started including third party advertisements on the

---

186 Federal Trade Commission, *Mrs. Fields Famous Brands, Inc., Mrs. Fields' Holding Company, Inc., and Mrs. Fields' Original Cookies, Inc*. (2003 February 27b), at http://www.ftc.gov/os/2003/02/mrsfieldscmp.htm (last visited on 9 August 2012). (US)

187 *Children's Online Privacy Protection Act of 1998 (COPPA),* 15 U.S.C. §§ 6501-6506 (1998) (US).

188 *Federal Trade Commission Act*, 15 U.S.C. § 41 (1914) (US).

189 Federal Trade Commission, *Bonzi Software, Inc., A Corporation, and Joe Bonzi and Jay Bonzi, Individually and as Officers of Said Corporation (DOCKET NO. C-4126)*. (2004, October 13), at http://www.ftc.gov/os/caselist/0423016/041013cmp0423016.pdf (last visited on 25 July 2012). (US)

190 Federal Trade Commission, *Facebook, Inc. (DOCKET NO. C-4365)*. (2012), at http://ftc.gov/os/caselist/0923184/120810facebookcmpt.pdf (last visited on 10 August 2012). (US)

members' pages. The company promised that it would not share any information with advertisers without the members' permission. The claim was false. The company claimed that if the members' accounts were deactivated or deleted, no one could access the information. However, Facebook continued to share photos and videos when requested. Facebook self-certified that it followed the US Safe Harbor program between the US and the EU. In reality, Facebook did not always comply with the Safe Harbor principles of notice and choice. On 10 August 2012, the FTC ordered that Facebook be carefully monitored by an independent agent for twenty years to correct the above violations.[191]

Google was a major international information technology and Internet service corporation. Google offered e-mail, web search, and chat resources. The corporation determined that it could profit from entering the social networking market by establishing Google Buzz.[192]

Gmail users were given an opt-in or opt-out option to Buzz; however the opt option was ignored. The default shared previously private information. Google self-certified that it followed the US Safe Harbor program between the US and the EU. In reality, Google did not always comply with the Safe Harbor principles of notice and choice. Google had agreed to FTC compliance orders; however, it failed to comply. Google used cookies to collect data on searches and DPSIP data. Google failed to provide for effective opt-out provisions for those using Apple computers. Google ignored Apple users that used the op-out options.[193]

Google claimed that it subscribed to the self-regulatory principles of the Network Advertising Initiative (NAI). The claim was false and further established that the self regulation model was flawed. The federal court ruled

---

191 *Ibid.*

192 Federal Trade Commission, *Google, Inc. (Docket C-4335)*. (2012), at http://www.ftc.gov/os/caselist/c4336/120809googlecmptexhibits.pdf (last visited on 20 November 2012). (US)

193 *Ibid.*

that Google had violated its compliance orders and the federal DPSIP law. The court issued civil penalties of 22.5 million USD. This was the highest damage award to date.[194]

The FTC cases reveal the need to address privacy and data security issues at the same time. The cases show that many corporations believe that they are above the law and that the violation fines are generally small. The cases show that even when the FTC has direct regulatory authority, the US approach to self-regulation prevails. The FTC and US law has not embraced the importance of modern DPSIP legal standards.

8.4.2 United States of America Federal Case Law

At times, the US Supreme Court has been a powerful force and formed the trajectory of legal analysis. Starting in 1938,[195] the Court declared it would shift focus from economic rights of businesses and the regulation of property to attending to non-economic individual rights. This new focus included "discrete and insular minorities." In *United States v Carotene Products Company*[196] Justice Harlan Stone wrote that a presumption of constitutionality exists when the law is within the Bill of Rights and the Fourteenth Amendment.

Several Supreme Court cases helped to define privacy in proper context. As noted above, in *N.A.A.C.P. v. Alabama*,[197] Justice Harlan declared, “This Court has recognized the vital relationship between freedom to associate and

---

194 *Ibid.*

195 The shift occurred during the midst of the Great Depression and prior to US entry into the Second World War. Corporate control of the Republic was rejected due to its failure to follow the social contract. From a long-term historic perspective, the shift was relatively short. The current state in this country has returned to pre-depression policies.

196 *United States v. Carolene Products,* 304 U.S. 144 (1938), n4 (US).

197 *NAACP v. Alabama*, 357 U.S. 449, 462, 78 S. Ct. 1163, 2 L. Ed. 2d 1488, (1958), 465 (US).

privacy in one's associations."[198] In this case, Alabama required the release of personally identifiable membership lists. The organization refused to release such lists. The case established that individuals can share information within an organization and not forfeit ownership of the information. The organization is then expected to refrain from sharing the information with others unless the person consented. Harlan was not concerned about the action of Alabama; instead, he was concerned the information could be released into private hands. Therefore, the individual could be exposed to "economic reprisal, loss of employment, threat of physical coercion, and other manifestations of public hostility."[199] He wrote, "The crucial factor is the interplay of governmental and private action, for it is only after the initial exertion of state power represented by the production order that private action takes hold."[200]

In *Gibson v Florida Legislative Investigation Committee,*[201] the court wrote that "One man's privacy may not be invaded because of another's perversity…If the files …can be ransacked … then all walls of privacy are broken down."[202] The facts of the *Gibson* and *N.A.A.C.P. v. Alabama* cases were similar. Gibson was president of the Miami branch of the NAACP and was asked by the state of Florida's Legislative Investigation Committee to produce a membership list of his organization. He refused and was found in contempt by the Committee, but the court exonerated him, saying no "compelling and subordinating governmental interest"[203] was at stake. Only one exception existed: when the government had probable cause and a warrant that the person was involved in a crime, the information could be released.

---

198 *Ibid.*
199 *Id.* at 462.
200 *Ibid.*
201 *Gibson v Florida Legislative Investigation Committee*, 372 U.S. 539, 548, (1963) (US).
202 *Id.* at 570.
203 Id. at 435.

In *Boyd v United States*, [204] Justice Bradley reviewed privacy protections in the Fourth and Fifth Amendments. He wrote: "It is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offense; but it is the invasion of his indefeasible right of personal security, personal liberty and private property."[205] The *Boyd* decision helped to build the model in which DPSIP is established as a privacy right in the US.

Olmstead was one of the most infamous technology and information privacy cases in US history. Chief Justice and former President William Howard Taft, declared that installing a telephone in a house eliminates Fourth Amendment protections.[206] The decision allowed subsequent administrations in the US, and after World War Two other countries, access to all types of electronic media without a warrant or any rule of law principle of checks and balances.

While it took forty years, *Katz v United States*[207] overturned part of the *Olmstead* decision. Justice Stewart ruled that the Fourth Amendment protects people - not places. However, the party must take steps to ensure a subjective expectation of privacy. The expectation must be reasonable by society standards. This test is still current law in the US.

In *United States Department of Justice v. Reporters Committee for Freedom of the Press*,[208] the Court found that the use of computer technology in collecting, storing, and sharing private information must be curbed. Justice Stevens reasoned that the computer age has invalidated traditional checks and balances of even public records privacy protections. Justice Stevens also adopted a definition of privacy. The Stevens definition stressed the need for individuals to control personal information about

---

204 *Boyd v. United States*, 116 U.S. 616, (1886), 630 (US).

205 *Ibid.*

206 *Olmstead v. U.S.*, 277 U.S. 438, 478 S. Ct. 564. 66 ALR 376, 72 L.Ed. 944, (1928), 466 (US).

207 *Katz v. United States*, 389 U.S. 347, 88 S.Ct. 507, 19 L.Ed.2d 576, (1967), 350-351 (US).

208 *U.S. Department of Justice v. Reporters Committee for Freedom of the Press,* 489 U.S. 749, (1989), 764 (US).

themselves.[209]

In 2003, the Supreme Court ruled that the right to liberty under the due process clause of the Fourteenth Amendment applied to private conduct. The Court determined that "It is a promise of the Constitution that there is a realm of personal liberty which the government may not enter".[210] The earliest US case on point was *Wheaton v. Peters*,[211] wherein the Court ruled that a "defendant asks nothing - wants nothing, but to be let alone until it can be shown that he has violated the rights of another."[212]

Boyd v. United States[213] was a landmark decision in the legal recognition of a right to privacy based on both the protection against unreasonable search and seizure of the Fourth Amendment and the right to avoid self-incrimination as provided by the Fifth Amendment. Justice Bradley, writing for the full court, used over two hundred years of American and English law to find that both Amendments protect the privacy of individuals from governmental intervention. The decision applies to criminal and civil actions.

Justice Brandeis argued that, "The makers of our Constitution conferred, as against the government, the right to be left alone – the most comprehensive of rights and the right most valued by civilized men."[214] In *Oklahoma Press Publishing Company v. Walling*,[215] the Court accepted Brandeis' position on constitutionally protected privacy rights and sociological jurisprudence.

---

209 *Ibid.*

210 *Lawrence v. Texas*, 539 U.S. 558, 564, 123 S.Ct 2472, 156 L.Ed.2d 508, (2003), 564 (US).

211 *Wheaton v. Peters*, 33 U.S. 591, 8 L.Ed. 1055,(1834),1055 (US).

212 *Ibid.*

213 *Boyd v. United States*, 116 U.S. 616, (1886) (US).

214 *Id.* at 478.

215 *Oklahoma Press Publishing Company v. Walling*, 327 U.S. 186, 66 S.Ct. 494, 90 L.Ed. 614, (1946) (US).

The right of privacy was also justified on First Amendment grounds. In *NAACP v. Alabama,*[216] the Warren Court ruled that "This Court has recognized the vital relationship between freedom to associate and privacy in one's associations."[217] "Inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs."[218]

The reasoning of Chief Justice Taft in the *Olmstead* case, in terms of physical intrusion, was not dead. In *Silverman v. United States,*[219] the Warren Court ruled that a physical intrusion violated privacy rights under the Fourth Amendment. The case involved placing eavesdropping devices to a private home's heating ducts without authorization. The Court determined that the government unreasonably intruded into the home. Thus, the person's right to retreat into his home should be free of unreasonable intrusion. With prophetic vision and perhaps cowardice, the Court wrote that "[w]e need not here contemplate the Fourth Amendment implications of ... other frightening paraphernalia which the vaunted marvels of an electronic age may visit upon human society."[220]

In 1965, the Warren Court finally recognized a constitutionally protected *zone of privacy* based upon the First, Third, Fourth, Fifth, and Ninth Amendments. The decision in *Griswold v. Connecticut*[221] determined that the Amendments protect invasions of the "sanctity of a man's home and privacies of life (and) is a constitutionally protected zone of privacy." In this case, Justice Goldberg wrote a concurring statement on the Ninth Amendment. He wrote that the "Framers of the Constitution believed that there are additional fundamental rights, protected from government infringement, which exist alongside those

---

216 *NAACP v. Alabama*, 357 U.S. 449, 462, 78 S. Ct. 1163, 2 L. Ed. 2d 1488, (1958) (US).
217 *Id.* at §. 3.
218 *Ibid.*
219 *Silverman v. United States*, 365 U.S. 505, 81 S.Ct. 679, 5 L.Ed.2d 734, (1961). (US)
220 *Id.* at 81 (US).
221 *Griswold v. Connecticut,* 38 1 U.S. 479, 85 S.Ct. 1678, 14 L.Ed.2d 510, (1965), 485 (US).

fundamental rights specifically mentioned in the first eight constitutional amendments."[222]

A year later, the court clarified the meaning of the Fifth Amendment's protection against self-incrimination, and that it was an essential value. The Court reasoned that "our respect for the inviolability of the human personality and of the right of each individual 'to a private enclave where he may lead a private life" must not be violated.[223]

The *Katz v. United States*[224] decision finally overturned *Olmstead*. In the facts of the *Katz* case, the government attached a listening and recording device outside of a phone booth without a warrant. The court ruled that the governmental action was an unconstitutional invasion of privacy under the Fourth Amendment. The Warren Court ruled that the Amendment governs the seizure of tangible items as well as recording or oral[225] statements. The Court found that a violation of a legitimate expectation of privacy could occur even without a physical intrusion. The Court wrote, "The Fourth Amendment protects people, not places."[226] The finding was that the "petitioner had manifested 'a reasonable expectation of' privacy in his conversation in a phone booth." The *Katz* decision established a two-part inquiry into the applicability of the Fourth Amendment. The measure was based on two essential factors: "(1) has the individual manifested a subjective expectation of privacy in the object of the challenged search and (2) is society willing to recognize that expectation as reasonable."[227]

The *Katz* ruling also addressed constitutional and legal protections of privacy. The Court found that "the protection of a person's general right to privacy –

---

222 *Id.* at 486.

223 *Tehan v. Shott,* 382 U.S. 406, 86, S.Ct. 459, 15 L.Ed.2d 453, (1966), 486 (US).

224 *Katz v. United States,* 389 U.S. 347, 88 S.Ct. 507, 19 L.Ed.2d 576, (1967) (US).

225 A case can be made that recording and oral now applies to electronic statements and communications.

226 *Id.* at 351.

227 *Id.* at 388.

his right to be let alone by other people – is like the protection of his property and of his very life, left largely to the law of the individual states."[228] The provision allows states to establish increased privacy protections.

The Burger Court found that a state law criminalizing "mere possession of obscene material was unconstitutional."[229] The decision declared that "It is now well established that the Constitution protects the right to receive information and ideas regardless of their social value, and to be generally free from governmental intrusions into one's privacy and control of' one's thoughts."[230]

The Court ruled that President Nixon's "authorization of electronic surveillance in the domestic security arena without judicial approval"[231] was unconstitutional. The Court balanced the government's duty to protect domestic security against the right of citizens to be secure in their privacy against unreasonable government intrusion. The Burger Court found that "broad and unsuspected governmental incursions into conversational privacy with electronic surveillance … necessitate the application of a warrant."[232] "By no means of least importance will be the reassurance of the public generally that indiscriminate wiretapping and bugging of law-abiding citizens cannot occur."[233]

8.4.2.1 Decisional – Information Cases

The Court also found that decisional privacy was constitutionally protected when state laws banning distribution of contraceptives were struck down. In

---

228 *Id.* at 350-351.
229 *Stanley v. Georgia,* 394 U.S. 557, 89 S.Ct. 1243, 22 L.Ed.2d 542, (1969), 589 (US).
230 *Ibid.*
231 *United States v. United States District Court*, 407 U.S. 297, 92 S.Ct. 2125, 32 L.Ed.2d 752, (1972), 297 (US).
232 *Ibid.*
233 *Ibid.*

Eisenstadt v. Baird,[234] the Burger Court found that the "right of the individual, married or single, to be free from unwarranted government intrusion into matters so fundamentally affecting a person as the decision to bear or beget a child" was protected.

The principles of decisional privacy and zones of privacy were again sustained in *Roe v. Wade*.[235] The Burger Court ruled that a woman has a constitutionally protected right to privacy in deciding if she wanted to terminate a pregnancy.

8.4.2.2 Expectation of Privacy Cases

In *United States v. Miller*,[236] the Burger Court ruled that a bank depositor had no expectation of privacy when presenting financial data that could be shared with bank employees. A major factor was the doctrine of the ordinary course of business practices exemption. However, the Congress did not agree with the decision; it passed the Right to Financial Privacy Act of 1978,[237] which established privacy of financial records for bank customers. The Right to Financial Privacy Act of 1978 voided the decision in *United States v. Miller*.

The Burger Court was not always consistent. The police required the New York telephone company to send information to a remote location that consisted of a pen register that was used as a device to record numbers dialed. In *United States v. New York Telephone Company*,[238] the Burger Court found the police order constitutional. The ruling was based on the argument that the "pen registers disclosed … neither the purpose of the communication, the identities of the parties communicating, nor whether the

---

234 *Eisenstadt v. Baird*, 405 U.S. 438, 92 S.Ct. 1029, 31 L.Ed.2d 349, (1972), 438 (US).
235 *Roe v. Wade*, 410 U.S. 113, 93 S.Ct. 705, 35 L.Ed.2d 147, (1973) (US).
236 *United States v. Miller*, 425 U.S. 435, 96 S.Ct. 1619, 48 L.Ed.2d 71, (1976) (US).
237 *Right to Financial Privacy Act of 1978*, 18 U.S.C. §§ 3401 3422 (1978) (US).
238 *United States v. New York Telephone Company*, 434 U.S. 159, 98 S.Ct. 364, 54 L.Ed.2d 376, (1977) (US).

communication was even completed."[239] Thus, the Court found that no legitimate expectation of privacy existed.

Two years later, the Burger Court expanded *United States v. New York Telephone Company*[240] to include the legal standard that there is no expectation of privacy when a person dials a telephone number. The Court ruled that a person "voluntarily conveys those numbers to the telephone company when he uses the telephone … (A) person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[241]

In *United States v. Karo*,[242] the police attached a beeper to an object that was taken into a private residence so that they could monitor activity inside the residence. The Burger Court ruled that this action was unconstitutional because it violated the Fourth Amendment. The monitoring could have been done by outside observation. The Court ruled that there was a justifiable interest in the privacy of the residence.

The Neo-Conservative Rehnquist Court built upon the *Karo* outside observation principle. In a case of the police using aircraft to observe illegal plants growing in a home backyard garden, the Court found that the person knowingly exposed his private garden to the public. There was no legitimate expectation of privacy of a garden around a home where it was visible from above.[243]

When the police used a navigable airship to photograph a Dow Chemical plant, the Rehnquist Court found no Fourth Amendment violation. Instead, the Court found that the airship was available to the public. Although the

---

239 *Id.* at 198.
240 *Smith v. Maryland,* 442 U.S. 735, 99 S.Ct. 2577, 61 L.Ed2d 220, (1979), 799 (US).
241 *Ibid.*
242 *United States v. Karo*, 468 U.S. 705, 104 S.Ct. 3296, 82 L.Ed.2d 530, (1984) (US).
243 *California v. Ciraolo,* 476 U.S. 207, (1986) (US).

airship enhanced human vision, the approach was constitutional.[244] "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[245] The Rehnquist Court found that there is no reasonable expectation of privacy when one places objects in the garbage left for collection, when the garbage is publicly accessible.[246]

In 2001, the Rehnquist Court placed some constraints on the observation of public spaces. The police used thermal imaging technology on a public street to monitor heat emanating from a private house. The technology showed where and what the people in the house were doing. The Court found the police use of the technology was unconstitutional under the Fourth Amendment. The Court again applied the outside observation principle. "To withdraw protection of this minimum expectation of privacy, would be to permit police technology to erode the privacy guaranteed by the Fourth Amendment."[247]

8.4.2.3 Informed Consent Consideration Cases

The issue of informed consent is critical to assessing DPSIP legal considerations. The first US court case involving reasonable care and consent was *Pratt v. Davis*.[248] In this case, a patient was subjected to surgery without any informed consent. The court ruled that "one's bodily integrity could not be violated without consent or knowledge."[249] In a similar case, Justice Cardozo emphasized the need for voluntary consent and ruled that voluntary consent violations were a form of assault.[250] Thus, the concept of informed consent in the US was established. Similar cases included

---

244 *Dow Chemical v. United States*, 476 U.S. 227, 106 S.Ct. 1819, 90 L.Ed.2d 226, (1986), 227 (US).
245 *California v. Greenwood*, 486 U.S. 35, 108 S.Ct. 1625, 100 L.Ed.2d 30, (1988), 35 (US).
246 *Ibid.*
247 *Kyllo v. United States*, 533 U.S. 27, 121 S.Ct. 2038, 150 L.Ed.2d 94, (2001), 27 (US).
248 *Pratt v. Davis* 118 111. App. 161, (1905), 161. (US).
249 *Ibid.*
250 *Schloendorff v The Society of New York Hospital,* 105 N.E. 92, (1914). (US).

Theodore v. Ellis;[251] *Hunter v. Burroughs*;[252] and *Wojciechowski v. Coryell*.[253] In *Salgo v. Leland Stanford, Jr., University Board of Trustees,*[254] the court applied a more fully developed informed consent principle that declared that there is an affirmative duty to disclose. One must offer free consent based on being fully informed of the risks, benefits, and alternatives. Plaintiff Salgo was disabled because of a medical procedure. Salgo received no information about alternatives, benefits, outcomes, or risks. Justice Bray used the informed consent statement in the brief provided by the American College of Surgeons[255] as the basic structure of the standard. The same principle of informed consent applies to DPSIP issues.

In *Tbornburgh v. American College of Obstetricians & Gynecologists*,[256] US Supreme Court Justice John Stevens addressed the issue of decision-making based on informed consent and the universal impact of the consent principle. He wrote "[I]t is far better to permit some individuals to make incorrect decisions than to deny all individuals the right to make decisions that have a profound effect upon their destiny."[257]

The principle of informed consent can be waived. One can waive the requirement simply by clearly declaring intent to do so. However, one must still have awareness of the consent principle. The consent cannot be coerced or be passive. The fundamental principle of autonomy and self-determination cannot be violated. Legal intervention is needed to protect privacy as self-regulation and historic standards of care are ineffective.

---

251 *Theodore v. Ellis*, 141 La. 709, 75 So. 655, 660, (1917). (US).

252 *Hunter v. Burroughs*, 123 Va. 113, 96 S.E. 360, 366-368, (1918). (US).

253 *Wojciechowski v. Coryell*, 217 S.W. 638, 644 (Mo.App, (1920). (US).

254 *Salgo v. Leland Stanford Jr. University Board of Trustees,* 317 P.2d 170, (1957). (US).

255 American College of Surgeons, Brief as Amicus Curiae in Support of Defendant and Appellant Frank Gerbode (1956). “A duty to disclose any facts which are necessary to form the basis of an intelligent consent.”

256 *Tbornburgh v. American College of Obstetricians & Gynaecologists,* 476 U.S. 747, 781, (1986), 781. (US)

257 *Ibid.* In terms of DPSIP legal principles, the informed consent is an opt-in option.

Starting in the 1950s, these principles became more standard because of case law decisions and an increasing pattern of consent violations. In the twentieth century, research and medical abuses were revealed. Classic examples include the medical experiments performed by the Nazis during World War Two. International consent standards were established during the Nuremberg Trials. The discovery of the state of Alabama Tuskegee syphilis studies added to the awareness of consent violations.[258] In the US, federal legislation was passed to establish the principle of informed consent and the need to protect unknowing victims of abuse.[259] These standards need to be applied to DPSIP policies.

Consumers gradually began to become more empowered over the course of the twentieth century. Issues of negligence on the part of goods and service providers became more relevant. Information consumerism grew, as well as the amount of consent violation litigation.[260]

In 1974, the state legislatures started to move into the area of informed consent. During the next three years, twenty- four states enacted informed consent legislation. The pattern continued through 1982 when all but three states had enacted protective legislation.[261]

State legislation and associated case law used the concept of enterprise liability as it is the cheapest cost avoider for no-fault liability. Those who experience injuries from products or activities placed on the market ought to be compensated by the related corporations, enterprises, governments,

---

[258] From 1932 through 1972, the Tuskegee Institute and the US Public Health Service studied the progression of syphilis in a group of poor Black males; some of which had the disease and some did not. The participants were never informed of their illness status and no treatment was ever provided. The subjects were given free meals, questionable medical care, and burial insurance.

[259] Ruth Faden & Tom L Beauchamp, *A History and Theory of Informed Consent* (Oxford University Press. 1986).

[260] E.S Glass, Restructuring Informed Consent: Legal Therapy for the Doctor-Patient Relationship, 179 *Yale Law Journal* 8, 1533-1576 (1970).

[261] Jessica W. Berg, et al., *Informed Consent: Legal Theory and Clinical Practice* (Oxford University Press 2nd ed. 2001).

institutional caretakers, municipalities, and professionals.[262]

The movement correlated with Lawrence Friedman's[263] description of the Total Justice Principle. The principle involves a general expectation of justice (i.e., fairness, due process in all situations, and a general expectation of compensation for wrongs known as recompense). The proposed concept of "protection of the uninformed consumer" was established.[264]

In 1974, the National Research Act[265] was passed. This Act established the National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. The Commission established the standard of Institutional Review Boards, which monitor all human subject research and related data collection. Protocols must be established, approved, and followed.[266] A similar approach can be used in DPSIP law.

The Act was a codification of the 1948 Nuremberg Code, which established that voluntary consent is essential and that the benefits of the research must outweigh the risks involved. The Act further incorporated the 1964 Declaration of Helsinki established by the World Medical Association. The declaration followed the Nuremberg standard and added that related research should be monitored by independent committees. In 1979, the National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research issued the Belmont Report, which established the principles of autonomy/respect for persons, beneficence, and justice for

---

262 Guido Calabresi, *The Costs of Accidents* (Yale University Press. 1970). The concept is that civil and criminal liability is imposed on each sector of the market for defective and harmful product or service based on market share.

263 Lawrence M. Friedman, *Total Justice* (Beacon Press. 1985).

264 John B Clutterbuck, Karl Llewellyn and the intellectual foundations of enterprise liability theory, 97 *Yale Law Journal* 6, 1114 (1988), at 1114. Examples include the legal justification of adhesion contracts, consumer protection, contracts, product liability, respondeat superior, strict liability, workers' compensation, and all obligations for health, safety, and security.

265 *National Research Act* amend. 45 CFR 46 (1974). (US). The current author was part of the research team that established U.S. Federal Research guidelines including informed consent.

266 *Id.* at § 474 (a).

research dealing with human subject research and data collection.[267]

8.4.2.4 Opt-in versus Opt-out Cases

One of the most significant DPSIP business, law, and human behavior issues is the question of whether data collectors should use an opt-in or opt-out[268] standard for data collection options. The majority of surveys show that data subjects prefer the opt-in option.[269] Corporations prefer opt-out because it increases participation by ignoring the participant's neuropsychological function. Therefore, corporations take advantage of human physiological function and dysfunction in decision-making for profit.[270]

Business proponents of opt-out procedures argue that corporations should be able to structure consent any way that they want, because doing otherwise would infringe on the corporations' right of free speech. On February 13, 2009, the Federal Court of Appeals for the District of Columbia ruled for the 2006 Federal Communications Commission opt-in principle.[271] The Court found that "the government has a substantial interest in protecting the privacy of customer information and that requiring customer approval advances that

---

[267] US Department of Health & Human Services, *The Belmont Report: Ethical Principles and Guidelines for the Protection of Human Subjects of Research; The National Commission for the Protection of Human Subjects of Biomedical and Behavioural Research*. (1979), at http://www.hhs.gov/ohrp/humansubjects/guidance/belmont.html (last visited on 21 July 2012).

[268] Opt-in means that one has to agree to any data collection. Opt-out means that the data collector can collect unless one opts-out – says no. The EU Directive (1995) favors opt-in. The direct marketing associations favor opt-out because of increased profits.

[269] Kim Bartel Sheehan, *How Public Opinion Polls Define and Circumscribe Online Privacy*, 9 *First Monday*, 7 (2004), http://www.firstmonday.org/issues/issue9_7/sheehan/ (last visited on 24 June 2012).

[270] See George R. Milne & Andrew J. Rohm, *Consumer Privacy and Name Removal Across Direct Marketing Channels: Exploring Opt-in and Opt-out Alternatives*, 19 Journal of Public Policy and Marketing 2, 238-249 (2000). and Jan Bouckaert & Hans Degryse, *Opt In Versus Opt Out: A Free-Entry Analysis of Privacy* Policies (The Fifth Workshop on the Economics of Information Security (WEIS 2006). Robinson College, University of Cambridge, England 26-28 June 2006). (2006), at http://weis2006.econinfosec.org/docs/34.pdf (last visited on 24 July 2012).

[271] *National Cable & Telecommunications Association v. Federal Communications Commission, United States of America, Qwest Communications International Inc. and Verizon*. (2009, February 13), at http://pacer.cadc.uscourts.gov/common/opinions/200902/07-1312-1164901.pdf (last visited on 2 April 2012). (US).

interest."[272] The Court also found that "the carrier's sharing of customer information with a joint venturer or an independent contractor without the customer's consent is itself an invasion of the customer's privacy."[273]

A 2011 study conducted by Stanford University Law School's Center for Internet and Society found that opt-out procedures are often ignored by Internet companies. The research studies the practices of sixty-five companies including AOL, BlueKai, eXelate, Google, Microsoft, and Yahoo. The study found that half of the companies continued to track transactions, even after data subjects had opted-out. The mechanisms included cookies and invisible third-party cookies.[274] When confronted, the companies claimed that the opt-out was for marketing, not tracking activities.

8.5 State Constitutional Declarations

A number of states have enacted constitutional protections of privacy. The following table shows the state provisions, the privacy code, and source.

Table 8.1 State Constitutional Declarations

State of the US	Code
State of Alaska (1956).	Article 1, Section 22: The right of the people to **privacy** is recognized and shall not be infringed.[275]
State of Arizona (1881)	Section 8: No person shall be disturbed in his **private affairs**, or his home invaded, without authority of law.[276]
State of California (1879)	Article 1, Section 1: All people are by nature free and independent and have inalienable rights. Among these

[272] *Id.* at 9.

[273] *Id.* at 11.

[274] Mike Swift, *Stanford Study Shows Opting Out of Web Tracking Not So Easy*, Mercury News. (2011), at http://www.mercurynews.com/rss/ci_18524333?source=rss (last visited on 25 July 2012).

[275] State of Alaska, *Constitution*. (1956), at http://old-www.legis.state.ak.us/cgi-bin/folioisa.dll/acontxt/query=*/doc/%7Bt25%7D (last visited on 10 July 2012). (US)

[276] State of Arizona, *Constitution*. (1881), at http://www.azleg.state.az.us/const/2/8.htm (last visited on 10 July 2012). (US)

	are … protecting property, and pursuing and obtaining safety, happiness, and **privacy.**[277]
State of Florida (1968)	Article 1, Section 23: **Right of privacy.** Every natural person has the right to be let alone and free from governmental intrusion into the person's **private** life except as otherwise provided herein.[278]
State of Hawaii (1978)	Article 1, Section 6: The right of the people to **privacy** is recognized and shall not be infringed without the showing of a compelling state interest.[279]
State of Illinois (1970)	Article 1, Section 6: Searches, Seizures, Privacy, and Interceptions: The people shall have the right to be secure in their persons, houses, papers and other possessions against unreasonable searches, seizures, invasions of **privacy** or interceptions of communications by eavesdropping devices or other means.[280]
State of Louisiana (1974)	Article 1, Section 5: Every person shall be secure in his person, property, communications, houses, papers, and effects against unreasonable searches, seizures, or invasions of **privacy**...Any person adversely affected by a search or seizure conducted in violation of this Section shall have standing to raise its illegality in the appropriate court.[281]
State of Montana (1972)	Article 2, Section 10: **Right of privacy.** The right of individual **privacy** is essential to the well-being of a free society and shall not be infringed without the showing of a compelling state interest.[282]
State of New Jersey (1947)	Article 1, Section 7: The right of the people to be **secure in their persons, houses, papers, and effects,** against unreasonable searches and seizures, shall not be violated.[283]
State of South	Article 1, Section 10: The right of the people to be

277 State of California, *Constitution*. (1879), at http://www.leginfo.ca.gov/cgi-bin/waisgate?waisdocid=8071921924+0+0+0&waisaction=retrieve (last visited on 10 July 2012). (US)

278 State of Florida, *Constitution*. (1968), at http://www.flsenate.gov/Statutes/index.cfm?Mode=Constitution&Submenu=3&Tab=statutes#A01S23 (last visited on 10 July 2012). (US)

279 State of Hawaii, *Constitution*. (1978), at http://www.state.hi.us/lrb/con/conart1.html (last visited on 10 July 2012). (US)

280 State of Illinois, *Constitution*. (1970), at http://www.ilga.gov/commission/lrb/con1.htm (last visited on 10 July 2012). (US)

281 State of Louisiana, *Constitution*. (1974), at http://www.senate.legis.state.la.us/Documents/Constitution/Article1.htm#%EF%BF%BD5.%20Right%20to%20Privacy (last visited on 10 July 2012). (US)

282 State of Montana, *Constitution*. (1972), at http://data.opi.mt.gov/bills/mca/const/II/10.htm (last visited on 10 July 2012). (US)

283 State of New Jersey, *Constitution*. (1947), at http://www.njleg.state.nj.us/lawsconstitution/constitution.asp (last visited on 10 July 2012). (US)

Carolina (2006)	**secure in their persons, houses, papers, and effects** against unreasonable searches and seizures and unreasonable invasions of privacy shall not be violated.[284]
State of Utah (1895)	Article 1, Section 14: The right of the people to be **secure in their persons, houses, papers, and effects** against unreasonable searches and seizures shall not be violated.[285]
State of Washington (1889)	Article 1, Section 7: Invasion of Private Affairs or Home Prohibited: No person shall be disturbed in **his private affairs, or his home invaded**, without authority of law.[286]

The number of states that have amended constitutions to include rights to privacy reveals the importance of the problem and the priority of instituting DPSIP legal standards. The trend suggests that states in the US may be able to move more quickly in establishing privacy law protections than the Federal government.

8.6 US State Legislation

The state of California was the first state in the US to pass massive privacy legislation; moreover, in 2000, the state of California established a statewide California Office of Information Security and Privacy Protection.[287] The California Security Breach Information Act established clear rules on computerized personal information and defined personal information. [288]

---

[284] State of South Carolina, *Constitution*. (2006), at http://www.scstatehouse.net/scconstitution/a01.htm (last visited on 10 July 2012). (US)

[285] State of Utah, *Constitution*. (1895), at http://le.utah.gov/~code/const/htm/CO_02015.htm (last visited on 10 July 2012). (US)

[286] State of Washington, *Constitution*. (1889), at http://www.courts.wa.gov/education/constitution/index.cfm?fa=education_constitution.display&displayid=Article-01 (last visited on 10 July 2012). (US)

[287] State of California, *California Office of Information Security and Privacy Protection*. (2009), at http://www.oispp.ca.gov/ (last visited on 4 September 2012). (US)

[288] State of California, *The California Security Breach Information Act (SB-1386), Civil Code §1798.29, §1798.82, & 1798.84* (2002), at http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html (last visited on 3 July 2012), §. 2e-f. Personal information includes the individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: Social

Under the Act, any business, person, or state agency that owns or licenses the processing of personal information must, with no unreasonable delay, notify any state residence if the unencrypted information has or may have been breached or obtained by an unauthorized person(s). The Act also applies to organizations that hire employees that reside in California or that outsource services for California employees and organizations doing business in California. A fine of $2,500 per breach of confidentially incidence, with a $500,000 per occurrence fine could be awarded.[289]

Breaches of confidentiality may include a variety of violations, such as deleting files, hacking, interception, and unauthorized modification. Violations also include misdirection,[290] retention errors, and unauthorized access. The data may be in files, printed copies, or computer screen views. Breaches can include auto-forwarding, forwarding, reply, and reply to all actions. Data viruses can be another source of violations.

The Act addresses a number of vulnerabilities, including the following:

1. Audit Log Tampering: Prevents tampering with audit log files data by restricting access to allow only authorized users and applications.
2. Buffer Overflow: Overflow of stored data into adjacent buffers, executing a code that triggers malicious or unauthorized activity.
3. Physical Theft : The theft of information through extraction from stolen hardware or storage media.
4. Root Attack: The ability to illegally obtain ‘trusted’ root access privileges.

Security number; driver's license number or California Identification Card number; account number, or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account. For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

289 *Id.* at § 4.

290 Includes sending data to the wrong e-mail address or person.

5. Unauthorized Data Viewing: The use of privileges to view information outside the requirements of a user's authorized role.
6. Unintended Administrator Privilege: The use of privileges to access, copy, or tamper with data outside the requirements of a user's authorized role.
7. Worms and Trojans: The alternation or insertion of executable code for the purpose of running an unauthorized application.[291]

A comprehensive search revealed no published cases under the *California Security Breach Information Act*. However, the state and a number of business organizations had provided extensive training on the provisions. The Act delineates risks that must be avoided. Several companies and corporations voluntarily complied with notifying customers of the policy, for example, CardSystems, ChoicePoint, and Lexus Nexus all responded to the Act.[292] None of these corporations wanted to pay the price or take the risk of being the first legal test case. States such as Arizona, Georgia, Maryland, and Rhode Island had passed legislation regarding Social Security Number identification and other protections.

8.7 US State Case Law

Some state case law has addressed some DPSIP and related issues. One of the earliest state court rulings that impacted federal law related to privacy was *Pavesich v New England Life Insurance Company*.[293] The state of Georgia Supreme Court ruled that privacy "has its foundation in the instincts of nature. It

---

[291] Vormetric Inc., *White Paper: California SB 1386 & AB 1950: Implementing Effective Encryption Protection for Personal Information Privacy*. (2005), at http://www.vormetric.com/downloads/SB_1386_AB_1950.pdf (last visited on 14 August 2012). 5.

[292] Robert Vamosi, *Security Watch: Congress Loves Identity Thieves*. (2005, November 11), at http://reviews.cnet.com/4520-3513-6381707-1.html (last visited on 14 August 2012).

[293] *Pavesich v. New England Life Insurance Company*, 122 Ga. 190; 50 S.E. 68; 1905 Ga. LEXIS 156, (1905), 69-70 (US).

is recognized intuitively …felt instinctively in its encroachment (and is based on) natural law."[294]

Natanson v. Kline[295] involved a female plaintiff who had undergone cancer surgery; her doctor recommended further radiation. The radiation worsened her condition. The Court determined that the failure to provide an informed consent constituted negligence. The Court found that patients have a right to know about possible consequences of treatment decisions, collateral risks and dangers involved, and the pros and cons of the treatment, as well as available alternatives. The description of the risks must include reliable information related to the imminence of harm, the magnitude of the alternative treatments, and the nature and probability of risks. The Court found that enterprises and professionals have a positive duty to disclose and obtain an informed consent. The principle of informed consent must apply to DPSIP laws.

In *Canterbury v. Spence*,[296] plaintiff Canterbury had back surgery and later fell from the bed and was paralyzed. The Court found that those under a duty to care and protect must use reasonable care that considers a personal right of self-determination. The ruling established that a person need not ask for information from the holder of the information, prior to the holder informing the person. The case finding expanded the standard from an issue of professional practices to a consideration of the information decision-making on the part of the person. The Court established a standard that considers the materiality of the information. The Court determined that there is a "right to consent to what happens to oneself, to self-determination, to make a self - decision."[297] The legal consent principles in this case should also apply to DPSIP principles.

---

294 *Ibid.*
295 *Natanson v. Kline*, 354 P.2d 671 (Kan. 1960). (US).
296 *Canterbury v. Spence*, 464 F.2d 772 (D.C. Cir. 1972). (US).
297 *Id.* at 783-786.

In *Scott v. Bradford*,[298] the Oklahoma Supreme Court established an individual – subjective person standard. The Court stated that "the scope of a physician's communication must be measured by his patient's need to know enough to enable him to make an intelligent choice. In other words, full disclosure of all material risks incident to treatment must be made."[299]

8.8 US Standards and Remedies

In the US, legislative, judicial, and administration of DPSIP standards is much like a small boat cast on open seas. The enforcement of standards and remedies are dependent on pendulum shifts from privacy concerns to governmental and corporate privilege. On a federal level, the general policy over the past decades has ignored international precedents and focused on self-regulation. Federal policy has been based on the faulty belief that markets are self-correcting - rather than self-serving.[300]

The greatest and most innovative US DPSIP protections appear to be at the state level. Several states have enacted innovative legislation and regulatory standards.[301] The problem with this approach is that enforcement is limited to state jurisdictional boundaries and does not cross state lines. In the US, state law is generally subservient to federal standards. The counter argument is the full faith and credit principle[302] that requires each state to accept all other states' attempts to regulate privacy protections. In reality, the US is tied to the outdated mode of fair information practices.

---

298 *Scott v. Bradford*, 606 P.2d 554, (1979). (US).

299 *Id.* at 558.

300 The belief is based on a misreading of Adam Smith's Wealth of Nations.

301 A classic example is the breach notification law passed by the State of California. This California state law has caused several other states to consider similar breach notification laws and resulted in an international focus on breach issues.

302 US Constitution, Article IV, Section 1.

8.8.1 Principles of Fair Information Practices

Various organizations, commissions, and governmental agencies have proposed and even adopted some Fair Information Practices. A review of a sample of the practices is warranted; however, legislation and an informed judiciary are also needed.

The Center for Democracy and Technology[303] and the Privacy Rights Clearing House[304] refined the Principles of Fair Information Practices. The principles are based on the work of the 1973 US Department of Health, Education, and Welfare, the 1980 Organization for Economic Cooperation and Development, the 1981 Council of Europe principles, and the 1995 Canadian Standards Association. The basic principles are noted in the following table:

Table 8.2 Fair Information Practices

Principle	Description
Openness	"The existence of record-keeping systems and databanks that contain personal data must be publicly known, along with a description of the main purpose and uses of the data."
Individual Participation	"Individuals should have a right to view all information that is collected about them; they must also be able to correct or remove data that is not timely, accurate relevant, or complete."
Collection Limitation	"There should exist limits to the collection of personal data; data should be collected by lawful and fair means and should be collected, where appropriate, with the knowledge or consent of the subject."
Data Quality	"Personal data should be relevant to the purposes for which it is collected and used; personal data should be accurate, complete, and timely."
Finality	"There should be limits to the use and disclosure of personal data: data should be used only for purposes specified at the time of collection; data should not be

303 Center for Democracy and Technology, *Privacy Basics: Generic Principles of Fair Information Practices*. (2008), at http://www.cdt.org/privacy/guide/basic/generic.html (last visited on 28 July 2012), 1.

304 Privacy Rights Clearinghouse, *A Review of the Fair Information Principles: The Foundation of Privacy Public Policy* (2004), at http://www.privacyrights.org/ar/fairinfo.htm (last visited on 28 July 2012), 1.

	otherwise disclosed without the consent of the data subject or other legal authority."
Security	"Personal data should be protected by reasonable security safeguards against such risks as loss, unauthorized access, destruction, use, modification or disclosure."
Accountability	"Record keepers should be accountable for complying with fair information practices."
Collection Limitation	"There must be no personal data record keeping systems whose very existence is secret."
Disclosure	"There must be a way for an individual to find out what information about him is in a record and how it is used."
Secondary Usage	"There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent."
Record Correction	"There must be a way for an individual to correct or amend a record of identifiable information about him."
Security	"Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data." [305]

However, not everyone embraced these fair information practices. John Poindexter,[306] the former director of the Defense Advanced Research Projects Administration's (DARPA) Total Information Awareness (TIA) project, strongly advocated for allowing data mining and knowledge discovery in databases. He proclaimed that data mining is necessary to fight terrorists. His goal was to have one system that could access all personal information - everything.[307] Poindexter was not new to Republican[308] conservative administrations. Poindexter's Total Information Awareness program was stopped in 2002 because of intense publicity but was quietly reinstituted. In 2006, the program was reinstituted under a new name: Disruptive Technology

---

[305] Center for Democracy and Technology, 2008, 1; *Privacy Rights Clearing House,* 2004, 1.

[306] While serving as President Reagan's advisor of the National Security Council, he supervised the sale of arms in the Iran–Contra legal violations. He was convicted for violating federal laws, trading with terrorists, shredding evidence, and lying to Congress. However, he did not serve any prison time because two far-right judges overturned the conviction.

[307] Everything included every bank card use, book bought or checked out, credit report, driver's license, e-mail, employment record, income tax records, license application, medical report, movie ticket, property record, and travel itinerary in the world.

[308] *United States v. United States District Court*, 407 U.S. 297, 92 S.Ct. 2125, 32 L.Ed.2d 752, (1972), 297 (US).

Office. The new program has stripped all privacy protections and abuse audit mechanisms.[309]

The program ran counter to the First Amendment regarding speech and the Fourth Amendment protections against searches without probable cause. The program also violated information privacy law standards. Daniel Solove placed the threat in a new perspective. He wrote that "Information is not the key to power in the Information Age—knowledge is. Information consists of raw facts. Knowledge is information that has been sifted, sorted, and analyzed."[310] Solove further compared the state of privacy violations in the US to Kafka's *The Trial*. He declared that "existing law protecting information privacy has not adequately responded to the emergence of digital dossiers."[311]

The September 11, 2001, attack on the New York World Trade Center towers opened the field for an authoritarian takeover, which was much worse than Eisenhower's farewell address warning of the dangers of the military-industrial complex.[312] A new public–private partnership was created to reject constitutional protections and rule of law principles. For example, the American-owned JetBlue® airline released five million passenger names and addresses to the military, simply upon request.[313] "Third parties that hold consumer information often comply with such requests because they want to

---

309 Shane Harris, *TIA Lives On*, National Journal. (2006, February 23), at http://www.nationaljournal.com/about/njweekly/stories/2006/0223nj1.htm (last visited on 8 June 2012), ¶ 4.

310 Daniel J. Solove, Privacy and Power: Computer Databases and Metaphors for Information Privacy, 53 *Stanford Law Review* 6, 1393 (2001), at 1456.

311 Daniel J. Solove, *The Digital Person: Technology and Privacy in the Information Age* (New York University Press. 2004), at 9.

312 Dwight D. Eisenhower, *Public Papers of the Presidents*,(Government Printing Office ed. 1960). After serving as the Supreme Allied Commander in WWII and two term President, Eisenhower warned that governmental agencies and large corporations were dictating governmental policies and ignoring the right of the people to self rule. The first draft of the speech included the term military-industrial-congressional complex.

313 Daniel J. Solove, Digital Dossiers and the Dissipation of Fourth Amendment Privacy, 75 *Southern California Law Review,* 1083 (2002a).

be helpful to the government or because compliance seems to be the path of least resistance."[314]

Robert O'Harrow[315] explained that the law of unintended consequences applies. He wrote,

> It's a simple fact that private companies can collect information about people in ways the government cannot. At the same time, they cannot be held accountable for their behavior or their mistakes the way government agencies can. Their capabilities have raced far ahead of the nation's understanding and laws.[316]

Neil Richards provided a further legal warning. He showed that, "To the extent that such private (data) collection is not state action, it allows the government, in effect, to outsource surveillance beyond the scope of otherwise applicable statutory and constitutional restrictions."[317]

The Bush administration built on the privacy violations of President Nixon and J. Edgar Hoover's misuse of massive dataveillance. The dataveillance was legally like the *general warrants* issued by the English King George III.[318] Such action "threatens both privacy and equality, and diverts government resources away from more effective responses to terrorism." [319]

---

[314] James X. Dempsey & Lara M. Flint, Commercial Data and National Security, 72 *George Washington Law Review,* 1459, 1476 (2004), at 1476.

[315] Robert O'Harrow, *No Place to Hide* (Free Press. 2006), 8-9.

[316] *Id.*

[317] Neil M. Richards, Reconciling Data Privacy and the First Amendment, 52 *UCLA Law Review* 4, 1149 (2005), at 1159.

[318] Jeffrey Rosen, *The Naked Crowd: Reclaiming Security and Freedom in an Anxious Age* (Random House. 2004), at 23. The King's agents could enter any house and search everything.

[319] *Id.* at 23.

The Bush administration ignored US Supreme court rulings. The *Griswold v. Connecticut*[320] Court ruled that "The First Amendment has a penumbra where privacy is protected from governmental intrusion."[321] In *Whalen v. Roe*,[322] the Court ruled that information privacy was a liberty guaranteed by the Fourteenth Amendment from state interference. Stan Karas identified the security–privacy power imbalance and total control implications. He argued that the "rationale behind the *Griswold* line of cases may be characterized as follows: intruding on private decisions is knowing, knowing is classifying, and classifying is impermissibly controlling."[323]

Paul Schwartz argued that "decisional and information privacy are not unrelated; the use, transfer, or processing of personal data by public and private sector organizations will affect the choices that we make."[324] Jeffry Rosen took the position that "when intimate information is removed from its original context and revealed to strangers, we are vulnerable to being misjudged on the basis of our most embarrassing, and therefore most memorable, tastes and preferences."[325]

8.9 United States of America Implementation System

The US DPSIP law is euphemistically termed sectoral. In reality, the system is a patchwork approach that functions much like rearranging the deck chairs on the Titanic. The American people consistently report a high interest in information privacy; however, the government and corporations ignore this data. Specialized legislation tends to be passed to resolve a current issue

---

320 *Griswold v. Connecticut*, 38 1 U.S. 479, 85 S.Ct. 1678, 14 L.Ed.2d 510, (1965), 483. (US).

321 *Ibid.*

322 *Whalen v. Roe*, 429 U.S. 589, (1977). (US).

323 Stan Karas, Privacy, Identity, Databases, 52 *American University Law Review,* 393 (2002), at 424.

324 Paul M. Schwartz, Property, Privacy, and Personal Data, 117 *Harvard Law Review* 7, 2055 (2004), at 2058.

325 Jeffrey Rosen, *The Unwanted Gaze: The Destruction of Privacy in America* (Random House. 2000), at 9.

and is then changed or ignored when the immediate issue is resolved, or replaced by another television sound bite issue, or shift in political power.

8.9.1 Self-Regulation

Since the Reagan administration, the US federal policy has been one of self-regulation and privatization. The current information privacy approach in the US was established by President William Clinton. His administration did not focus on regulatory control on privacy issues in any substantive way. His administration's Framework for Global Electronic Commerce[326] favored non-governmental self-regulation. The Framework's basic principles included:

1. The private sector should lead.
2. Governments should avoid undue restrictions on electronic commerce.
3. Where governmental involvement is needed, its aim should be to support and enforce a predictable, minimalist, consistent and simple legal environment for commerce.
4. Governments should recognize the unique qualities of the Internet.
5. Electronic Commerce over the Internet should be facilitated on a global basis.[327]

Section Five of the Framework document addresses some privacy concerns. The Framework report reinforces the importance of informational privacy in US law but also addresses free speech and the free flow of information dilemma. The position is that "data-gatherers should inform consumers what information they are collecting, and how they intend to use such data; and data-gatherers should provide consumers with a meaningful way to limit use and re-use of personal information."[328]

---

326 White House, *Framework for Global Electronic Commerce*. (1997), at http://www.technology.gov/digeconomy/framewrk.htm (last visited on 5 August 2012).

327 *Id.* at 2.

328 *Id.* at §. 5, ¶ 5.

Three privacy principles were reviewed but left to self-regulation. These privacy principles included:

> First, an individual's reasonable expectation of privacy regarding access to and use of, his or her personal information should be assured.
> Second, personal information should not be improperly altered or destroyed. And,
> third, personal information should be accurate, timely, complete, and relevant for the purposes for which it is provided and used.[329]

The Framework report declared that the "Administration considers data protection critically important. We believe that private efforts of industry working in cooperation with consumer groups are preferable to government regulation, but if effective privacy protection cannot be provided in this way, we will reevaluate this policy."[330] When data showed that the system was not working well, the Clinton Administration did little to rectify the situation. When the Federal Trade Commission[331] called for comprehensive legislation, still nothing was done.

Joel Reidenberg[332] documented the self-evident truth that self-regulation is a means by which corporations and industries attempt to avoid governmental regulations and enforcement powers. Industries tend to advocate self-regulation when a threat of legal action exists or major public reactions become evident.[333]

---

329 *Id.* at §. 5, ¶. 7

330 *Id.* at §. 5, ¶. 21.

331 Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace: A Report to Congress*. (2000), at http://www.ftc.gov/reports/privacy2000/privacy2000.pdf (last visited on 26 July 2012).

332 Joel R. Reidenberg, Privacy in the Information Economy-- A Fortress or Frontier for Individual Rights? 44 *Federal Communications Law Journal* 2, 195 (1992).

333 John W. Maxwell, et al., Self-Regulation and Social Welfare: The Political Economy of Corporate Environmentalism, 43 *Journal of Law and Economics*, 583 (2000).

Regulatory advocates are found on both sides of the issue. The continuum includes the data in the following table:

Table 8.3 Self-Regulation Arguments

Arguments For Self-regulation	Arguments Against Self-regulation
Reduces government and tax payer costs. [334]	The costs are passed on to the consumers in increased costs and lowered standards. Enforcement costs are higher.
Development and administrative costs are lower.	Standards are lower, less enforceable, and balanced. Compliance is not standard or equitable. Corporations will seek a competitive advantage by not following standards.
Industry members bring expertise [335]	The expertise can be and has been used in legal policy making.
The focus is on reasonable compliance as determined by the industry.	Compliance is based on the Rule of Law. Sanctions and expulsion are limited and have limited effect. There is no means of legal enforcement.[336]
Rules are more transparent and meet industry member needs.[337]	Legal approaches are more transparent and meet all stakeholders' needs. There is no recourse for individuals harmed.[338]
Industry groups have special knowledge.[339]	Industry groups should share special knowledge. The approach raised antitrust or anti-competitive issues.
Industry can better monitor compliance and performance.	The standards are self-serving. To be successful, the benefits must be high or compliance costs are low.[340]

---

334 Margot Priest, The Privatization of Regulation: Five Models of Self-Regulation, 29 *Ottawa Law Review* 2, 233 (1997).

335 *Id.*

336 Deidre K. Mulligan & Janlori Goldman, *The Limits and the Necessity of Self-Regulation: The Case for Both, in Privacy and Self-Regulation in the Information Age* (U.S. Department of Commerce eds., Government Printing Office 1997).

337 Douglas C. Michael, Cooperation Implementation of Federal Regulations, 13 *Yale Journal on Regulation*, 542 (1996).

338 Deidre K. Mulligan & Janlori Goldman, *The Limits and the Necessity of Self-Regulation: The Case for Both, in Privacy and Self-Regulation in the Information Age* (U.S. Department of Commerce eds., Government Printing Office 1997).

339 Maria Chiara Malaguti, Private-Law Instruments for Reduction of Risks on International Financial Markets: Results and Limits of Self-Regulation, 11 *Open Economies Review* 1, 247 (2000).

Self-regulation is more responsive to environmental changes.[341]	Independent agencies can effectively respond to environmental changes within broad legislative principles.
Self-regulation decreases operating costs.[342]	The approach ignores the damage costs of self-serving standards.
Self-regulation avoids legal standards including the Constitution and judicial standards.	Self-regulation can avoid legal standards including the Constitution and judicial standards. No checks and balances are provided. Enforcement is voluntary. Free-riders take advantage of the low costs of non-compliance.[343]

Some examples of successful self-regulation exist. Bar Associations and Security Dealer Associations are examples of effective self-regulation. To be effective, the industry group must be able to deal with the entire field, not just members. The self-regulation organization must have the power to grant or withdraw a license or certification to be involved in the field, monitor member and non-member activities, and punish violators effectively.[344]

Dale Kunkel and Ursula Goette[345] document some major problems with the self-regulation model. For instance, to compete with television in the 1950s, motion pictures started adding more sex and violence because the FCC would not allow such depictions on television. In the 1960s, public concerns about the increased use of sex and violence in motion pictures started to mount. The industry self-regulating organization, the Motion Picture Association of America (MPAA), did not respond for eight years. Self-regulation failed. In another example, in 1970, the National Association of

---

340 Douglas C. Michael, Cooperation Implementation of Federal Regulations, 13 *Yale Journal on Regulation,* 542 (1996).

341 George Milne & Mary J. Culnan, Strategies for Reducing Online Privacy Risks: Why Consumers Read [Or Ddon't Read] Online Privacy Notices, 18 *Journal of Interactive Marketing* 3, 15 (2004).

342 *Ibid.*

343 John W. Maxwell, et al., Self-Regulation and Social Welfare: The Political Economy of Corporate Environmentalism, 43 *Journal of Law and Economics*, 583 (October 2000).

344 See Stephen G. Breyer, *Regulation and its Reform*,(Harvard University Press ed. 1982); Stephen G. Breyer, *Breaking the Vicious Circle: Toward Effective Risk Regulation*,(Harvard University Press ed. 1993).

345 Dale Kunkel & Ursula Goette, Broadcasters' Response to the Children's Television Act, 2 *Communication Law and Policy* 3, 289 (1997).

Broadcasters started negotiating with its members to increase informational and educational programming for children. However, the issue was not addressed until the Congress passed legislation twenty years later. In this instance, self-regulation failed again. When the push for stopping television cigarette advertising started in the 1960s, the Broadcasters' association passed a weak standard which was voluntary and had no regulatory effect. However, the practice did not stop until 1994, when the Congress passed regulatory legislation. Self-regulation failed again. In 1973, the National News Council was formed to help self-regulation of journalists and press corporations by establishing voluntary ethical standards, fairness, and public accountability. In 1984, the effort at self-regulation failed due to member non-compliance. Thus, the self-regulation model does not provide incentives to comply or control the choices of other players. The urge for profits, power, and business advantage are render self-regulation ineffective in dealing with the issues that the law can mandate, enforce, and punish.

Another problem with the US approach is that political appointees can lie under oath to the Senate with impunity. In May 2001, Timothy J. Muris, the Bush appointee for the Federal Trade Commission chair, refused to make public his views on privacy. He stated that he would make sure that the Commission would maintain involvement on the issue.[346] In October of the same year, after he was appointed, he announced that the Commission was dropping its prior support for privacy legislation.[347]

The US model of self-regulation for DPSIP is not working. Under the self-regulation and financial security model, the Bank of New York Mellon (BNY Mellon) reported the breach of data on 12.5 million customers' account details that included addresses, dates of birth, names, and Social Security

---

[346] Edmund Sanders, *FTC Nominee Sails Through Senate Confirmation Hearing*, Los Angeles Times (2001, May 17), at 3.

[347] Jonathan Krim, *FTC Will Not Seek New Privacy Laws*, Washington Post (2001, October 5), at E1.

numbers.[348] In the first seven months of 2008, more expansive data breaches occurred than in the entire prior year. Four hundred and forty-nine businesses, governmental agencies, and universities reported the loss or theft of over 127 million individual records.[349]

The relative inaction on DPSIP issues of the Clinton Administration transformed into hostility from the George Walker Bush Administration. Privacy became a casualty of the "War on Terror," increasing governmental powers, a corporate republic, and Neo-Conservative nirvana.

8.9.2 Safe Harbor Agreement

To avoid a trade war with the EU over the Directive on Data Privacy, the Clinton administration negotiated the 2000 Safe Harbor agreement.[350] Prior to 2000, the EU had rejected the first six privacy proposals.[351] Under the agreement, selected businesses in the US could agree to follow basic data protection and information privacy standards to reach a level of *adequate protection* under the EU Directive.[352] Data protection authorities in the EU would allow data transfers with such firms without challenge.[353] US companies feared that the agreement was too strict, whereas Europeans saw the agreement as too lenient and unenforceable. US-based businesses did

---

348 Iain Thomson, *Bank of New York Loses 12.5 Million Customer Details*, SC Magazine for IT Security Professionals. (2008, September 1), at http://www.securecomputing.net.au/News/121357,bank-of-new-york-loses-125-million-customer-details.aspx (last visited on 1 September 2012).

349 Brian Krebs, *Data Breaches Have Surpassed Level For All of '07, Report Finds* Washington Post. (2008, August 26), at http://www.washingtonpost.com/wp-dyn/content/article/2008/08/25/AR2008082502496.html (last visited on 27 August 2012), ¶ 2.

350 European Commission, *US-EU Safe Harbor Frameworks*. (2011), at http://export.gov/safeharbor/index.asp (last visited on 4 August 2012).

351 Anna Shimanek, Note, Do You Want Milk with Those Cookies?: Complying with the Safe Harbor Privacy Principles, 26 *Iowa Journal of Corporate Law* 2, 455 (2001).

352 See Chapter 3, § 3.4.3 of this work.

353 European Commission, *US-EU Safe Harbor Frameworks*. (2011), at http://export.gov/safeharbor/index.asp (last visited on 4 August 2012).

not perceive DPSIP protection as a cost of doing business.[354] The EU decided not to try to extend the principles with the US.[355]

Graham Pearce and Nicholas Platten[356] correctly assessed the legal, policy, and political status of privacy in the US. The authors stated that the powers that be do not like legislative–legal solutions and international standards. The work of the Clinton and subsequent Bush administrations presented prima facie evidence of this statement. As early as 1998, John Mogg, Director General of the European Commission, told US business and political leaders that US privacy laws reveal that "Most of what we see is not meaningful ... the industry codes we have seen have no teeth."[357]

The Safe Harbor agreement was accomplished to protect corporate profits, not DPSIP law standards.[358] Edmund Andrews reported that the US was concerned because it had an entire industry that accumulated, analyzed, collected, and sold personal data. The corporate supported politicians were concerned that consumers would use privacy standards for nuisance litigation to protect legitimate privacy concerns.[359] The selling point was that the agreement was consistent with the self-regulation mantra.

The Safe Harbor agreement shows that Europeans have much stronger privacy protections than those in the US. The agreement is basically meaningless because violations are referred to the national court. The principles protect US companies—not citizens. To be covered by the Safe Harbor agreement, a US company only had to voluntarily sign up and provide

---

354 Tamara Loomis, A Few Companies Have Complied with EU Law, 228 *New York Law Journal*, 1 (2001, August 30), at 5.

355 *Ibid.*

356 Graham Pearce & Nicholas Platten, Orchestrating Transatlantic Approaches to Personal Data Protection: A European Perspective, 22 *Fordham International Law Journal* 5, 2024 (1999), 2048.

357 *Ibid.*

358 Marie Clear, Comment, Falling into the Gap: The European Union's Data Protection Act and its Impact on U.S. Law and Commerce, 18 *John Marshall Journal of Computer and Information Law* 4, 981 (2000).

359 Edmund L. Andrews, *European Law Aims to Protect Privacy of Data*, New York Times (1998, October 25), at A1.

a self-certifying declaration process.[360] Once on the list, the company's privacy protection policies are "deemed adequate." No external review occurs. Data transfers are uninterrupted and prior approvals are waived or automatically granted. The company is exempt from any member state data protection negotiations. A safe harbor company must state that it complies with EU Standards on data protection. Again, the commitment is based on a self-declaration with no monitoring or remedies. The topics include choice, ownership, transfer, access, data integrity, and dispute resolution. The standard is much less rigid than the standards in the EU.[361]

In theory, enforcement is based on the business pressures of self-regulation. Depending on the industry sector, the Department of Commerce (DOC), Department of Transportation (DOT), Federal Communications Commission (FCC), and Federal Trade Commission (FTC) have enforcement responsibility.[362] The history shows that enforcement is essentially non-existent.

As part of the original negotiations, nothing would be done from the signing date of 1 July 2001 through informal agreement in November 2001 as an informal grace period. The actual data protection principles were ignored because neither party wanted a trade war. France and Sweden blocked some data transfers with little impact. US companies have been slow to register for safe harbor status. The business mindset is that the costs outweigh the benefits, given that neither the Europeans nor the US aggressively enforced the agreements. Microsoft reluctantly joined the agreement only after Spain and Dun & Bradstreet complied. Their compliance came only after Sweden cut-off data transfers.[363] As established

---

360 European Commission, *US-EU Safe Harbor Frameworks*. (2012), at http://export.gov/safeharbor/index.asp (last visited on 4 August 2012).

361 See Chapter 3, § 3.4.3 of this work

362 European Commission, *US-EU Safe Harbor Frameworks*. (2011), at http://export.gov/safeharbor/index.asp (last visited on 4 August 2012).

363 Barry J. Hurewitz, *US - EU Privacy "Safe Harbor" Greeted with Skepticism*, Wilmer Hale. (2001), at

in Chapter Two, even if the "powers that be" are willing to establish and follow sound laws and support the rule of law, data protection and information privacy laws are meaningless unless the legal principles are enforceable.

Even if the basic safe harbor and self-regulation models were not fundamentally flawed, privacy legal problems would still persist. The Department of Commerce and the Federal Trade Commission do not have the expertise, resources, and statutory power to enforce compliance of DPSIP standards.[364] There is no objective model to show what effective enforcement would entail.

8.10 United States Sociolegal Concerns

Kim Sheehan[365] did a meta-analysis of forty-three established and respectable public opinion poll studies related to information privacy views in the US. The data showed a number of population concerns regarding information privacy. The data provided a contrast to the current legal constraints on US DPSIP law. The presentation of the data included the essential question, the number of questions in the forty-three studies examined, the measurement and the question response range.

---

http://www.wilmerhale.com/publications/whPubsDetail.aspx?publication=2367 (last visited on 22 July 2012).

364 Rachel K. Zimmerman, The Way the "Cookies" Crumble: Internet Privacy and Data Protection in the Twenty-First Century, 4 *New York University Journal of Legislation and Public Policy,* 2, 439 (2000).

365 Kim Bartel Sheehan, *How Public Opinion Polls Define and Circumscribe Online Privacy*, 9 *First Monday*, 7 (2004), http://www.firstmonday.org/issues/issue9_7/sheehan/ (last visited on 24 June 2012).

Table 8.4 Poll Meta Analysis Data

Question	Number of questions	Measurement	Question Response range
Right of Privacy	1	Degree to which is essential	81% say essential
Privacy as control over who gets information	6	Degree of importance, risk, comfort level	75–84% extremely important; 50% uncomfortable over who gets information; 75% see as a risk.
Privacy as control over collection of information	8	Degree of importance	69–74% view as extremely important
Privacy: information that can be stolen	4	Level of risk or worry	43–70% worried / extremely worried; 69% see as risk
Privacy on the Internet	9	Levels of concern	30–50% very concerned; 79–83% concerned
Financial records /credit card information	9	Level of concern	64–84% concerned/very concerned
Social Security Number (SSN)	2	Level of concern	75% very concerned
Health records	3	Level of concern	47–65% concerned/very concerned
Directory information home/phone	5	Level of concern	51–54% very concerned
Web tracking	8	Level of comfort /violation	95% uncomfortable; 43–67% agree is violation
Government access /monitoring	7	Support or oppose	65–74% oppose
Website sharing information	6	Level of concern /comfort /invasion of privacy	65–89% consider violation of privacy; 50–84% concerned; 92% uncomfortable

Government should pass laws to protect online privacy	9	Level of agreement	38–63% agree
Current laws protect consumers	6	Level of agreement	57–87% agree
Violators should be disciplined	1	Level of agreement	94% agree
Opt–in rather than Opt-out	4	Support or oppose	78–88% support
Websites should disclose policies	1	Level of agreement	93% agree

The Sheehan mega-data showed that the majority of those polled in the various studies maintained that the government should pass laws that protect information privacy. Individuals should have the power to protect their rights that include private causes of action. The data supported the view that information privacy was in trouble in the US. The people studied maintained that there was or should be a right to privacy and that people should have control over both the collection of their personal information and who gets information once collected. The subjects were concerned about information theft and about the lack of Internet privacy. The subjects were also concerned about financial and credit card information, social security numbers, health records, home, and phone directory information. The majority opposed government access and monitoring of personal data. The majority also maintained that web tracking and website sharing was a privacy violation. The majority did not think that current laws protected consumers' privacy, but they did think the government should pass more protective privacy laws, and that violators ought to receive discipline. The vast majority supported an opt-in standard, rather than the business preferred opt-out, for data collection. The vast majority also agreed that websites should disclose and follow their privacy policies. The Electronic Privacy Information Center

also tabulated a number of polls that show that privacy concerns and privacy misinformation were reported by the majority of subjects.[366]

A study of 7,088 adults, by Ipsos/Queen's University[367] found that sixty-three percent of those in the US were concerned about information privacy protections. The Angus Reid[368] study revealed that seventy percent of the sample was concerned about their privacy. The use of new technology was a major factor. Over the last three decades, opinion results supported the belief that business and government would protect information privacy; however, belief in real protections had drastically declined. Eighty–four percent of the population opposed the government placing private information on the Net, but the government did it anyway.[369]

A Harris[370] poll found eighty-three percent of Americans reported that they would stop doing business with a company that did not protect personal information. Ninety percent wanted a transparent privacy policy. Sixty-two percent wanted an independent monitor on the practices, and ninety-one percent would do business with such a firm if the practices were audited.

Table 8.5 Harris Poll

Statement	**1999 Disagreement**	**2000 Disagreement**	**2001 Disagreement**
"Most businesses handle the personal information they collect about consumers in a proper and confidential way"	34%	43%	56%
"Existing laws and organizational practices			

366 Electronic Privacy Information Center, *Public Opinion on Privacy* (2008), http://epic.org/privacy/survey/default.html (last visited on 6 April 2012).

367 Ipsos / Queen's University (2006).

368 Angus Reid Global Monitor (2006).

369 Alice Robbin, The Loss of Personal Privacy and Its Consequences for Social Research, 28 *Journal of Government Information* 5, 493 (2001).

370 Harris Interactive, *Privacy On and Off the Internet: What Consumers Want* (Study No. 15229) (Author 2002).

provide a reasonable level of protection for consumers today"	38%	47%	62%

Table 8.6 Concerns

Statement	Voiced a major concern
The company will share or sell my information to other companies with whom I have no relationship.	75%
The transaction will not be secure, and other companies or individuals may gain access to my credit card information.	70%
My personal information may be stolen and used by a hacker or intruder.	69%
I may receive unwanted advertisements for unwanted products and services (spamming or junk mail).	59%
The company will not follow the promises outlined in its privacy policy.	56%
The company will use my information outside of the specific transaction for which it was intended (, to offer me other products and services).	53%

A 2008 Consumer Report[371] poll addressed American privacy concerns. The organization was highly respected. The data showed:

Table 8.7 Consumer Concerns

Issue	Percent
Internet companies should always ask for permission before using personal information	93%
Worry about credit card data being stolen	82%
Concerned about companies tracking and profiling behavior	72%
At a minimum want to be able to opt-out	72%
Incorrectly confident that what they do online is private and not shared without their permission	61%
Incorrectly believe that companies must identify themselves and indicate why they are collecting data and	57%

[371] Consumer Reports, *Consumers Alarmed About Online Privacy, 25% Provide Fake ID to View Sites* (2008), http://www.marketingcharts.com/interactive/consumers-alarmed-about-online-privacy-25-provide-fake-id-to-view-sites-6265/ (last visited on 20 March 2012).

whether they intend to share it with other organizations	
Are uncomfortable with third parties collecting information about their online behavior	54%
Uncomfortable with Internet companies using their email content or browsing history to send them ads	53%
Incorrectly believe their consent is required for companies to use the personal information they collect from online activities	48%
Incorrectly believe a court order is required to monitor activities online	43%

Fox and Lewis[372] have conducted a number of relevant studies. They found that seventy percent of Americans supported new laws to protect information privacy. Fox found that eighty-six percent favored opt-in to data collection processes. Companies should ask permission prior to using personal data. Fifty-four percent reported that web site tracking of activities was harmful and a privacy violation. Ninety-four percent argued for legal punishment for privacy violators. Eleven percent wanted violating company owners sent to prison. Twenty-seven percent wanted violating owners fined. Twenty-six percent wanted any violating web site shut down. Thirty percent wanted a published list of privacy violating fraudulent web sites.[373]

In 2006, *Consumer Report*, a well-respected consumer publication, conducted a survey on privacy concerns in the US. The survey revealed that seventy-two percent of the respondents were concerned about the protection of their person data, including financial data.[374]

---

372 Susannah Fox & Oliver Lewis, *Fear of Online Crime: Americans Support FBI Interception of Criminal Suspects' Email and New Laws to Protect Online Privacy*, Pew Internet & American Life Project (2001), http://www.pewinternet.org/~/media//Files/Reports/2001/PIP_Fear_of_crime.pdf.pdf (last visited on 24 May 2012).

373 Susannah Fox, et al., *Trust and Privacy Online: Why Americans Want to Rewrite the Rules*, Pew Internet & American Life Project (2000), http://www.pewinternet.org/~/media/Files/Reports/2000/PIP_Trust_Privacy_Report.pdf.pdf (last visited on 7 June 2012).

374 Melissa Campanelli, *Privacy, Security Top Consumer Worries Online: Consumer Reports at FTC Forum* (2006, November 7), http://www.dmnews.com/Privacy-security-top-consumer-worries-online-Consumer-Reports-at-FTC-forum/article/93362/ (last visited on 1 January 2012), at ¶ 1.

The Truste's 2006 survey of 1,025 consumers found that privacy concerns impacted e-businesses. In the prior six months of the year, seventy-one percent did not register or buy online because of data protection and information privacy concerns. Forty-one percent of the respondents provided inaccurate information when requested for personal information.[375]

Customers were privacy conscious according to a study by a company named Javelin Strategy & Research. The data showed that seventy-seven percent of customers would no longer shop at businesses that did not protect their private data. Eighty-five percent would spend more on sites that they perceive as protecting personal data.[376] A study by Carnegie Mellon University also found that customers would pay more for goods on sites that protect their privacy.[377] A study of US online purchasers revealed that sixty-one percent were concerned about data privacy. The percentage was up from forty-seven the year before. Prior to the current time, the percentage of concern had decreased for the last five years.[378]

Independent research in all of the countries addressed in this study revealed that citizens and business executives were significantly concerned about DPSIP issues. Many of the concerns were counter to national legislation and court decisions. Politicians and jurists can and certainly do argue and maneuver around DPSIP issues. Businesses and corporations can

---

375 Cara Wood, *Web Users Have False Sense of Security: Truste, TNS*. (2006, December 7), http://www.dmnews.com/Web-users-have-false-sense-of-security-Truste-TNS/article/93762/ (last visited on 26 December 2012), at 4.

376 David Utter, *Study: Data Breaches Break Consumer Trust* (2007, April 11), http://www.securitypronews.com/news/securitynews/spn-45-20070411StudyDataBreachesBreakConsumerTrust.html (last visited on 7 December 2012), at 3-4.

377 Jon Brodkin, *Shoppers Willing to Pay Extra for Privacy Confidence, Study Finds* (6 June 2007), http://www.networkworld.com/news/2007/060607-privacy-confidence-survey.html (last visited on 2 January 2012).

378 Anick Jesdanun, Internet Privacy Concerns Rising, Study Suggests: Findings Come Amid a Record Number of Data Breaches in 2007, Associated Press (2008, January 16), at A1.

and do corrupt the process.[379] The above research shows that the majority of US citizens want strong DPSIP legislation and regulation.

8.11 United States of America Critique

Historically, US law has insisted on checks and balances to protect individuals and society. Protective mechanisms include court orders, warrants, and subpoenas.[380] Vital balances have been generally maintained. Privacy concerns were protected in the US through the Earl Warren Supreme Court. Such protections were diminished starting with the Republican-appointed Burger, Rehnquist, and Roberts courts.

Table 8.8 Expectation of Privacy Supreme Court Cases

Reasonable Expectation of Privacy Missteps	**US Supreme Court**
Generally (although not always) notice of search should be contemporaneous.	*Richards v. Wisconsin,* 520 U.S. 385 (1997).
Plain view items need no warrant.	*Coolidge v. New Hampshire,* 403 U.S. 443 (1971).
Search incidental to valid arrest – no warrant.	*United States v. Edwards,* 415 U.S. 800 (1974).
Confidential records held by a third party under contract - no warrant.	*United States v. Miller,* 425 U.S. 435 (1976).
Telecommunication data – no warrant.	*Smith v. Maryland,* 442 U.S. 735 (1979).
The government can do whatever it wants with illegally seized data.	*United States v. Janis,* 428 U.S. 433, 455 (1975).

379 See: Jeffrey D. Clements, *Corporations Are Not People: Why They Have More Rights Than You and What You Can Do About it* (Berrett-Koehler Publishers, Inc ed. 2012). Thom Hartmann, *Unequal Protection: The Rise of Corporate Dominance and the Theft of Human Rights* (Rodale ed. 2002). Robert G. Kaiser, *So Damn Much Money: The Triumph of Lobbying and the Corrosion of American Government*,(Alfred A. Knopf ed. 2009). Lawrence Lessig, *Republic, Lost: How Money Corrupts Congress - and a Plan to Stop It* (Twelve - Hachette Hook Group ed. 2011).

380 Gina Marie Stevens, *Privacy: Total Information Awareness Programs and Related Information Access, Collection, and Protection Laws (RL31730)*, U.S. Congressional Research Service. (2003), at http://www.cdt.org/security/usapatriot/030214crs.pdf (last visited on 20 July 2012).

Constitutional protections do not apply to domestic security where different policies or approaches may be needed.	*United States v. U.S. District Court for the Eastern District of Michigan,* 407 U.S. 297 (1972). p. 322

The US approach to DPSIP legal protection is ineffective. Perhaps the best evidence is found in the declaration that "Congress has granted drug abusers greater privacy protection than lawful users of the Internet."[381]

Joel Reidenberg examined the legal history of US privacy laws. The study found that "the American legal system responds incoherently and incompletely to the privacy issues raised by existing information processing activities in the business community."[382] The sectoral approach is a byproduct of history, political conflicts, free market mythologies, lack of historical knowledge, and a lack of public awareness. The patchwork approach worked for some of the time in some areas; however, large protection gaps exist.

Daniel Solove declared that the "existing law protecting information privacy has not adequately responded to the emergence of digital dossiers."[383] Charles Weiss concluded that "American values on privacy were defined in a previous, less technological era. These values needed to be reexamined and redefined for a modern era of data mining and knowledge discovery."[384]

The US has refused to follow a comprehensive approach in lieu of English common law, the various cultural standards in the Western World, ethnocentric social traditions, and partisan politically established statutory law. The US is at variance with other Western countries and has a recent thirty-

---

381 Joel R. Reidenberg, E-commerce and Trans-Atlantic Privacy, 38 *Houston Law Review* 77, 717 (2001), at 726.

382 Joel R. Reidenberg, Privacy in the Information Economy-- A Fortress or Frontier for Individual Rights? 44 *Federal Communications Law Journal* 2, 195 (1992), at 199.

383 Daniel J. Solove, *The Digital Person: Technology and Privacy in the Information Age* (New York University Press. 2004), at 9.

384 Charles Weiss, The Coming Technology of Knowledge Discovery: A Final Blow to Privacy Protection, 2004 *University of Illinois Journal of Law, Technology and Policy* 2, 253 (2004), at 271.

year history of being a privacy rogue nation. Either privacy laws are passed but ignored or new "privacy" legislation is passed that destroys traditional privacy rights. Some governmental restrictions exist; however, businesses can do what the market will bear, while the government circumvents legal restrictions by allowing and then buying or requesting private corporations to provide information that was illegal for the government to obtain directly.

The US Government Accountability Office[385] issued a privacy report and testified on the need for the US to pass a new privacy law. The report found that current US privacy legislation[386] is inadequate to meet current needs. The definition of "system of records" is unclear and not consistently followed. Public notices are difficult to find and do not specify the real purpose of the information collection. The enacted fair information standards are not followed. The Accountability Office recommended "Applying privacy protections consistently to all federal collection and use of personal information. Ensuring that use of personally identifiable information is limited to a stated purpose…Establishing effective mechanisms for informing the public about privacy protections."[387] The current laws do not protect data mining processes, and the Government is circumventing the law by buying or getting information from other sources.

The report concluded with measured recommendations. The evaluation included "(1) the Privacy Act and E-Government Act do not always provide protections for federal uses of personal information, (2) laws and guidance may not effectively limit agency collection and use of personal information to specific purposes, and (3) the Privacy Act may not include effective mechanisms for informing the public."[388]

---

385 United States Government Accountability Office, *Congress Should Consider Alternatives for Strengthening Protection of Personally Identifiable Information*. (2008, June 18), at http://www.gao.gov/new.items/d08795t.pdf (last visited on 18 June 2012).

386 See §§ 8.3.6 and 8.3.7 of the Chapter.

387 *Id.* at 1.

388 *Id.* at 21.

The Privacy Act has systemic problems. The Act was shortsighted and included a number of problematic exceptions. Moreover, the Act applied only to governmental agencies that had their own system of records. In *Henke v. United States Department of Commerce*[389] the Court ruled that data retrieval was not controlled under the act.

Protecting informational privacy has been a transient priority in the legal tradition of the US. Free speech and information privacy protections are, in reality, complimentary. The legal principle "allocates rights and responsibilities" while insuring "fairness and transparency in the collection and use of personal information."[390] The recent development of a self-regulation policy is not working, and people in the US are becoming increasingly concerned. The DPSIP self-regulation movement started in 1996 by President Clinton and was expanded under Bush W. The Office of Management and Budget and the Federal Trade Commission "lack the statutory authority, the resources, and the reporting requirements to operate effectively on privacy issues. There are too many complaints, too little adjudication, and too little oversight."[391]

While states in the US led the way for breach notification laws, the legislation has not always been effective.[392] Bruce Schneier, Chief Security Technology Officer at the BT Group, reported that such laws have loopholes, like limited

---

389 *Henke v. United States Department of Commerce*, 83 F.3d 1453, 1461 (D.C. Cir. 1996) (quoting Bartel v. FAA, 725 F.2d 1403, 1408 n.10 (D.C. Cir. 1984). (1996). (US)

390 Marc Rotenberg, *Privacy in the Commercial World: Subcommittee on Commerce, Trade, and Consumer Protection, House Committee on Energy and Commerce*. (2001, March 1), at http://energycommerce.house.gov/reparchives/107/hearings/03012001Hearing43/Rotenberg68.htm (last visited on 21 August 2012), at 2.

391 Marc Rotenberg, *Privacy in the Commercial World: Subcommittee on Commerce, Trade, and Consumer Protection, House Committee on Energy and Commerce*. (2001, March 1), at http://energycommerce.house.gov/reparchives/107/hearings/03012001Hearing43/Rotenberg68.htm (last visited on 21 August 2012), 4.

392 As of 1 October 2011 only Alabama, Kentucky, New Mexico and South Dakota had no breach notification statutes.

notification standards. As in the UK, penalties are not a significant deterrent.[393]

In many cases, security breaches are not reported. "One reason is that the penalty for failing to disclose a breach under state laws is often minimal—just a maximum of $10,000—less than a business might spend figuring out which records were stolen in the breach."[394]

The legal and judicial history of DPSIP in the US is a source of cognitive dissonance and a *schizoid* approach to problem solving. When it was revealed that Supreme Court nominee Judge Bork liked to rent pornographic films from his local video store, his fellow conservative and Republican legislators cried that such data should be private and passed a special legislation protecting video rental. The same legislators invalidated the law after the World Trade Center attack.

The US courts have recently developed a pernicious doctrine to limit individual privacy rights against business and governmental desires. The reasonable expectation of privacy doctrine[395] was used to protect business and governmental abuses and agendas. The burden of proof is placed on the victim so that the more powerful are not held accountable.

A classic case in support of this assessment was *United States v. Miller*.[396] In a case of financial privacy violations, the Supreme Court ruled that there were no constitutionally protected privacy rights for banking records. Making deposits and writing checks voluntarily places the information available to another party and to the flow of commerce. The disclosing party thus bears the risk of whatever actions businesses or the government may take. Courts followed the new doctrine and denied privacy protections to information to

---

393 Ben Worthen, *Why All The Data Breaches? Businesses Just Don't Care*. (2008, September 9), at http://blogs.wsj.com/biztech/2008/09/09/why-all-the-data-breaches-businesses-just-dont-care/ (last visited on 9 September 2012), at 6.

394 *Ibid.*

395 *Katz v. United States*, 389 U.S. 347, 88 S.Ct. 507, 19 L.Ed.2d 576, (1967). (US).

396 *United States v. Miller,* 425 U.S. 435, (1976). (US)

banks, dialed telephone numbers, and trash left in trash bags because the data was voluntarily placed in commercial flows.[397]

In *United States v. Kennedy*,[398] the defendant provided information to his Internet Service Provider to open and maintain an account. The Court determined that since the defendant had voluntarily provided personal information for the service, he had no reasonable expectation of privacy concerning his ISP records because he knowingly revealed the information to obtain the service.

The legal standard changes when a corporation is involved. Corporations have the legal right to protect their informational property and relationship channels.[399] There is no test of reasonable expectation of privacy. Why does such a dual standard exist?

Under current DPSIP legal standards, businesses and the government are not regulated by any standard of assessment, evaluation, plan, or review. All can collect, sell, and use personal information freely. International standards are ignored with no recourse.

After the Watergate scandal, Senator Frank Church established the Select Committee to Study Government Operations with Respect to Intelligence Activities.[400] Church, a Democrat from Idaho, served as Committee Chair. Congress passed the 1978 Foreign Intelligence Surveillance Act (FISA), which established special courts of review for national security warrants and intervention reviews.[401] However, the legal lesson was learned for only a

---

397 *Smith v. Maryland*, 442 U.S. 735, (1979); U.S.: *California v. Ciraolo*, 476 U.S. 207, (1986); *California v. Greenwood*, 486 U.S. 35, 108 S.Ct. 1625, 100 L.Ed.2d 30, (1988). (US)

398 *United States v. Kennedy*, 81 F. Supp. 2nd 1103 (D. Kan., 2000). (US)

399 *Felsher v. University of Evansville*, 755 N.E. 2d 589 (Ind. 2001). (US)

400 Frank Church, *Senate Select Committee to Study Government Operations with Respect to Intelligence Activities, 94th Congress, Final Report on Intelligence Activities and the Rights of Americans* (United State Printing Office. 1976, April 26).

401 Foreign Intelligence Surveillance Act (FISA) amend. Public Law 95-511, 92 Stat. 1783 (1978) (codified at 50 U.S.C. § 1801-1811) (1978). (US)

short period of time. By 2001 and the era of the Bush Administration, the US Patriot Act was passed; this law changed the FISA processes.[402] The entire process was then suspended in the name of national defense.

The Department of Defense Technology and Privacy Advisory Committee's (TAPAC) final report documented that US privacy protection laws and judicial precedents are disjointed, inadequate, and outdated.[403] For example, The Electronic Communications Privacy Act (ECPA)[404] made a clear regulatory distinction between *in storage* and *in transit,* which is no longer meaningful. The government used such distinctions to violate the spirit of the law and user's expectations.[405] The Act suffered from poor development or intentional inconsistencies. For example, the Act applied to video surveillance only when sound was recorded at the same time.

The problems of DPSIP law in the US are not as complex as they are *schizoid*. There is no independent regulatory function for such concerns. The federal government does not require reporting or accountability or state actions. The Executive Branch ignores and violates statutory protections with immunity. Congress is beholden to special interest lobbies and failed political philosophies. Congress is either slow to change or jumps on the current call for action. In 1934, Congress passed the Communications Act,[406] which outlawed wiretaps of all types. A complete reversal was done in 1968 with the Omnibus Crime Control and Safe Streets Act.[407] Congress passed laws but did not effectively require any accountability or oversight. Even the Supreme

---

402 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 amend. Public Law 107-56, § 204, 115 Stat. 272 (codified at 50 U.S.C. § 1804(a)(7)(B)). (2001). (US)

403 United States Department of Defence Technology and Privacy Advisory Committee, Safeguarding Privacy in the Fight Against Terrorism (Author. 2004, March), 6.

404 *Electronic Communications Privacy Act of 1986* (ECPA Title I) 18 U.S.C.A. §§ 2510-2521 (1986). (US)

405 *United States v. Scarfo*, 180 F. Supp. 2d 572 (D.N.J. 2001) (US)

406 *Communications Act of 1934* amend. ch. 652, § 605, 48 Stat. 1064 (codified as amended at 47 U.S.C. § 605) (1934). (US)

407 *Omnibus Crime Control and Safe Streets Act of 1968*, Pub. L. No. 90-350, 82 Stat. 197 (codified as amended at 18 U.S.C. § 2511-2520) (1968). (US)

Court was not exempt from a pattern of non-accountability and lack of consistent oversight. In *Olmstead v. United States,*[408] the Court refused to apply the Fourth Amendment to wiretaps. Thirty-nine years were required for the Court to reverse the error in *United States v. Katz*.[409]

The US approach to Privacy Impact Assessment (PIA) issues is at best, schizoid. Congress has suggested that the government require PIA standards for new technology – if practicable. However, the implementation of the policy has not been swift or uniform. Kenneth Bamberger[410] studied how agencies deal with mixed legislative policies and subvert the process.

A number of United States Supreme Court anti-information privacy decisions must be overturned or legislatively corrected. The legal fiction of requiring a reasonable expectation of privacy doctrine must be voided. According to the *United States v. Miller*[411] decision, bank records are not protected by the Fourth Amendment because there is no confidentiality and the information is freely given to the bank. The ruling must be over-turned. In *Smith v. Maryland*,[412] the court found no reasonable expectation of privacy for dialed phone numbers because the numbers were voluntarily disclosed and recorded during phone company business activities. This ruling also needs to be over-turned.

As early as 1987, Spiros Simitis[413] showed that in the US, all sectors of the government - courts, executive, and legislative failed to establish DPSIP protections. The pursuit of governmental power and business profits trumped civil liberties-rights, consumer protection-safety, data security, market

---

408 See *Olmstead v. United States* (1928). (US)

409 See *United States v. Katz* (1967). (US)

410 Kenneth A. Bamberger, Regulation as Delegation: Private Firms, Decision-making, and Accountability in the Administrative State, 56 *Duke Law Journal* 2, 377 (2006).

411 See *United States v. Miller* (1976). (US)

412 See *Smith v. Maryland* (1979). (US)

413 Spiros Simitis, Reviewing Privacy in an Information Society, 135 *University of Pennsylvania Law Review* 3, 707 (1987, March).

fairness, and governmental security protections. In 2002,[414] the federal government established a standard that at lest federal administrative agencies must conduct a PIA when agencies develop or purchase information technologies or change current systems when there is a privacy risk. The standard was not fully implemented and not extended to the private sector.

By 2009, the Office of Management and Budget reported that only fifty-six percent of federal agencies were in compliance with the 2002 act requiring PIAs. The data was reported based on agency self-reports.[415] The lack of adoption was based on the lack of public input into the process and neo-conservatives refusing to appoint the required chief privacy counsel in the Office of Management and Budget. Neo-conservatives successfully re-framed privacy issues as a danger to national security concerns.[416]

Data protection and information privacy law in the United States is essentially a legal fiction and failure. The good news is that other countries have established sound protections. Substantive DPSIP laws are needed to limit access to and misuse of personal data that apply to all governmental, business, organizational, and personal actors. Procedural DPSIP laws and rules are needed to support compliance, provide accountability, monitor failures, insure remedies, and allow private causes of action. Strict liability standards should apply. An independent regulatory body with full rule making, enforcement, adjudication powers, and educational powers must be established. The regulatory agency must have strict rules to protect it from corporate and governmental interference. The standards of the rule of law must apply. DPSIP audits should be required for all related programs and

---

414 *E-government Act* amend. (Pub.L. 107-347, 116 Stat. 2899, 44 U.S.C. § 101, H.R. 2458/S. 803) § (2002) (US).

415 Office of Management and Budget., *Fiscal Year 2009 Report to Congress on Implementation of the Federal Information Security Management Act of 2002*. (2009), at http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/FY09_FISMA.pdf (last visited on 12 March 2012).

416 See Kenneth A. Bamberger & Deirdre K. Mulligan, PIA Requirements and Privacy Decision-Making in US Governmental Agencies, in *Privacy Impact Assessment* (David Wright & Paul De Hert ed.^eds., Springer 2012).

databases, proposed projects or business concerns, intellectual property protections, and all governmental actions that impact on privacy.

At times, task forces and committees can perform some insightful work; however, if someone did not want to deal with the issue, he or she referred it to a committee. A number of taskforces and committees have considered the issue of security and information privacy in the United States. The blue ribbon panels included the Markle Foundation Task Force on National Security in the Information Age,[417] McCormick Tribune Foundation's Cantigny Conference on Counterterrorism Technology and Privacy,[418] US Department of Defense Technology and Privacy Advisory Committee,[419] and the United States Department of Homeland Security.[420] A review of the recommendations of these committees reveals two general truths. Each report made similar recommendations, which suggested an acceptance of a standard data protection perspective similar to the EU approach. Second, the majority of recommendations were ignored or failed to attend to DPSIP concerns, which suggested that the *powers that be* were going to do what they wanted despite the evidence and the demands of the citizens. The government and business were not interested in consistent DPSIP laws and reforms.

As noted above, the various states in the US have been advancing DPSIP issues far more often and effectively than the federal government. Over the

---

417 Markle Foundation Task Force On National Security In The Information Age, *Mobilizing information to prevent terrorism: Accelerating development information sharing of a trusted environment* (2006, July), at http://www.markle.org/downloadable_assets/2006_nstf_report3.pdf (last visited on 1 December 2012).

418 McCormick Tribune Foundation's Cantigny Conference On Counterterrorism Technology and Privacy, The Cantigny Principles on Technology, Terrorism, and Privacy. 27 *National Security Law* Report 1, 14 (2005), at http://www.abanet.org/natsecurity/nslr/2005/NSL_Report_2005_02.pdf (last visited on 22 September 2012).

419 United States Department of Defence, Technology and Privacy Advisory Committee, *Safeguarding Privacy in the Fight Against Terrorism*. (2004, March), at http://www.cdt.org/security/usapatriot/20040300tapac.pdf (last visited on 5 December 2012).

420 United States Department of Homeland Security, *Privacy Office - DHS Data Privacy and Integrity Advisory Committee*. (2008), at http://www.dhs.gov/xinfoshare/committees/editorial_0512.shtm (last visited on 10 December 2012).

last year, Congress has proposed some information privacy legislation; however, no real actions have been taken. Some proposals, if passed, will preempt state legislative efforts. Thus, such a federal DPSIP law will actually diminish established state protections.

On 23 February 2012, the White House released a consumer privacy bill of rights.[421] The document supports the view that DPSIP issues are a major concern and have reached historic proportions. Privacy is not outmoded as it is the heart of a democracy and a necessary consumer protection issue. The privacy bill of rights includes provisions for individual control of personal information, transparency of privacy and security practices, and respect of context related to private commercial organization and data-broker DPSIP practices. The bill establishes that consumers have a right to data security of their information. Consumers have a right of accuracy and access. Consumers also have a right to limits on personal data collection and retention. Consumers also have an accountability right that organizations adhere to the bill of rights.[422]

The Executive would prefer that the federal Legislature pass the Consumer Data Privacy Bill of Rights as a federal statute. If the Legislature fails to enact the principles, the Executive argued that the bill of rights provides for a non-statutory template for DPSIP protections that would increase consumer trust and innovation.[423] The document suggests that enforcement of DPSIP principles should be assigned to the FTC and States Attorney Generals. The goal is to create US DPSIP standards that establish and maintain increased international DPSIP interoperability.

---

421 The White House, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy. (2012), at http://www.whitehouse.gov/sites/default/files/privacy-final.pdf (last visited on 23 February 2012).

422 *Id.* at 1.

423 *Id.* at 2.

While the document does not shift the historic US DPSIP self-regulation model, it does declare that such efforts are preliminary. The document advocates that strong governmental enforcement powers are also needed through the FTC.[424] The *Consumer Data Privacy Bill of Rights* proclaimed rights of individual control, transparency, respect for context, and security. The rights also include access and accuracy, focused collection, and accountability.[425]

The Whitehouse publication of the *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*[426] is a recognition of DPSIP legal and regulatory issues. The document may be politically acceptable; it actually limits progressive state actions and ignores international DPSIP legal trends. In reality, the proposal is understandably, a dollar short and a day late.[427] The document focuses on private organizational practices while ignoring governmental practices.

8.12 Summary of United States of America Literature and Issues Reviewed

The intent of this thesis is to conduct a comparative analysis of DPSIP responses in five different nations. Part of the comparison uses a benchmark approach of key issues. The issues include legal support of DPSIP protections, legal support of corporate privacy and data protection standards, information privacy data protection and security declarations, the use of regulatory agencies, sectoral legislation, and data controllers. The benchmark standards also include data processor requirements, data

---

424 *Id.* at 29.

425 *Id.* at 47–48.

426 The Whitehouse, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*. (2012), at http://www.whitehouse.gov/sites/default/files/privacy-final.pdf (last visited on 23 February 2012).

427 An idiom for an action that is too little and historically too late – ignorant of the evolution of international DPSIP standards.

subjects, data security destruction, cross-border data flow, exemptions and exceptions, and the current stage of the approach based on evolutionary stages. The following table presents the summary based on the benchmark model.

Table 8.9 Comparative Model of US Legal Support of DPSIP Models

ISSUE DESCRIPTION	US CURRENT RESPONSE
CM.1: Legal Support of DPSIP Protections	
Signatory, Adheres, and/or Complies with International Human Rights Standards	(See Appendix A.)
Signatory, Adheres, and/or Complies with EU DPSIP Standards	No
Signatory, Adheres, and/or Complies with APEC DPSIP Standards	Yes
Federal Constitutional Law	Examples are given but the term is not directly used.
Federal Legislative Efforts	Contradictory
Federal Common Law	Limited
Province /State Constitutional Law	Some (e.g., California)
Province / State Legislative Efforts	Some
Province /State Common Law	Some

CM.2: Legal Support of Corporate Privacy and Data Property Protection Issues	US CURRENT RESPONSE
Copyright Protections	Yes
Database Protection	Yes
Patient Protections	Yes
Service Mark Protections	Yes
Trade Mark Protections	Yes
Trade Secret Protections	Yes
Privacy Impact Audit Required Before Use	No
Privacy Impact Audit Required Before Government Protections Granted	No
Checks and Balances on Corporate Collection, Use, and	No

Transfer of Individual DPSIP Data	

CM.3: Information Privacy: Data Protection and Security Declarations	**US CURRENT RESPONSE**
Definitions Provided	Some; self-regulatory guidelines.
Personal and Sensitive Data Defined	Guidelines
Definitions Effectively Address Advanced Data Mining Technologies	No
All Holders and Users Held Accountable	No

CM.4: Regulatory Agency	**US CURRENT RESPONSE**
Independent of Legislative and Executive Branches	None to Limited
Administrative Power	None to Limited
Investigative Power	None to Limited
Regulatory Powers	None to Limited
Education Function	None to Limited
Enforcement Powers	None to Limited
Structure	None to Limited
Responsibilities Defined	None to Limited
Accountability	None to Limited
Governmental Chief Privacy Officer/ Commissioner Required	None to Limited
Governmental Privacy Audits Required as Part of Legislation Passage	No
Business Chief Privacy Officer/ Commissioner Required	None to Limited. Health exception.
Employees are Personally Liable for Violations	None to Limited
Business Privacy Audits Required	None to Limited
Agency Educational Function	Limited

CM.5: Sectoral DPSIP Legislation	**US CURRENT RESPONSE**
Credit Reporting Agencies	Some
Criminal Justice Record Restrictions	Some
Health Information	Yes
Health Information Exceptions	Limited
Electronic Medical/Health Record Controls	Limited

CM.6: Data Controllers	US CURRENT RESPONSE
Notice Required	Limited
Opt-in	Limited
Opt-out	Some
Must Be Lawful and Fair	In theory
System Access Controls	In theory
Data Quality And Integrity	In theory
Accurate	In theory
Complete	In theory
Up to Date	In theory
Limited to Needed Data	In theory
Relevant	In theory
Not Misleading	In theory
Data Retention Limitation	In theory
Data Transfer Controls	In theory
Openness on Information Held	In theory
Breach Disclosures Required	Some
Breach Penalties	Limited

CM.7: Data Processor Requirements	US CURRENT RESPONSE
Informed Consent Required	In theory
Rationale is Provided	In theory
Fair Processing	In theory
Legal Processing	In theory
General Data	In theory
Sensitive Data	In theory
Accuracy	In theory
Timely	In theory
Duration of Record Keeping Controls	Limited

CM.8: Data Subjects	US CURRENT RESPONSE
Ownership by the Subject	No
Control Over Access	In theory
Alter, Amend, Correct, and Delete Errors	In theory
Notification Requirement	In theory

CM.9: Data Security and Destruction	**US CURRENT RESPONSE**
Security Must Be State of the Art	Limited
Technology Use – Cost of Implementation Not a Defense	No

Tracking	No
Safeguards Required	In theory
Protects from Alteration	In theory
Protects Against Disclosure	In theory
Protects Misuse	In theory
Protects Against Unauthorized Internal and External Access	In theory
Unauthorized Access Penalties	In theory
Timely Notice of Breaches	In theory
Strong Remedies Provided	No

CM.10: Cross-Border Data Flow	**US CURRENT RESPONSE**
Individual Informed Consent Required	Limited
Transfer Source Is Accountable	No
Outsource Service Controls	No

CM.11: Exemptions and Exceptions	**US CURRENT RESPONSE**
Only Permitted With Compelling Justification	In theory
Checks and Balances – Court Order Required	No
Government Agencies	No
Intelligence and Defense	Yes
Police Actions	Yes
Small Business Exemption	No

CM.12 DPSIP Evolutional Stages	**US CURRENT RESPONSE**
DPSIP.0 Limited DPSIP legal Issues	Yes
DPSIP.1.0 Establishes PII; does not fully address security issues; focus on limited legal consent and notice.	Yes
DPISP.2.0 Accepts PII standards; does not fully address security issues; focus on a legally based harm based analysis.	In theory
DPSIP.3.0 PII and non-PII data fused; privacy, data protection and security issues are interrelated; legal audits, checks, and balances needed for all personal	No

information stakeholders. New technologies are required to pass privacy audits (e.g., RFID, Internet of Things) and require use of privacy enhancing technologies in all new IP approvals.	

Sameer Hinduja[428] reported research data on privacy and public views. A total of 71.5 percent of a sample of 1,482 subjects reported that Internet privacy laws should be developed and implemented. A total of 77.5 percent of the sample chose privacy over convenience. His work concluded,

> The collection of data and its exploitation for commercial gain, its unauthorized distribution to third parties, and the archiving and storage of that data for interminable periods of time weakens the civil protections of freedom of association and privacy. Self-regulation is ineffective, and legislation appears to be the only way to best serve the citizenry of the United States, and to prevent American companies from taking advantage of the online consumer.[429]

Consumer Policy Solutions conducted a study of 1,035 adults and 260 pairs of parents and teens. The data showed that 97 percent reported that privacy protections were somewhat or very important while 95 percent said that the safety of the Internet was somewhat to very important.[430] However, the US government executive, legislative, and judicial branches have done little to meet the threats. The public policy in the US does not meet the basic regulatory standards of AU, CA, the UK, and the EU. However, some state governments have advanced innovations like breach notification.

---

428 Sameer Hinduja, Theory and Policy in Online Privacy, 17 *Knowledge, Technology, & Policy* 1, 38 (2004), at 55.

429 *Ibid.*

430 K. C. Jones, *Online Safety, Privacy Tops Parents' Concerns*, Information Week. (2008, July 22), at http://www.informationweek.com/news/security/client/showArticle.jhtml?articleID=209400624 (last visited on 22 July 2012), at 3.

Chapter Nine compares and contrasts DPSIP standards in AU, CA, SA, the UK, and the US. The chapter reviews what can be learned from the historic experiences, strengths, trends, and weaknesses of each approach. The chapter shows that SA should[431] consider establishing sound, modern, and effective DPSIP laws and regulation.

[431] Should, ought to but not necessarily will.

CHAPTER NINE: DATA PROTECTION AND SECURITY LAW: COMPARATIVE EVALUATION

The current study is a comparative analysis of data protection and security legal standards in five countries. The purpose is to present to SA suggestions on the next strategic step in DPSIP legal protections. This interdisciplinary study integrates comparative, positive, and sociolegal approaches. Rather than applying an isolated legal perspective, the author integrates a behavioral, business, jurisprudence, legal, philosophical, and psychosocial perspective because the law does not function in isolation from the human condition

9.0 Overview of the Chapter

This chapter provides a summary of the research findings proposed in Chapter One. The chapter will show that, from an academic perspective, bifurcation of information privacy, data protection, and data security is in some people's self interest; however, from a legal perspective, bifurcation of information privacy, data protection, and data security is not justified. The comparative positive law analysis of the subject countries will involve independent socio-legal data that will be presented. A meta-analysis of the subject countries' analysis of legal and policy approaches will be examined. The legal justifications for DPSIP will be explored. The chapter will present a textual analysis of international and specific national DPSIP statutes to aide in the understanding of current issues and future developments of DPSIP law in SA and the international community.

9.1 Summary of Research Question Findings

The basic questions and objectives investigated in this thesis were based on Sir Edward William Cooke's legal interpretation standards set in *Heydon's*

Case.[1] The issues were addressed as they relate to the legal challenges of DPSIP legal concerns. The summary includes the general and specific research questions posed, and the author's responses based on the research findings.

1. **What was the common law before the advent of personal information becoming a commodity and means of social control?** Before the evolution to the information age and advances in information technology, each country and geographical area addressed DPSIP legal issues based on local cultural and legal standards. Minimal threats to privacy existed because of the time and effort needed to compile massive amounts of information.[2]

2. **What was the mischief and defect for which the common law did not provide?** The common law focused on past principles and was ill prepared for massive accelerated information change. Specifically, the common law principle of stare decisis[3] was ill prepared for massive business, economic, political, social, and technological shifts. The common law standard was reactive rather than proactive, and it was ill prepared for new threats that were based on greed and social control by business and government policies. Governments claimed that the end justified the means; businesses claimed the divine rights of kings and queens to harvest profits.[4]

3. **What comparative legal principles and procedures formed the "cure for the diseases" of the invasions of DPSIP?** The current study has explored the legal justifications for DPSIP legislation and regulation based on the best practices of the countries studied. International and social legal data supports the solution.

---

[1] *Heydon's Case* 76 Eng. Rep. 637, (1584). (UK)
[2] See § 1.1 and 2.4.1 of this study.
[3] Stare decisis means to stand by things decided.
[4] For a chronology from 1791 to 2011, see Robert Gellman & Pam Dixon, *Online Privacy*, (Contemporary World Issues, ABC-CLIO ed. 2011) at 107-126.

4. **How can SA best respond to the DPSIP law principles?** The current chapter proposes specific recommendations that SA should and must consider to meet and extend international DPSIP standards. SA can ignore international DPSIP standards, follow the trend, or advance DPSIP protections.

The general research questions were as follows:

1. **Could the law effectively respond to the fundamental DPSIP legal principles raised by computer technology and the information economy violations?** In some of the countries and areas analyzed in this study, international-specific and country-specific DPSIP laws do respond to DPSIP issues effectively. Even effective DPSIP legal approaches must be periodically re-evaluated to meet current deviant practices.

2. **What were the national and international legal standards related to DPSIP legal principles before the advent of computer technology and the information economy violations**? Some countries (e.g., the US) developed privacy-related tort violations. Other countries (e.g., the UK and SA) resisted such an approach. Early responses to the technology threat were generally advisory guidelines.[5]

3. **What DPSIP flaws and defects did the computer technology and the information economy create that the existing law did not adequately protect?** Justice Michael D. Kirby summarizes the AU view of DPSIP issues. He argues that historically information privacy has been protected by costs, inconvenience, impermanency, and indexing problems. The privacy concerns that began with the modern computer era in the 1980s have increased due to technical developments that have raised the accessibility, power, storage

[5] For a historical and legal analysis see Gini Graham Scott, *The Death of Privacy: The Battle for Personal Privacy in the Courts, The Media, and Society*, (Changemakers Publishing and Writing ed. 2011). See Chapter 3 of this study.

capacity, and speed of computer processing. Justice Kirby argues that the right to confidentiality of communications, honor, privacy, and reputation must be protected.[6]

4. **What DPSIP legal principles and procedures should form the "cure of the diseases" of the new information economy violations**? SA has the option of passing legislation that brings it into the general EU DPSIP 2.0 standards or moving to address the more current DPSIP 3.0 standards.[7] The data from the current study argues that all of the countries in the study must move towards adopting DPSIP 3.0 legal standards.

5. **How can the law best respond to computer technology and the information economy challenges of fundamental principles of DPSIP law?** SA has the option of passing legislation that brings it into the general EU DPSIP 2.0 standards; otherwise, it can move to address the more current DPSIP 3.0 standards.[8] The data from the current study supports the argument that all of the countries in the study must move to adopting DPSIP 3.0 legal standards.

Specific research questions were as follows:

1. **Can DPSIP be protected from computer technology and the information economy violations?** Appropriate laws, regulations, incentives, and structures can require that business and government organizations comply with DPSIP 3.0 standards.[9] The basis of the approach must be interdisciplinary, comparative, progressive, and based on the rule of law.

---

[6] The Hon Justice Michael D. Kirby, Privacy in Cyberspace, 21 *University of New South Wales Law Journal* 2, 323 (1998), at 323. See also §§ 1.2 and 2.3 of this study.
[7] See § 9.6 of this chapter.
[8] See § 9.6 of this chapter.
[9] Richard H. Thaler & Cass R. Sunstein, *Nudge: Improving Decisions About Health, Wealth, and Happiness*, (Yale University Press ed. 2008).

2. **What were the appropriate DPSIP laws, and what were they based on?** The current study has addressed this essential question. The author argues[10] that the basis of an effective DPSIP legal approach must be interdisciplinary, comparative, progressive, and based on the rule of law as noted above.

3. **How are DPSIP legal principles violated?** Businesses and governments violate DPSIP legal principles because of greed, negligence, and weakened technology standards. Legislative corruption and judicial recalcitrance have delayed, weakened, and violated basic rule of law principles. Some political leaders in the countries studied seek a democracy that protects civil and human rights; whereas, others seek a corporate republic that serves corporate interests and a fascist state.

4. **Should DPSIP legal principles ever be violated?** No. However, when legal justification exists, with court approval and established checks and balances, certain reasonable and unambiguous established exemptions must be allowed.

5. **Does a proposal exist on how to best establish DPSIP law protections?** Respectfully, the current study and recommendations in this chapter present a proposal on how SA and the other countries in the study can best establish effective DPSIP legal protections. The basic recommendation conflicts with some business and political interest groups' positions as has been seen in the opposition to the SA proposed DPSIP law. The charge of the study is that the issues must be periodically re-evaluated. To be effective, DPSIP laws and regulations must become proactive rather than reactive. The only way to meet this challenge is to establish an independent authority to monitor developments in the field that has the power and authority to regulate and adjudicate DPSIP issues.

---

[10] See Chapters 3 through 9 of this study for the author's rationale.

The current study replicates and validates the findings of previous independent studies on international DPSIP efforts.[11] Countries like SA[12] have yet to fully establish DPSIP legal principles. The US has failed because of a policy and legal commitment to self-regulation. The self-regulation policy has allowed corporations and government agencies to use personal information data as they see fit. As noted in previous chapters, the data protection response of the EU, AU, CA, and the UK have resulted in some legal and policy failures.

In all of the countries in this study, DPSIP protections remain a concern. Many of the national laws explored in this study have not adapted to technological advancements. Significant protection gaps exist because of inadequate enforcement and monitoring. Those countries that have stronger DPSIP laws exempt police services from any DPSIP responsibilities or even warrants. Countries like the US and AU exempt many businesses.[13] Companies in all of the countries ignore DPSIP policies and claim ownership of and use data for marketing purposes.[14]

Organizations in the countries studied in this work are constantly collecting and retaining more information regarding more people. Such collection continues even when a person has opted out. The data is used for purposes that are not transparent, and the information is often shared with other businesses and government organizations. Few DPSIP laws provide an individual right of action, and even when an individual right exists, the

---

[11] See Global Internet Liberty Campaign, *Privacy and Human Rights: An International Survey of Privacy Laws and Practice*. (2008), at http://www.gilc.org/privacy/survey/intro.html (last visited on 16 July 2012) and Privacy Protection Study Commission, *Personal Privacy in an Information Society*. (1977), at http://www.epic.org/privacy/ppsc1977report/ (last visited on 29 July 2012).

[12] As of 20 August 2013, SA has passed the POIP Act. At the time of this writing, the bill has not been signed.

[13] See Chapters 4 and 8 in this study.

[14] Global Internet Liberty Campaign, *Privacy and Human Rights: An International Survey of Privacy Laws and Practice*. (2008), at http://www.gilc.org/privacy/survey/intro.html (last visited on 16 July 2012)

standards for damages are unrealistic. Technology developers do not insure that protections are protected by design.[15]

9.1.1 Is the Bifurcation of Information Privacy, Data Protection, and Data Security Justified?

Jack M. Balkin[16] recognizes the existence of surveillance states. The essential question is whether governments will protect the people and require that both public and private surveillance conform to the rule of law. DPSIP laws and regulations that apply to private and public information gathering and use are critical to maintaining the rule of law.

Information privacy is the term used in the US; *data protection* is the term used in most of the world. *Data security* refers to information technology practices and standards to make data and systems secure. For some time, the two fields were considered to be different. Information privacy and data protection were considered to be topics of legal concern. Data security was considered to be an area of interest in information technology and risk management.[17]

Such a bifurcation may be academically viable; however, the two areas are interconnected.[18] One cannot have data protection without data security. The reverse is also true. DPSIP legislation and regulation must address issues related to both protection and security.

---

[15] Privacy Protection Study Commission, *Personal Privacy in an Information Society*. (1977), at http://www.epic.org/privacy/ppsc1977report/ (last visited on 29 July 2012).

[16] Jack M. Balkin, The Constitution in the National Surveillance State, 93 *Minnesota Law Review* 1, 1 (2008), at 3-4. See also Jack M. Balkin, The Constitution in the National Surveillance State, in *The Constitution in 2020* (Jack M. Balkin & Reva B. Siegel eds., Oxford University Press 2009) at 198.

[17] See Susan Landau, *Surveillance or Security? The Risks Posed by New Wiretapping Technologies*, (The MIT Press ed. 2010).

[18] See § 3.3.7 of this study.

9.2 Legal Analysis

The focus of this study included a sociolegal analysis of DPSIP issues. The study included a comparative law - business practices, analysis. A positive law analysis was also conducted. The focus addressed DPSIP issues internationally and in five different countries.

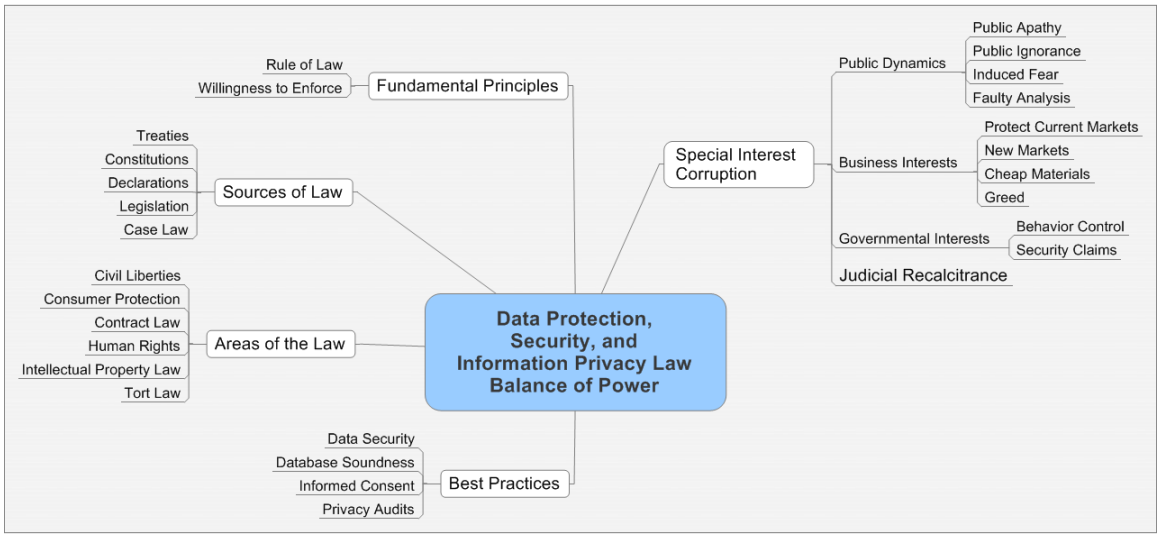
9.2.1 Sociolegal Analysis

The analysis included a review of fundamental principles of the rule of law and sources of law. The relevant areas of the law were presented. The study explored data on special interest corruption issues. The problems of willingness to enforce DPSIP standards were explored.

Relevant sources of DPSIP laws were examined. Related areas of the law were addressed. The study concludes with a review of DPSIP 3.0 best practices. The following figure graphically presents the mind map[19] used to analyze related connections.

[19] A mind map is a visual diagram used to examine and present complex information in a rational model. The map starts with a central node or core concept. Lesser nodes represent the major categories of the central concept. The map shows the subcategories of the lesser categories. For centuries, mind maps have be used to assist brainstorming, problem solving, and visual thinking by educators, engineers, philosophers, and psychologists. Mind maps are used to generate ideas, make decisions, and solve problems. Mind maps helps to direct the study and organization of information.

Figure 9.0 Sociolegal Analysis



9.2.2 Comparative Law - Business Practices

As a part of the comparative law analysis of the countries in the current study, a number of related international studies were reviewed and the data re-analyzed following a meta-analysis model. Relevant data was extracted from the World Economic Forum global information technology report and the privacy international study of major corporations. This analysis places the DPSIP issues in a relevant objective perspective.[20]

The World Economic Forum[21] publishes a global information technology report. The report studies data from 138 countries that account for ninety-eight percent of the world's gross domestic product. Countries are ranked from the best (lower scores) to worst (higher scores). A number of DPSIP related issues are addressed in the report. The rankings on usage data and regulatory data factors for the five countries in this study are reported in the following table. The country related to this study with the highest score in each category is noted in bold.

[20] See Chapters 4 – 8 of the current study.
[21] Soumitra Dutta & Irene Mia, *The Global Information Technology Report 2010–2011: Transformations 2.0* (World Economic Forum. 2011).

Table 9.0 Comparative Technology and Regulatory Data

Issue	AU	CA	SA	UK	US
Usage Data					
Networked readiness[22]	17	8	61	15	**5**
Internet users[23]	20	11	107	**7**	15
Use of virtual social networks[24]	9	6	88	**3**	12
Extent of business Internet use[25]	20	8	52	**6**	7
Usage data weighted average	16.5	8.25	77	**7.75**	9.75
Regulatory Data					
Freedom of the press[26]	16	**9**	20	18	38
Effectiveness of law-making bodies[27]	**4**	11	29	12	45
Laws relating to information and communication technologies[28]	**9**	10	32	15	16
Judicial independence[29]	9	11	43	**8**	34
Efficiency of legal framework in settling disputes[30]	12	14	19	**8**	33
Efficiency of legal framework in challenging regulations[31]	**13**	18	20	16	35
Protection of asset and property	14	**10**	29	17	40

[22] *Id.* at xix.
[23] *Id.* at 372.
[24] *Id.* at 374.
[25] *Id.* at 380.
[26] *Id.* at 317.
[27] *Id.* at 320.
[28] *Id.* at 312.
[29] *Id.* at 322.
[30] *Id.* at 323.
[31] *Id.* at 324.

rights[32]					
Intellectual property protection[33]	14	**13**	27	17	24
Regulatory data weighted average	**11.38**	12	27.38	13.88	33.13

The usage data scale[34] reports the international rankings on networked readiness, number of Internet users, virtual social network users, and business Internet usage. Of the countries in the current study the UK earned the highest ranking followed by CA, the US, and AU. SA ranked a little lower than the international mean. However, the score is an indication of a number of opportunity factors not necessarily related to usage data. SA is above the international mean for business Internet usage and networked readiness.

The regulatory data scale[35] addresses several important issues that can impact current and future DPSIP regulatory issues. Freedom of the press is a measure of press control by government and corporate sources. The measure is often not supportive of DPSIP regulatory efforts. Effectiveness of law-making bodies indicates how successful law makers may be at legislating DPSIP standards. A further measure is the level of laws relating to information and communication technologies. Judicial independence is a measure of how effective the courts may be in developing and enforcing DPSIP standards. Ineffective or non-existent DPSIP regulations require an effective legal framework to challenge erroneous regulations or gaps in regulations. DPSIP legislation requires the legal framework to be effective in settling disputes. The level of intellectual property protection has a potential for strong DPSIP legal standards; however, it can also show a strong anti-DPSIP preference for businesses over the interests of people. A similar dynamic can be found in measures of protection of asset and property rights. AU, CA, and the UK have the highest scales of the countries studied. The

[32] *Id.* at 325.
[33] *Id.* at 326.
[34] The scale was developed using the raw data reported in the World Economic Forum's original study.
[35] *Ibid.*

difference between AU and CA is statistically small. Prior chapters have shown that CA has much stronger DPSIP legislative and regulatory programs. The SA data suggest possible reasons why the country has been slow to develop strong DPSIP legislation. The US data provides insight into the ineffectiveness of the historic sectoral approach, self-regulation, and a refusal to adopt modern DPSIP legal standards.

The data from the current study provides some insights into the DPSIP laws and approaches of the subject countries. Not all factors are a zero-sum game; instead, SA can view the issues on a continuum of polar opposites. Are DPSIP legal issues one of corporate liberty that includes the view of "buyer beware," or is it aimed at the protection of dignity and of the individual and of community interests? Is the justification one of economic rights of the corporate republic, or the political rights and interests of the people and society? Should the approach be sectoral or comprehensive? Should the oversight of DPSIP laws and practices be ruled by market and political forces or a truly independent government office? Should the DPSIP legal standards be fragmented or comprehensive? When a balance is required, should the law favor the capitalistic interests of businesses, corporations, and the super rich, or should it favor maintaining cultural and legal standards of the rule of law, human rights, and the social contract? Given the reality of judicial biases, such standards must be included in the legislative mandate.

An independent international study that included the countries in the current study addressed DPSIP and surveillance issues.[36] The findings are consistent with the data in the current study. The US and UK ranked as endemic surveillance societies—the lowest rating. AU and SA ranked as having a systemic failure to uphold safeguards. CA ranked as having some safeguards but weakened protections; however, it did not make the list of countries with the worst DPSIP records. AU made the worst records list for not having DPSIP constitutional protections. SA ranked in the list of countries with the

[36] Privacy International, *Leading Surveillance Societies in the EU and the World 2007*. (2007, December 28), at http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559597 (last visited on 2 January 2008).

worst record because of its communication data and retention policies, poor privacy enforcement; and lack of statutory protections. The UK made the worst DPSIP list because of its border and transborder issues, communication data retention policies, communications interception practices, lack of constitutional DPSIP protections, data-sharing practices, use of identity cards and biometrics, as well as surveillance of medical, financial, and movement practices, and visual surveillance. The US made the list for border and transborder issues; communications interception practices; use of identity cards and biometrics; lack of privacy enforcement; lack of privacy leadership; lack of statutory protections; surveillance of medical, financial and movement practices; visual surveillance; and workplace monitoring.

Privacy International[37] examined twenty-three "consumer-facing" companies. The population included firms noted on lists of different top fifty to top 500 firms. The selection measures included market share, number of users, services offered, and site traffic. Rankings were based on corporate administrative details, corporate leadership on DPSIP issues, customer and user controls, data collection and processing standards, and data retention policies. The companies were also evaluated on their ethical compass, fair gateways and authentication processes, openness and transparency, use of privacy-enhancing innovations and privacy invasive innovations, and responsiveness.

The corporations that were "generally privacy-aware but in need of improvement"[38] included the BBC, eBay, Last.fm, LiveJournal, and Wikipedia. The companies that were "generally aware of privacy rights, but demonstrate some notable lapses"[39] included Amazon, Bebo, Friendster, LinkedIn, Myspace, and Skype. The organizations that showed "serious lapses in

[37] Privacy International, *A Race to the Bottom - Privacy Ranking of Internet Service Companies*. (2007), at https://www.privacyinternational.org/article/race-bottom-privacy-ranking-internet-service-companies (last visited on 2 June 2012). Privacy International is a global organization whose mission is "to defend the right to privacy across the world, and to fight surveillance and other intrusions into private life by governments and corporations."

[38] *Id*. at 1.

[39] *Id*. at 1.

privacy practices"[40] included Microsoft, Orkut, Xanga, and YouTube. The corporations that showed "substantial and serious privacy threats"[41] included AOL, Apple, Facebook, Hi5, Reunion.com, Windows Live Space, and Yahoo! Google was the one organization that was rated as having a "comprehensive consumer surveillance and entrenched hostility to privacy."[42] The data reveals that DPSIP legal issues relate to governments and businesses.

9.2.3 Comparative DPSIP Positive Law Analysis

Relevant sources of DPSIP laws were examined. Related areas of the law were addressed. An analysis of each of the DPSIP standards established by the countries in the study standards was assessed.

9.2.3.1 Legal Support of DPSIP Protections

All of the countries in the study are signatories of various International Human Rights agreements. Only CA and the UK are approved under the EU DPSIP standards. AU has attempted to meet the EU standards; however it has not been granted approved status. The US has negotiated a Safe Harbor agreement with the EU. SA is still attempting to establish compliance standards. AU and the US have been involved in the establishment of APEC DPSIP standards, which offer fewer data protections than the EU standards.[43]

Of the countries studied, only SA has a clear Constitutional privacy protection clause. The US Supreme Court has found a penumbra in the Bill of Rights for privacy protections. While SA is currently working on a national DPSIP law, the other countries in the study already have DPSIP laws. The US approach tends to be contradictory based on the industry sector. Limited or mixed DPSIP related common law is found in the countries studied.[44]

---

[40] *Id*. at 1.
[41] *Id*. at 1.
[42] *Id*. at 1.
[43] See tables 4.1, 5.3, 6.2, 7.2, and 8.9 of the current work.
[44] *Ibid.*

With the exception of some states in the US, the countries studied do not have provincial or state DPSIP constitutional declarations. Provincial or state DPSIP legislative efforts have been found in AU, CA, the UK, and the US. DPSIP related common law has also been established in these countries on the provincial or state level.[45]

9.2.3.2 Support of Corporate Privacy and Data Property Protection Issues

All of the countries studied provide for protections of copyright, data base, patent, trade mark, service mark, and for trade secret protections on the basis of a property right.[46]

None of the countries in the study require a privacy impact audit prior to any use. Only AU requires a limited privacy impact audit before government protections are granted. CA and the UK have provided for checks and balances on corporate collection, use, and transfer of individual DPSIP data. AU has limited checks and balance protection on such practices.[47]

9.2.3.3 DPSIP Declarations

Of the four countries that have passed DPSIP legislation, all have provided key definitions for personal and sensitive information. Unfortunately, the definitions are all technologically outdated. None of the current definitions effectively address advanced data mining technologies or make all data holders and users accountable to DPSIP standards.[48]

---

[45] *Ibid.*
[46] *Ibid.*
[47] *Ibid.*
[48] *Ibid.*

9.2.3.4 Regulatory Agency Powers

Of the countries studied, only the US has some independent regulatory agencies that do not directly report to the executive or legislative branches. All of the regulatory agencies in the study have administrative powers, investigative powers, and an educational function. All of the agencies have defined responsibilities, accountability standards, and require the appointment of a governmental chief privacy officer or commissioner. None of the countries require businesses to do privacy audits.[49]

The AU DPSIP agency does not have strong enforcement or regulatory powers. CA and the US do not mandate that governmental privacy audits be required as part of legislation passage. AU does not require a business chief privacy officer or commissioner. CA does not hold employees personally liable for DPSIP violations.[50]

9.2.3.5 Sectoral DPSIP Legislation

All of the countries in the study provide some DPSIP protections for industry sectors. All restrict credit reporting agencies. AU has the strongest credit reporting agency restrictions and provides a model for all. All of the countries protect individual health information, with some exceptions. All of the countries are attempting to confront the DPSIP risks related to electronic health or medical records. CA and the UK do not provide for criminal justice record restrictions. The US has limited restrictions on criminal justice records. AU has the strongest restrictions on criminal justice records and provides a model for all.[51]

---

[49] *Ibid.*
[50] *Ibid.*
[51] *Ibid.*

9.2.3.6 DPSIP Data Controller Standards

All of the countries in the study establish some standards for data controllers. With the exception of the latest SA Bill, all of the countries in the study require a notification requirement and allow Opt-Out provisions. Only the UK does not provide for any Opt-In provisions. All of the countries in the study require that collected data be accurate, complete, and limited to needed data; be lawful and fair, not misleading; and be relevant, and up to date. Each provides standards for data quality and integrity, data retention limitations, openness on the information held, and system access controls. Only some states in the US require breach notification standards and breach penalties.[52]

9.2.3.7 DPSIP Data Processor Requirements

All of the countries that have passed DPSIP legislation require some form of informed consent for data processing. A rationale for the processing should be provided, and the processing must be fair and legal. The processing must also be accurate, timely, and protect sensitive information. The standards for the duration of record keeping are limited. AU, CA, and UK standards allow for limited data ownership by the subject. SA and the US do not accept the ownership of data by the subject. AU and CA do not provide data subjects the right to have control over access. All of the countries studied allow data subjects to have the limited power to alter, amend, correct, or delete data errors. Each provides for a limited notification requirement for data subjects.[53]

9.2.3.8 DPSIP Data Security Standards

Generally, the countries in the study require that data security standards and technology be state-of-the-art. Tracking of the security processes is not required once data has been merged. The US has no such standard at all for merged data. Adequate safeguards are mandated by the other countries.

---

[52] *Ibid.*
[53] *Ibid.*

The standard is only adequate encryption. The security process must protect from unauthorized alteration, disclosure, misuse, and internal and external unauthorized access. AU provides for civil and criminal penalties for unauthorized access. CA, the UK, and the US provide for access penalties based on the cause of action. AU and CA do not allow a technology cost of implementation defense. None of the countries in the study provide for strong remedies for data security inadequacies.[54]

The data shows a wide variance in the DPSIP responses between the countries in the study. Such a situation sends mixed messages and inconsistent standards to businesses, governments, and the people.

9.3 DPSIP Legal Justification

Robert Gellman and Pam Dixon recently summarized the legal justification for DPSIP concerns. In addressing issues of information privacy, Gellman and Dixon wrote that "privacy is a right, a human right, a legal right, a moral right, a property right, a positive right, a negative right, a value, and an economic interest, a personal interest, a societal interest, and other things."[55] DPSIP standards focus on legal principles and the security of individuals, business, and government data. The issues include asset protection, contract law, information control, intellectual property law, property law, tort law, and privacy law conflicts.

The DPSIP protection model suggests that data protection and information privacy is an individual right; more importantly, it is a societal protection from misuse of power. The model empowers the individual to access and control information privacy data and increases the need for state-of-the-art data protection security for those who hold the data.[56]

---

[54] *Ibid.*
[55] Robert Gellman & Pam Dixon, *Online Privacy: A Reference Handbook*, (ABC-CLIO, LLC ed. 2011), at 1.
[56] See § 2.7.1 of this work.

Informed consent, confidentiality, due process, and privacy legal principles must apply to all data protection and information privacy recordkeeping systems. These principles must be considered whenever an information privacy contract is formed. Collection and use of personal information requires a contract clearly affirmed through standard contacting principles. A valid offer, acceptance, consideration, intent to be bound, specific terms, and performance should be required.[57]

DPSIP law is justified under the principles of information and knowledge control law.[58] Pricilla Regan defined privacy as a collective value, not just an individual value, based on the economic view of collective and public goods. One can not benefit from a collective good without others benefiting.[59] Free riders, government or business, should not use information without legally obtaining consent and paying for it.[60] Alan Westin advocated the need for individuals to have control over their personal information. He argued that free societies recognize a personal information privacy right. Only extraordinary exceptions should trump this right.[61]

Whether by intent, design, or regulatory ignorance, intellectual property law has become a major force negating some DPSIP legal issues.[62] Granting anti-privacy intellectual property protections gives owners considerable legal power and protection. The intellectual property codes do not require any type of environmental or information technology impact study prior to granting a patent or copyright. Because of this failure, legal protections as applied to technology or software that violate privacy rights must be re-considered to stay current with regulatory standards in other fields. Two major problems have arisen: first, software patents started, despite a long history against awarding protections to mathematical formulations and business practices.

---

[57] See § 2.7.2 of this work.
[58] See § 2.7.3 of this study.
[59] Pricilla M. Regan, *Legislating Privacy: Technology, Social Values, and Public Policy* (University of North Carolina Press 1995), at 227.
[60] *Id.* at 228.
[61] Alan Westin, *Privacy and Freedom*, at 42 (Atheneum 1967).
[62] See Chapter 5.

Second, cookies received legal protection without being subject to a sound legal review.[63]

The economic value of information in the current era cannot be denied. Large corporations and even some courts claim that information is a financial property asset; however, little attention is given to the original owners and creators. Personal information can be bought and sold, has high value, and is measurable. Moreover, license rights can be assigned and transferred. Individuals whose private information is collected in data bases have property rights to that information or data. The information, similar to a copyright, is owned by the author, the data subject.[64] Adam Moore[65] further argues that information privacy is an intangible property right. Personal information is owned by the subject of the information; the person must be able to restrict the use as privacy property right. Frank H. Esterbrook[66] argues that intangible intellectual property is "no less the fruit of one's labor than is physical property".[67]

Vine Deloria Jr. and David Wilins[68] advance the position that property relates to individuality, personal freedom, and sovereignty contrasted to material objects. The existence of intellectual property protections supports this view. Personal information and traditional views of property are like matter and energy: each is inseparable – neither is dominating. The law must recognize each issue as equal. The legal principles afforded to one must be applied to the other. The Deloria and Wilins position is built upon the classic work of

---

[63] See § 2.7.4 of this study.

[64] Brian Gongol, *Privacy as a Property Right* (2006), at http://www.gongol.com/research/economics/privacypropertyright/ (last visited on 2012, November 1).

[65] Adam D. Moore, *Intangible Property: Privacy, Power, and Information Control, in Information Ethics: Privacy, Property, and Power* (Adam D. Moore ed., University of Washington Press 2005).

[66] Frank H. Esterbrook, Intellectual Property is Still Property, in *Information Ethics: Privacy, Property, and Power* (Adam D. Moore ed., University of Washington Press 2005) at 117. See also § 2.75 of this study.

[67] See § 2.7.5 of this study.

[68] Vine Deloria Jr. & David E. Wilkins, *The Legal Universe: Observations on the Foundation of American Law* (Fulcrum Publishing ed. 2011).

Charles A. Reich.[69] Reich argued that property was not a tangible product; however, it was a relationship that produced income and value. Governments establish occupational and professional licenses based on individual behavior which is considered a property right. Data subject information is a form of wealth and property owned by the subject.[70] The function of such property is to protect the dignity, independence, and pluralism over which the majority or other forces have to yield to the individual. In this sense, property is not tangible but a set of behaviors and relationships that produce value created by the data subject, thus forming a circle of legal protection. Businesses, governments, and organizations must compensate, explain, and justify any interference with or taking of such property.

Edward Bloustein argued that "privacy began its modern history as a tort."[71] Privacy tort law began with the publication of an article by Warren and Brandeis. In the work, the authors advocated protections against unwanted publication of personal information while protecting the "products and processes of the mind"[72] and protecting one's "inviolate personality."[73] The authors argued that "political, social and economic changes entail recognition of new rights, and the common law ... grows to meet the demands of society."[74] Warren and Brandeis argued that privacy rights required "protection, without the interposition of the legislature"[75]

In January 2012, the Ontario Court of Appeals of CA[76] first recognized an intrusion upon seclusion tort.[77] The Court found that DPSIP issues are essential to the individual's well being, and are a fundamental democratic value worthy of protection under the law.

---

[69] Charles A. Reich, The New Property, 73 The *Yale Law Journal* 5, 733 (1964).
[70] Even if only as the owner of raw materials.
[71] Edward J. Bloustein, Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser, 39 *New York University Law Review* 962 (1964), at 963.
[72] Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, 4 *Harvard Law Review* 5, 193 (1890), at 194.
[73] *Id.* at 192.
[74] *Id.* at 193.
[75] *Id.* at 195. See § 2.7.6 of this study.
[76] The highest Court in the Providence
[77] *Jones v. Tsige*, 2012 ONCA 32, (18 January 2012). (CA)

9.4 Comparative Legal and Policy Research Findings

A linguistic textual analysis was conducted on the DPSIP international documents presented in this study.[78] This qualitative research method determines common related concepts, as well as identifies key legal issues and regulatory responses.[79] The analysis shows that there are generally accepted legal and regulatory recommendations and standards. The consensus is that the law must provide for an independent regulatory body with considerable power, and that it must require a DPSIP authority at the government and business organization level. This analysis forms the basis of DPSIP 3.0 recommendations.

DPSIP law and regulations must provide for inspection activities to evaluate information business activities including an analysis of competition practices. Inspection activities extend to all processes related to individual data and information and to the quality of that data and information. Inspection of individual or group objections to the practices of an organization holding such data is required.

The regulatory body must have the authority to insure legal compliance, establish regulatory guidelines, and adjudicate disputes. This authority includes the right to inspect organizational DPSIP-related practices. The authority of the regulatory body must extend to business and government organizations' data and information practices. The regulatory body must also have the authority to insure compliance with DPSIP principles, processing standards, and security protections. In addition, the regulatory body must have the authority to monitor competitive standards across economic sectors, insure acceptable confirmation standards (including state-of-the-art technology), and mediate objections.

---

[78] See Chapter 3 International Legal Standards & Guidelines.
[79] See Chapter § 1.12 Data Processing and Analysis.

The regulatory body must insure organizational compliance with DPSIP laws and regulations including collection and use of data, individual rights, and DPSIP principles. A legal compliance balance is needed to limit deviate behaviors and acceptable legal standards. Specific areas of concern include collection practices, insuring an informed consent, and data processing practices. Organizations have an obligation to protect personal civil rights around DPSIP issues and to implement consumer protection standards on the range of use of data issues.

The regulatory body must also perform an educational function. The public and organizations must be educated on current data practice standards and changes in DPSIP legal principles.

The regulatory body must also have the power to monitor and set standards for data collection practices. The standards include any policy changes, individual access to records, and consumer protections and human rights.

The regulatory body must issue confirmation reports related to business and government compliance, inspections, and information practices. The confirmation reports include practices related to data protection and security compliance, adherence to data protection principles, as well as individual civil and human rights.

The regulatory body must insure that an informed consent is provided by data subjects for the collection and use of personal information. The data subjects must be asked and provide informed consent for every collection, processing, and data transfer function.

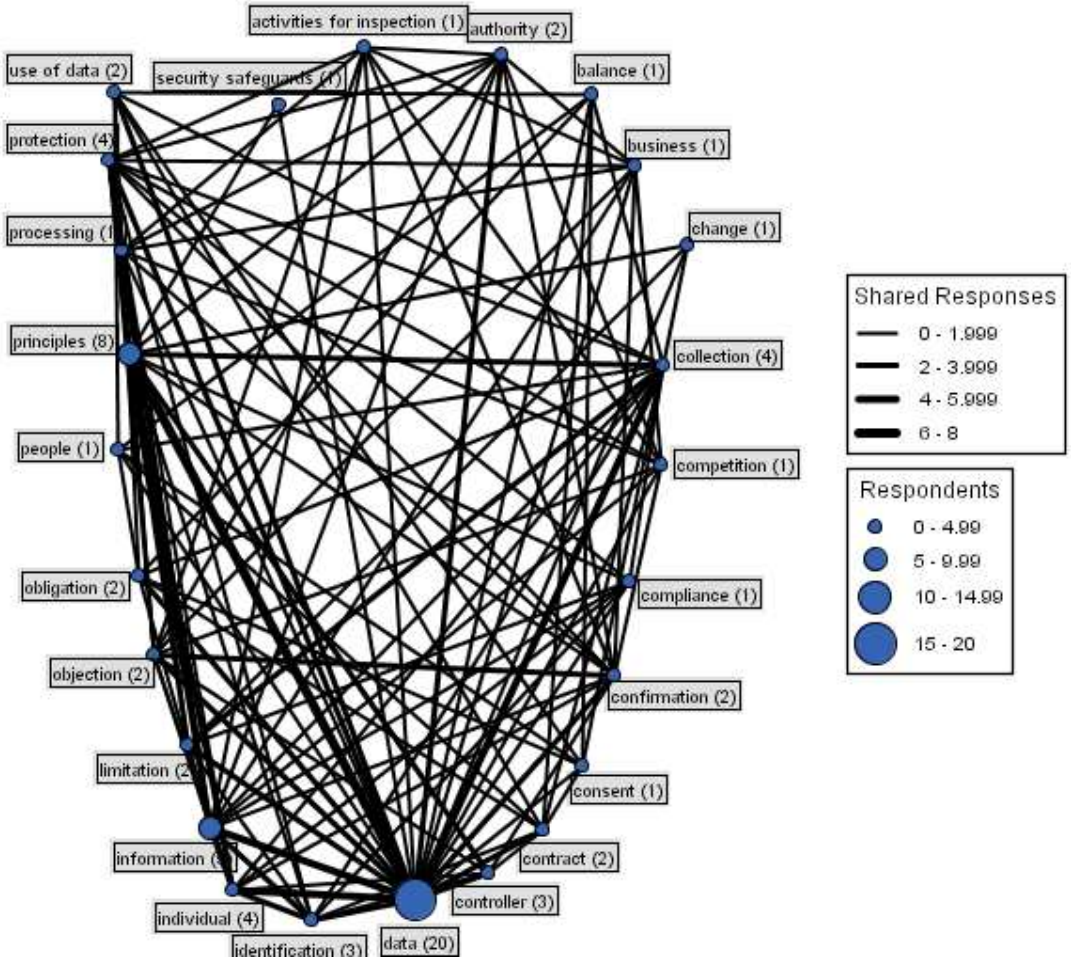
The regulatory body must insure that contract law principles are enforced in all DPSIP functions; specifically, there must be a means to balance the contracting power differences, collection and processing consents. Data processing and systems that do not identify personal-related data directly or indirectly must have a competent informed consent.

The body must insure that data controllers abide by individual identification principles as well as by DPSIP legal and regulatory principles including confirmation of compliance with contract law provisions as they apply to data collection and processing. The regulatory body must insure that those functions that are generally exempted from standard DPSIP regulations still comply with checks and balances. Such organizations must still follow the spirit of DPSIP and rule of law principles.

Finally, the regulatory body must have the power and obligation to monitor the processing and use of all personal data processes and insure that legal protections are provided. State-of-the-art data security principles and practices must be applied in all DPSIP situations. The following graph[80] shows the textual analysis of the interconnections discussed above.

[80] Textual analysis results are presented numerically and in a graphic presentation. The graphic presentation includes a data legend. The shared responses are presented by connection lines of various widths and darkness. The wider and darker lines represent a higher number of shared responses. The number of data points as noted by the respondents is represented by circles at the connection nodes. The size of the circle represents the range of respondents. Larger circles represent key concepts and issues.

Figure 9.1 International DPSIP Textual Analysis



Graph 9.1 shows the interconnections noted in the proceeding paragraphs. The graph reveals the need for a comprehensive DPSIP approach. DPSIP issues are a systemic problem that requires a system level resolution.

9.5 Comparative Textual Research Findings

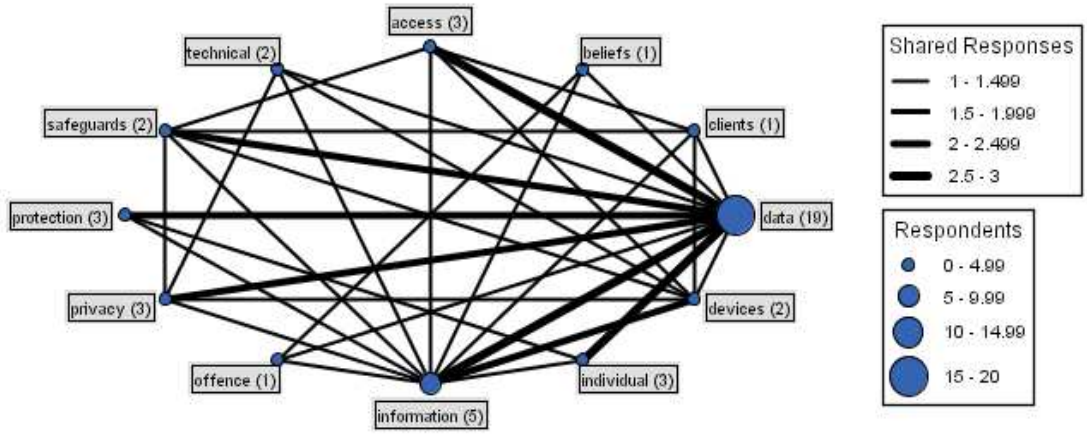
This data reveals that current DPSIP legal and regulatory update efforts and the SA approach can benefit from a linguistic analysis. Prior to the advancements in technology and the development of advanced data mining technology practices, the concept of regulating personally identifiable information (PII) was sufficient. Discrete PII identification currently provides

little protection. The interrelated categories of terms must be considered in modern DPSIP legislation and regulatory efforts.

9.5.1 Definition: Data Protection

The following graph reveals the inter-relationship of key terms related to data protection legislation based on standard qualitative textual analysis methods. The database included information drawn from AU, CA, EU, SA, UK, and the US. Each term refers to personally identifiable information and data security. The analysis shows some common use of terms. The findings are noted in the following figure:

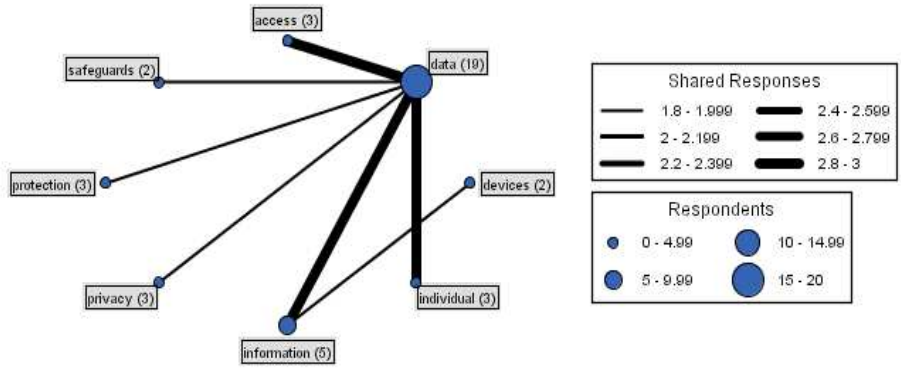
Figure 9.2 Data Protection Terms



An effective DPSIP approach must address the interconnections of privacy, data protection, and data security. The connections must address technical and policy protections. Users need to be aware of the risks and safeguards.

The relationship of key terms related to DPSIP legislation in AU, CA, the EU, SA, UK, and the US were analyzed using standard qualitative textual analysis methods. The finding is noted in the following figure:

Figure 9.3 Term Relationships



The common themes of the selected data protection legislation reveal that such legislation involves the regulation of technical devices and access to information about individuals. These legislative acts provide limited safeguards to protect privacy concerns.

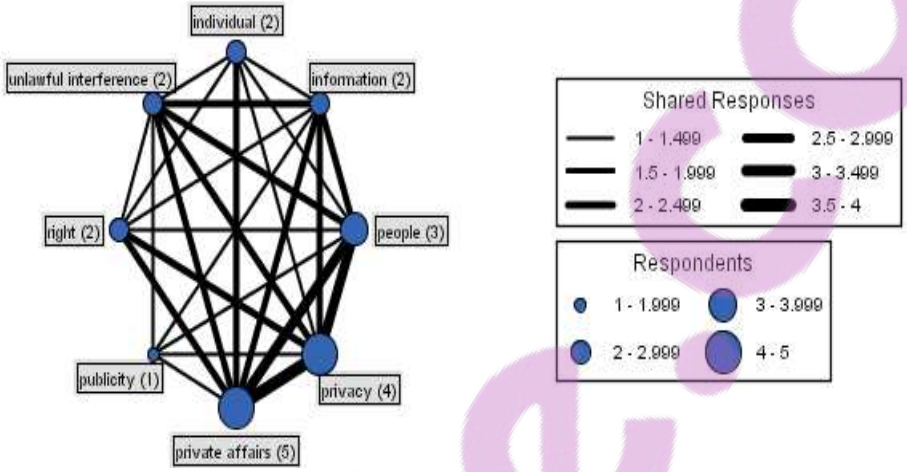
Access includes either accessing or obtaining access to data. *Belief* embraces personal and religious beliefs. *Clients* consist of actual clients and client files. *Data* incorporates access to data from data bases, electronic data files, personal data, security of data, sensitive personal data, test data, and use of data. *Individual* refers to living individual human beings. *Information* comprises accountability for information, confidential information, heterogeneous information systems, information, and sensitive stored information.

9.5.2 Textual Definitions: Information Privacy

Data protection is the term most often used in the EU and its member nations for personally identifiable information. *Information privacy* is the term most often used in CA and the US. Although the two terms are similar, it is important to further define information privacy and examine legislative exceptions.

The following graph shows the information privacy law definitions of privacy based on standard qualitative textual analysis methods. The data is based on legislative acts and the legal literature.

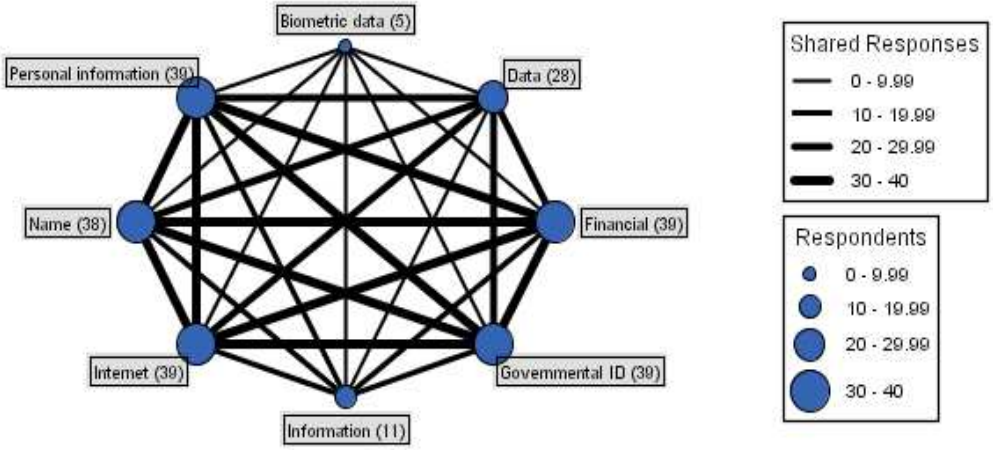
Figure 9.4 Privacy Definitions



The *individual* category includes identifiable human individuals or persons. The *information* category comprises personal correspondence, papers, and personally identifiable data. The term *people* encompasses family, home, houses, leading one's own life, likeness, and reputation. *Privacy* consists of invasions, false light, and property rights. *Private affairs* include communications, life, organizations, and related personal affairs. *Publicity* incorporates release of embarrassing information that can detract from one's reputation and false light publicity. *Right* includes the right to have one's data and private information free from unwanted uses, protected, and secure. *Unlawful interference* covers appropriation, arbitrary, interference, misuse, not duly authorized, not reasonable, seizures, unlawful, and wrong.

The following graph reveals a range of operational definitions based on standard qualitative textual analysis methods. The data is based on progressive legislative acts.

Figure 9.5 Operational Definitions



This analysis of data protection and information privacy legislation reveals considerable overlap in the listing of sensitive data. While some are more complete than others, there are essentially eight data classifications: biometric data, data, financial, government ID, information, Internet, name, and personal information.

Biometric data includes unique fingerprint, iris image, retina image, voiceprint, or other unique physical representation. *Data* comprises unencrypted data elements. *Financial data* consists of access codes, access to personal financial data, account numbers, balances, credit card numbers, credit cards, debit cards, debit card numbers, financial account data, financial resources, and tax information. *Government ID* encompasses driver's license numbers, government ID cards and numbers, motor vehicle license numbers and data, non-driver ID card data, social security numbers, and data.

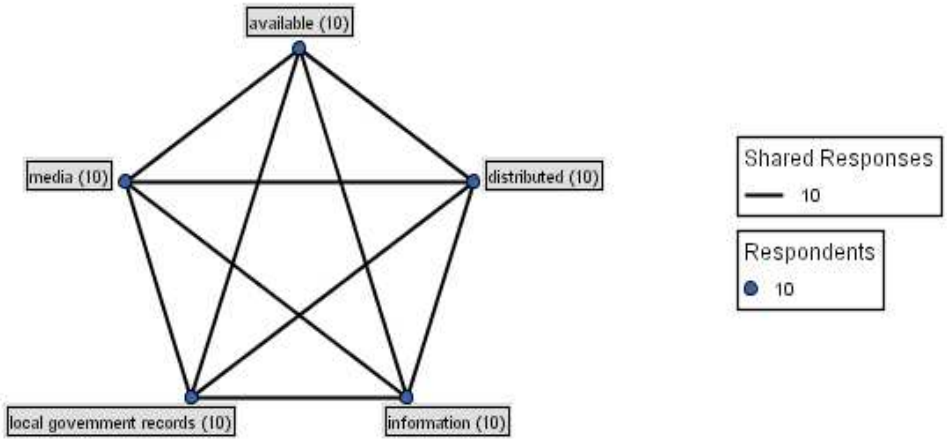
Information data contains membership information, personal ID information, phone number, photo ID card data, and residence data. *Internet* includes electronic access codes, codes, identification numbers, Internet accounts, passwords, and security codes. *Name* covers an individual's first initial, first name, last name, middle initial, middle name, surname, and user name. The name is usually tied to one or more other categories of data and information privacy. *Personal information* includes date of birth, electronic signature, employer, and mother's maiden name. Personal information also

incorporates sensitive personal data. Such data consists of association or union membership, criminal charges or record, ethnic origin, mental condition or health, physical condition or health, political opinions, racial identification, religious beliefs, and sexual life.

With the exception of the listings in the categories for *biometric data* and *information data,* the majority of all of the data categories are noted in the legislative acts. Biometric data is related to the date of the Act and use of such technologies. The information category is also related to older Acts and court decisions on directory data ownership.

An essential part of any information privacy law definition includes those factors excluded from legal regulation. The findings regarding the categories of such exclusions are based on standard qualitative textual analysis methods and shown in the following graph.

Figure 9.6 Exclusions



Available comprises information that is publicly available including distributed directories. *Distributed* focuses on available information distributed through the full range of media resources. *Information* incorporates available published data. *Local government records* include available local or state information, directories, or media releases. *Media* covers the full range of information media resources. Media comprises bona fide advertising

statements, association publications, charitable publications, fraternal nonprofit corporations, broadcasts over radio or television, directories, journals, magazines, news, news bureaus, newspapers, reporters, or any other type of media activity entity or item. The list includes Internet posts, blogs, and social media. The exclusions found in this analysis are problematic. For example, if the government or a business wants to bypass the letter and spirit of DPSIP principles, all it has to do is leak a story to the press to make the data legally available for use for whatever purpose.

Of the legislation examined, only two pieces of legislation did not require data protection and information privacy exemptions to be lawful. These two jurisdictions allow for stolen information that is publicly released to be in the public domain. That standard is a source of cognitive dissonance. The majority of legislation requires that the collection, use, and distribution of the data must be lawful. Data in federal, state, or local government files are exempt; however, whether to release the data is a government decision. If the government releases the information to the public, then privacy constraints are ineffective.

If one seeks information under freedom of information acts, then the data is again controlled by the government. One of the most troublesome features of the exemption lists typically in place is a clause that allows widely distributed media release of information privacy data that is otherwise protected. Under these provisions, it was lawful for the George W. Bush administration to release private and secret information identifying Valerie Plame Wilson[81] as a U.S. Central Intelligence Agency operative. The Bush administration secretly released the data to widely distributed media. The release of the data was declared lawful because the data was released by the government; however, the release was illegal under other national security laws.

---

[81] Valerie Plame Wilson, *Fair Game: My Life as a Spy, My Betrayal by the White House*, (Simon & Schuster ed. 2007).

9.6 Summary

This chapter provided a summary of the research findings to the questions proposed in Chapter One. This chapter showed that, from an academic perspective, bifurcation of information privacy, data protection, and data security is in some people's self interest; however, from a legal perspective, bifurcation of information privacy, data protection, and data security was not justified. The comparative positive law analysis of the subject countries involved independent socio-legal data. A meta-analysis of the subject countries' analysis of legal and policy approaches was examined. The legal justifications for DPSIP laws and regulations ware explored. The chapter presented a textual analysis of international and specific national DPSIP statutes to aide in the understanding of current issues and future developments of DPSIP law in SA and the international community.

Chapter ten will propose new Gold Standards of DPSIP protections. The proposals are based on the comparative analysis of the current study and reflect recent legal changes in DPSIP standards in the countries studied and the EU reconsiderations of legal approaches. The proposals provide a means for SA to take a lead in DPSIP protections.

CHAPTER TEN: DATA PROTECTION AND SECURITY LAW: GOLD STANDARD PROPOSAL

> *There are three major reasons for the movement towards comprehensive privacy and data protection laws. Many countries are adopting these laws comprehensive privacy and data protection laws for one or more of three major reasons. : To remedy past injustices. … To promote electronic commerce. … To ensure laws are consistent with Pan-European laws.*[1]

10.0 Overview of the Chapter

This chapter concludes the author's research.[2] The findings and recommendations presented in this chapter are solely the author's own; they do not represent the legal or policy views of the faculty, research supervisor, or the School of Law of the University of South Africa. The focus of the work is to stimulate discussion and perhaps debate on what the author considers to be key issues related to the development of DPSIP law internationally and specifically in SA. The author maintains that SA faces a strategic choice: follow historic Pan-European approaches or take the lead in national and international DPSIP standards. Respectfully, SA can certainly make its own decision. However, this chapter discusses the factors that legislators in SA should consider when making their decision and proposes a DPSIP 3.0 gold standard based on a comparative study of major international parties.

The chapter addresses the need for DPSIP legislation and regulation. The approach to effective regulation must address the connection with data

---

[1] Global Internet Liberty Campaign, *Privacy and Human Rights: An International Survey of Privacy Laws and Practice*. (2008), at http://www.gilc.org/privacy/survey/intro.html (last visited on 16 July 2012).

[2] The views and recommendations in this chapter are based on the author's interdisciplinary research, education, training, and experience. The proposals do not necessarily reflect the views of the law faculty at UNISA or the university. The proposals do not necessarily reflect the views of any affiliation the author may have with organizations or employers of the author. The purpose of this chapter is to stimulate academic and professional dialogue and legal – policy development.

security, protection, and privacy. Key DPSIP issues that must be addressed are presented alphabetically to make the data easier to access. The issue recommendations are based on the research conducted internationally and from the countries included in the study. The chapter addresses the issue of providing exemptions to DPSIP law and regulations. Alternative legal considerations, limitations of the current study, and future research recommendations are addressed. The chapter concludes with the need for DPSIP vigilance.

10.1 Comparative Gold Standard of DPSIP Principles—DPSIP 3.0

From an international perspective, as noted in Chapter One, DPSIP laws and policies have gone through four evolutional stages at this time:

- DPSIP 0 in which few DPSIP legal protections exist.
- DPSIP 1.0 which established some legal standards focused on limited legal consent and notice.
- DPISP 2.0 which accepts personal information standards but does not fully address security issues centered around a harm based legal analysis, and
- DPSIP 3.0 in which sensitive and non-sensitive personal data is fused; information privacy, data protection, and security issues are interrelated; legal audits and checks and balances are needed for all personal information stakeholders; new technologies are required to pass privacy audits (e.g. RFID) and to employ the use of privacy enhancing technologies in all new IP approvals.

The countries in the present study fall at various points along the continuum between DPSIP 2.0 and DPISP 3.0. Justice Kirby of AU argues for enhanced privacy rights, including a right not to be indexed. The positive principles include the following rights: access to data, effective encryption of personal communications, fair treatment, human checking of adverse decisions, protection of personal information privacy, and understanding automated

decisions.[3] The CA standard is that information privacy is essential to the democracy and the individual person. All personal information is owned by the person who has the legal right to control the exchange of the information.[4] The DPSIP law enacted in the CA province of Alberta clearly defines personal information, breach notification, and transfer of information outside of CA notification.[5] DPSIP 3.0 legal and regulatory standards build on international data protection and security standards[6] rather than replacing them.

DPSIP 3.0 legal and regulatory standards must address all DPSIP players—government, juristic, business and corporate, organizational, and natural persons. The standards of data security and information privacy and data protection standards must apply to all these persons. Establishing and maintaining DPSIP legal checks and balances is essential. Legal and regulatory DPSIP standards must be applicable to all or there is no rule of law. DPSIP 3.0 protections require specific and unified principles. Dedicated and powerful change agents are required for innovative implementation.[7]

10.2 Data Security

Historically, the fields of data security and data protection developed independently. As the technology and applications evolved, it is evident that there is no information privacy or data protection without computer and data security protections. All DPSIP 3.0 legal standards must apply to private and government data collectors, processors, and transfer of data processes. A strict liability standard must be applied to the range of data security issues.

---

[3] The Hon Justice Michael D. Kirby, Privacy in Cyberspace, 21 *University of New South Wales Law Journal* 2, 323 (1998), at 323.

[4] See *R. v. Dyment*, 2 S.C.R. 417 at 427-428, 55 D.L.R. (4th) 503, 66 C.R. (3d) 348, (1988), 427. (CA) and Information Canada, Privacy and Computers (A Report of a Task Force Established Jointly by Department of Communications/Department of Justice) (Author. 1972), 13.

[5] See § 5.6.1 of this work.

[6] See §§ 3.37, 3.5, 3.7 of this work.

[7] See Viktor Mayer-Schonberger & Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think* (An Eamon Bolan Book/Houghton Mifflin Harcourt ed. 2013); Evgeny Morozov, *The Net Delusion: The Dark Side of Internet Freedom* (PublicAffairs ed. 2011); and Evgeny Morozov, *To Save Everything, Click Here: The Folly of Technological Solutionism* (PublicAffairs ed. 2013).

The issues include controlling tracking tools like cookies by any name, encryption options, filtering, identification authentication, phishing, and spam. Intellectual property law standards must address associated data security issues. On a more technological level, data security issues include protections from malicious and mobile code; mathematical computer security models; physical and web-based vulnerabilities; Trojan Horse attacks; and virus protections. Mandating periodic vulnerability assessments and security awareness programs is critical.[8]

Data processes, as defined above, must meet strict liability requirements to establish standards for detecting, responding, remediating, and managing data security issues. Managers and employees should be held to state-of-the-art application controls. Data organizations must monitor and control systems. Such organizations must conduct security audits, carry out system and data inspections, and maintain high quality data security standards.[9] Data security standards require that **i**ntellectual property protections can not be provided for technologies and practices that do not meet DPSIP design requirements.

Bruce Schneier made a cogent argument that national security and individual privacy are not opposites. The legal issue is not a zero-sum game.[10] Police states provide security, but there are no major immigration trends into those states.[11] Schneier further explained that information privacy and data security must work together.[12] Anti-privacy security tactics alone do not significantly improve security and often do more harm than good. Government security

---

[8] Seymour Bosworth, et al., *Computer Security Handbook* § 1 (John Wiley & Sons 5th ed. 2009a). See also Tim Mather, et al., *Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance*, (O'Reilly Media, Inc. ed. 2009).

[9] Seymour Bosworth, et al., *Computer Security Handbook* § 2 (John Wiley & Sons 5th ed. 2009b).

[10] In game theory, a zero-sum game exists whenever the rules require that when one party wins, the other party must lose

[11] Bruce Schneier, *What Our Top Spy Doesn't Get: Security and Privacy Aren't Opposites* (2008, January 24), http://www.wired.com/politics/security/commentary/securitymatters/2008/01/securitymatters_0124?currentPage=all (last visited on 24 January 2008), at 4.

[12] *Id.* at ¶ 6.

claims that restrict DPSIP issues are often wrong or address fake cases.[13] The security versus privacy issue is a false dichotomy and is based on generating fear. The reality is that "There is no security without privacy. And liberty requires both security and privacy."[14] All data mining efforts must be transparent and must have strong legal and regulatory controls.

DPSIP 3.0 laws and regulations must follow the CA approach of focusing on privacy-enhancing technology, privacy by design, and privacy by re-design.[15] The approach must require privacy audits and controls related to information technology, physical design and networked infrastructure, and must be accountable for all business and government personal information practices. DPSIP 3.0 standards must be designed and operated on the basis of an embedded default standard. The approach must be proactive and preventative. Information life cycles must be established and followed. The design must provide respect for users, be transparent, and be visible.[16]

DPSIP 3.0 standards require that all organizations that collect, hold, process, or transfer data must have an identifiable data controller. This controller must register data-processing activities with the DPSIP authorities.[17] This standard was established in the UK and provides that negligence or deliberate loss of data is a criminal offense subject to a punishment of at least two years in jail. Lord Erroll stated that "Data controllers need to wake up to the importance of personal data, whether in the public or the private sector."[18]

Data controllers must insure that data security procedures are constantly used to meet or exceed legal operational standards. Administrative and technological security procedures must guarantee that adequate prevention

---

[13] *Id.* at ¶ 8.
[14] *Id.* at ¶ 12.
[15] Ann Cavoukian, *What is Privacy by Design?*, Information & Privacy Commissioner Ontario. (2010), at http://www.privacybydesign.ca/ (last visited on 6 July 2010).
[16] Ann Cavoukian & Claudiu Popa, *Privacy by ReDesign: A Practical Framework for Implementation*, (Information & Privacy Commissioner Ontario ed. 2011).
[17] See Part 3 §§17-26.
[18] Tom Young, *Lose Data and You Go To Jail*. (2008, May 8), at http://www.computing.co.uk/computing/news/2216073/lose-jail-3989942 (last visited on 10 May 2008), ¶ 4.

procedures exist and there is no unauthorized or malfeasant access, copying, disclosure, erasure, modification, reading, or removal of personal data.

10.3 Data Protection and Information Privacy

The findings of the current study reveal that comprehensive DPSIP 3.0 legislation is a necessity. Such laws and the regulatory agencies the laws establish must have significant enforcement power.[19] The legal standards must apply to anyone who collects and rents/sells personal information. Such persons must always inform the user, and all uses of data should be processed on an opt-in only consent."[20] The proposed DPSIP standard is not voluntary nor is it a data protection directive. The standard is regulatory and applies to all parties that are involved in the personal information sector. The following issues are a significant part of DPSIP 3.0 standards; however, the list is not exhaustive. New technology will develop that has DPSIP implications, so the standards must be technology neutral. The key application factor must always consider the spirit of the law and technological advancements. For ease of presentation and access, the following DPSIP 3.0 principles are presented in alphabetic order similar to a statutory definition of terms.

10.3.1 Administration

All government departments, agencies, and coordinating bodies must appoint a Chief Privacy Officer (CPO)[21] to oversee the processing of DPSIP data and insure compliance[22] to DPSIP laws and regulations. All such activities may be

---

[19] Terence Craig & Mary E. Ludloff, *Privacy and Big Data*, (O'Reilly Media, Inc ed. 2011) at 89.

[20] *Ibid.* See also Susannah Fox & Oliver Lewis, *Fear of Online Crime: Americans Support FBI Interception of Criminal Suspects' Email and New Laws to Protect Online Privacy*, Pew Internet & American Life Project. (2001), at http://www.pewinternet.org/~/media//Files/Reports/2001/PIP_Fear_of_crime.pdf.pdf (last visited on 24 May 2008). See § 4.11 of this study.

[21] Such a practice has been successful under the US HIPAA law and regulation.

[22] Compliance requires knowledge, concerted efforts, and useful guidelines, and checklists. See examples in Lothar Determan, *Determann's Field Guide to International Data Privacy Law Compliance* (Edward Elgar ed. 2012); Nancy Flynn, *The Social Media*

audited and investigated by the state [province] and federal DPSIP office. Private businesses and organizations that are involved in DPSIP issues shall also be required to appoint a CPO to serve the same function and apply the accountability standards of government agencies internally. The CPO is responsible for full compliance with DPSIP laws and regulations, conducting and verifying privacy impact assessments prior to implementation as well as throughout operations, managing privacy by design standards and subject access standards, dealing with complaints, keeping pace with technological enhancements, supervising all trans-company and transnational data transfers, and maintaining current best DPSIP practices.

The operations of the CPO must be independent. Independence requires that the office must have economic and political freedom, its own infrastructure, separate premises, sufficient financial and staffing support, and use of state-of-the-art technology. The CPO and related staff must constantly fulfill the highest levels of professional integrity, comply with the law, be free of conflicts of interest, and must not be beholden to business or government representatives. CPO functions must be transparent. After government agency CPO officials leave office, they may not establish a DPSIP consulting role or work in related employment in the private sector for a period of five years.

The office shall have the power to investigate and hear complaints. The government CPO shall have the power to order compliance with the law, regulations, and office findings. The office shall have the option of seeking judicial enforcement relief or, when appropriate, means of redress under international arbitration and alternative dispute resolution standards and treaties.[23] The government CPO shall have the power to issue administrative

---

Handbook: Policies and Best Practices to Effectively Manage your Organization's Social Media Presence, Posts, and Potential Risks (Pfeiffer ed. 2012); and John J. Trinckes Jr, *The Definitive Guide to Complying with the HIPAA/HITECH Privacy and Security Rules* (CRC Press ed. 2013).

[23] See United Nations, *Convention on the Recognition and Enforcement of Foreign Arbitral Awards*. (1958), at http://www.uncitral.org/pdf/english/texts/arbitration/NY-conv/XXII_1_e.pdf (last visited on 20 August 2012).

fines and penalties that have the force of law when DPSIP laws and regulations are violated. The office may petition the courts to issue criminal penalties when warranted.

10.3.2 Applicability Scope

DPSIP 3.0 standards apply to government agencies, private organizations, data controllers, data processors, those who maintain mailing lists, and marketing organizations. The DPSIP 3.0 standards apply to all personal data processing: manual, electronic, or any form of technology. The focus includes data mining and data surveillance practices that currently include variations of cookies, RFID, spyware, and surveillance.[24] These behavior-tracking processes must be connected to an identified or identifiable person.[25]

The 3.0 standards apply to all Near Field Communications (NFC), which includes now-ubiquitous mobile devices including RFID, mobile devices, and smart phones. Such technologies provide new benefits and conveniences to users. NFC also provides some privacy and security benefits. However, some risks exist that must be considered.[26] The privacy and security risks include ascertaining the identity of an anonymous user, data being leaked (transferred) without consent, improperly redirecting the device to an unknown website, initiating a (pay-per-use) service without the knowledge of the device user, interception or eavesdropping on wireless communications, lack of

---

[24] See Kenneth K. Dort, *Recent Trends in Cyberspace Law: Data Security and Privacy, in Understanding Developments in Cyberspace Law: Leading Lawyers on Analyzing Recent Trends, Case Law, and Legal Strategies Affecting the Internet Landscape* (Thomas Reuters Aspatore ed., Thomas Reuters / Aspatore 2012).

[25] See *Amann v. Switzerland*, ECHR 27798/95, (2000),¶ 65. (EU) The purpose is "to secure in the territory of each Party for every individual ... respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him" (Article 1), such personal data being defined as "any information relating to an identified or identifiable individual" (Article 2).

[26] See Michael A. Tomasulo & Scott N. Godes, Helping Clients Evaluate Their Cyber Risks, in *Understanding Developments in Cyberspace Law: Leading Lawyers on Analyzing Recent Trends, Case Law, and Legal Strategies Affecting the Internet Landscape* (Thomas Reuters Aspatore ed., Thomas Reuters / Aspatore 2012).

adequate notice and transparency of operations, receiving unwanted or malicious content, and secret tracking of a device user's location.[27]

10.3.3 Breaches

Breaches of DPSIP data violate the law. Legal responsibility shall rest with those causing the breach whether intentional, unintentional, or by negligence. Legal responsibility shall also rest with the holder and processor of the data. Breaches have become a major DPSIP problem. In the US alone, since 2005, there have been over 543 million reported breaches. While any given data breach is a problem in itself, breached data can also lead to four times more cases of identity theft in the next year.[28]

The following types of conduct will all be considered as breaches: hacking, malware, spyware, insider actions, payment card fraud, physical loss, potable losses, stationary devices, and unintended disclosure. Breaches shall also include data collection without an opt-in informed consent including data collection by means of cookies and related electronic tracking. Should a contractor or employee intentionally breach information, it will be considered as insider breaching. Payment card fraud shall include the use of skimming devices at point-of-service terminals to obtain data that enables fraudulent use of credit and debit cards. Physical loss shall include loss where data is discarded, lost, or stolen including loss of non-electronic records such as paper documents. Portable device breaches refer to discarded, lost, or stolen devices that have DPSIP data and are not adequately protected. Such portable devices include CDs, data tapes, hard drives, e-books or readers, laptop computers, PDAs, portable memory devices, smart phones, and other potentially related devices. Stationary devices refer to electronic devices not

---

[27] Ann Cavoukian, *Mobile Near Field Communications (NFC) "Tap 'n Go" Keep it Secure & Private*, Information and Privacy Commissioner of Ontario. (2011), at http://www.ipc.on.ca/images/Resources/mobile-nfc.pdf (last visited on 12 December 2012).

[28] Privacy Rights Clearinghouse, *Data Breaches: A Year in Review. The Top Half Dozen Most Significant Data Breaches in 2011* (2011), at https://www.privacyrights.org/top-data-breach-list-2011 (last visited on 16 December 2012).

designed for mobility, including computers or servers that are discarded, lost, or stolen whilst storing DPSIP data. Unintended disclosure includes sensitive DPSIP information published on a website and data that is mishandled or sent by e-mail, fax, or mail to the wrong party.[29] All breaches must result in notification to the parties affected or those who might be affected, as well as notification to the regulatory agency within 24 hours.

10.3.4 Breach Notification

The first legal requirement for a breach notification standard started in the State of California in the US.[30] The DPSIP law enacted in the CA province of Alberta further establishes a breach notification standard.[31] AU law establishes the same principle.[32]

DPSIP 3.0 adopts the breach notification legal standard. Data controllers must notify affected data subjects and the DPSIP legal authorities of a data breach within 24 hours thereof. The notification must explain the nature of the breach and provide means for affected data subjects to protect themselves from further harm at no expense to the data subject.

10.3.5 Compatibility Declarations

The body politic is based on the principle of the social contract. All government officials swear an allegiance to a constitution or to a ruling king or queen. All of the countries included in this study are committed to a rule of law standard. Behaviorally, juristic and natural persons swear an allegiance to be subject to the rule of law, if only for legal protections.

---

[29] Privacy Rights Clearinghouse, *How to Use the Chronology of Data Breaches*. (2011), at https://www.privacyrights.org/data-breach-how-to (last visited on 17 December 2012).

[30] State of California, *The California Security Breach Information Act (SB-1386), Civil Code §1798.29, §1798.82, & 1798.84* (2002), at http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html (last visited on 3 July 2009). (US)

[31] See § 5.6.1 of this work.

[32] See § 4.11 of this work.

[88] See § 4.6.6 of this work.

DPSIP 3.0 adopts the AU compatibility standard.[33] When making DPSIP decisions and/or policy-related standards, all bureaucrats, courts, executives, and parliamentarians must sign compatibility statements with DPSIP decisions and policies. The compatibility declaration is signed under penalty of perjury with strict civil and criminal penalties applied. The DPSIP 3.0 compatibility standard is also applicable to all executives and officials in the private sector. Violation of the signed compatibility standard is subject to civil and criminal action subject to a DPSIP commission or personal right of action.

10.3.6 Data

DPSIP 3.0 expands the historic definitions of personally identifiable information (PII). References to personal data and data subjects include any direct or indirect identifier or given name or number. Facial recognition software, GPS, on-line activities, and behavioral targeting data are included. Data also includes biometric, cultural, economic, genetic, medical, mental, physical, physiological, and social identifiers.

10.3.7 Data Mining

One of the major advantages of modern information technology is the ability to search, sort, and mine data. Data mining activities must be transparent[34] and must meet the spirit and letter of DPSIP 3.0 legal standards.

---

[34] See Bill Bonner, The Problem of the "Problem" of Privacy, in *Privacy: Management, Legal Issues and Security Aspects* (Tobias K. Buckner & Betram L. Knowles ed., Nova Publishers 2012).

10.3.8 Data Ownership

Information privacy related data must be owned by the natural person or data subject. With a clear informed consent, the data may be shared for limited purposes. Sharing such data does not transfer the ownership right. The natural person or data subject has a moral right as found in intellectual property law, especially copyright law.

The DPSIP 3.0 data ownership principle is based on Section 20 of the SA *Copyright Act* that sets forth some fundamental principles.[35] The data subject "shall be deemed to be the owner of the copyright in question."[36] The natural person data subject "shall have a right to claim authorship of the work and to object to any distortion, mutilation or other modification of it, where such action is or would be prejudicial to the honor or reputation of the author."[37]

The intellectual property laws in all of the countries studied in the current work provide government enforced information privacy and ownership property rights to juristic and selected natural persons. The protections include breach of confidence, copyright, design rights, exclusive rights, infringement, moral rights, passing off,[38] patentable inventions, patents, secrecy, service marks, trademarks, and trade secrets.

The DPSIP protections afforded to juristic persons must also be applied to natural persons. John Rawls[39] argues that two basic principles of justice apply. The principles include the following:

> First: each person is to have an equal right to the most extensive scheme of equal basic liberties compatible with a similar scheme of liberties of others. Second: social and economic inequalities are to be

---

[35] Copyright Act 98 of 1978 (1978). (SA) See section 6.3 of Chapter six of this work.
[36] *Id.* at § 20(2).
[37] *Id.* at § 20(1).
[38] Falsely presenting one's work or product as though it was another's.
[39] John Rawls, *A Theory of Justice*, (The Belknap Press of Harvard University Press rev. ed. 1999) at 53.

> arranged so that they are both (a) reasonably expected to be to everyone's advantage, and (b) attached to positions and offices open to all.[40]

Granted, some juristic persons (i.e., companies and corporations) create value by combining or altering natural resources. When such an economic value-added product is created, the natural resources are purchased for a fee. Such is not the case in DPSIP situation. The DPSIP 3.0 alternative is to purchase the natural resource with consent and a fee.

When a corporation is declared bankrupt, DPSIP records must be disposed. The data may be destroyed. When an existing competitor in the exact same industry sector desires the data, it can negotiate with the bankruptcy court for control over the data. If the court approves the transfer, the new holder must contact each data subject and request an opt-in to the transfer. The only data that can be used is when data subjects have opted-in. All other data must be destroyed.

10.3.9 Data Retention Limits

Data controllers and ISPs may only retain personal data for as long as necessary and to the limits covered in the informed consent. Data shall be kept for at least six months and no longer than two years.[41]

10.3.10 Independence of Office

DPSIP 3.0 legislation should establish an independent Privacy Data Commissioner Model.[42] A registration and licensing system should be

---

[40] *Id.*

[41] European Union Directives, *Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC*. (2006), at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF (last visited on 4 September 2008), at Article 6.

established for the purpose of regulatory control, which would also provide an income stream and increase enforcement powers.[43] The Privacy Commissioner must have the authority to address issues that arise in both government and private organizations. Both government agencies and private organizations must appoint a chief privacy officer who is mandated to comply with the DPSIP law and regulations.[44]

The CA province of British Columbia privacy office maintains independence from the government and government's powers.[45] In CA, the provinces that have enacted DPSIP legislation place enforcement of such acts, including freedom of information laws, under that same agency.[46] Commissioner findings may be subject to judicial review. A similar independence is found with the FTC in the US.[47] The functions of the independent privacy commission are noted in AU law.[48]

A functional independent regulatory agency has an increased ability to address current and evolving technology issues. Legislatures and the executive branches must address a full range of issues while delivering on commitments to past supporters and future financial funders. The judiciary tends to be very conservative in response to technological change; in the countries studied, the judiciary is tied to continuing a common law approach.

With few exceptions, governments have allowed or advanced the interests of corporations over the will of the people. Companies have created or found gaps, and taken possession. When people have objected, such organizations claimed foul. Once one company gets away with an end run play,[49] others join the game. One only has to examine the historic behavior of direct

---

[42] Industry Canada, *Privacy and the Information Highway Regulatory Options for Canada* (Author. 1996). See also § 4.1 of this work.
[43] See §§ 4.1 and 5.8 of this work.
[44] See § 5.8 of this work.
[45] See § 5.62 of this work.
[46] See § 5.6.5.1 of this work.
[47] See § 8.4.1 of this work.
[48] See § 4.6.1.1 of this work.
[49] A strategy in which legal constraints or restrictions are bypassed by deceit or trickery.

marketers, monopolies, and companies like Google, Facebook, and Wal-Mart to see such evidence.

Given the rapid technological change related to DPSIP issues, only an independent regulatory agency has the power to ask relevant questions, investigate problem areas, and intervene effectively. Such an agency can evolve and keep pace with technological change in a way that legislative and judicial case law can not. Following the AU standard, the agency can proceed even when specific damages are not required.[50]

10.3.11 Information Privacy Rights

Information privacy rights are a collective, not just an individual value. The value is based on the economic view of collective and public goods. One cannot benefit from a collective good without others benefiting.[51] Free riders, government or business, should not use information without legally obtaining consent and paying for it.[52] DPSIP 3.0 extends the information privacy right beyond PII to include practices related to behavioral marketing, data mining, and information surveillance.[53] The principle also includes identifiers like cookies, ISP addresses, and genetic data. The new approach adopts the AU standard of credit reports being limited to credit worthiness.[54] DPSIP 3.0 also adopts the AU standards on spent convictions related to criminal records.[55]

---

[50] See Australian Government Office of the Privacy Commissioner, *Issues Paper: A Commonwealth Statutory Cause of Action for Serious Invasion of Privacy; Submission to the Attorney-General's Department*, Author. (2011), at http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/%289A5D88DBA63D32A661E6369859739356%29%7E14B+-+Office+of+the+Australian+Information+Commissioner+-+Word.pdf/$file/14B+-+Office+of+the+Australian+Information+Commissioner+-+Word.pdf (last visited on 12 December 2012).

[51] Pricilla M. Regan, *Legislating Privacy: Technology, Social Values, and Public Policy* (University of North Carolina Press 1995), at 227.

[52] *Id.*, at 228.

[53] See also § 8.6 of this work.

[54] See § 4.1 of this work.

[55] See § 4.6.12 of this work.

10.3.12 Informed Consent and Confidentiality

Prior to collecting, storing, using, distributing, or selling personal information data, the data subject of the information should give an affirmative, freely given, explicit, and informed consent. The informed consent should meet the legal requirements for any lawful written informed consent and be verified by an opt-in process. If a default option is present it should be opt-out or left blank.[56] Silence does not indicate consent.

In AU, consent cannot be a condition to receive products, services, or supplies.[57] CA law also requires an informed consent for data collection and processing.[58] DPSIP 3.0 consents must be explicit, must be subject to simple removal, may not be bundled, apply to any personal profiling, and must be required for all direct marketing activities.

10.3.13 Liability

DPSIP 3.0 legislation and regulations must establish a liability standard for violations. On balance, the most effective standard is strict—an absolute liability standard as noted in AU.[59] The Office of the Australian Information Commissioner and the Australian Law Reform Commission has established recommendations similar to DPSIP 3.0 liability standards. A DPSIP cause of action should be established without proof of damages. As a human right, invasion of privacy should not be subject to proving damages. Such an action

---

[56] See § 2.5.1 of this study. See Charles J. Sykes, *The End of Privacy: Personal Rights in the Surveillance Society*, at 246 (St. Martin's Press 1999).

[57] Ibid. at (¶ 4.3.3), 35.

[58] Canadian Federal Government, *Personal Information Protection and Electronic Document Act*. (2000), at http://laws.justice.gc.ca/en/showtdm/cs/P-8.6 (last visited on 1 November 2012).

[59] See Parliament of New South Wales, *Legislation Review Committee: Strict and Absolute Liability*. (2006), at http://www.parliament.nsw.gov.au/Prod/parlment/committee.nsf/0/88212f7a0a84b436ca2571870022bc55/$FILE/Strict%20and%20Absolute%20Liability%20Discussion%20Paper.pdf (last visited on 6 December 2012).

should apply only to natural persons. The AU view is that juristic or non-human entities do not qualify for a human right.[60]

Liability extends to the breach of confidentiality obligations, breach of privacy obligations, breach of security obligations, damage to tangible property, data loss, illegal acts or omissions, intellectual property infringement, loss caused by service interruption, loss of tangible property, misuse of data, and personal injury (including sickness and death). Liability extends to psychological and psychosocial injury, as well as unlawful acts or omissions.

When a chief privacy officer commits an act of negligence or malpractice related to DPSIP 3.0 standards, the officer and the agency or organization are jointly civilly and criminally responsible. The parties are jointly and severally liable. The liability extends to third-party providers.

The legal analysis principles of accomplice, alternative, derivative, enterprise, market-share, stockholders, and vicarious liability apply. Liability attaches when an individual has been subjected to an act that involves an unauthorized surveillance of the person, or one's home or family life has been subjected to interference—directly or indirectly. Liability attaches when a person's electronic, oral, or written correspondence is disclosed, interfered with, misused, or used without prior informed consent. Liability also attaches when sensitive facts of an individual's private life have been disclosed. Furthermore, liability attaches to government and business employees who access personal data for private purposes or gain. Sensitive facts include more than PII and sensitive information.[61]

---

[60] Australian Government Office of the Privacy Commissioner, *Issues Paper: A Commonwealth Statutory Cause of Action for Serious Invasion of Privacy; Submission to the Attorney-General's Department*, Author. (2011), at http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/%289A5D88DBA63D32A661E6369859739356%29%7E14B+-+Office+of+the+Australian+Information+Commissioner+-+Word.pdf/$file/14B+-+Office+of+the+Australian+Information+Commissioner+-+Word.pdf (last visited on 12 December 2012).

[61] *Id.*

The standard legal analysis of damages can be used in DPSIP cases to determine penalties. Such standards include accumulative, benefit-of-the-bargain, consequential, continuing, discretionary, enhanced, excess, foreseeable, future, hedonic, intervening, irreparable, punitive, putative, reliance, restitution, treble, uncertain, and unliquidated damages.

Legal causes of actions may include either individual or class action litigation parties. Damages, including punitive damages, fines, and penalties shall be awarded to the litigants.[62] Following the AU standard, "no maximum award of damages" (e.g., financial judgments) for noneconomic should be considered.[63]

The civil and criminal penalties for a DPSIP violation shall be no less than the maximum penalties for intellectual property violations sought by business organizations and juristic persons. The same principle applies to government agencies. The non-inclusive list shall include standards for copyright, moral rights, patent rights, publicity rights, service mark, trademarks, trade-secrets, and unfair competition protections.

10.3.14 Licensure

All organizations that collect or process DPSIP data must be licensed by the government. Significant DPSIP 3.0 violations can be punished by a revocation of the DPSIP license and criminal sanctions. Such processors must also file an annual audit notification filing similar to the practice in the UK.[64] Chief Privacy Officers must also be licensed and face similar penalties for DPSIP violations. This approach is similar to laws that regulate professionals whose practices involve consumer protection.[65] Failure to

---

[62] The DPSIP damages pattern in the US has been to award penalty payments to not-for-profit privacy advocacy groups.

[63] Australian Government, *Issues Paper: A Commonwealth Statutory Cause of Action for Serious Invasion of Privacy*, (Australian Government ed. 2011 September).

[64] United Kingdom Government, *The UK Data Protection Act of 1998*. ch. 29. Part III § 16 (1998), at http://www.hmso.gov.uk/acts/acts1984/1984035.htm (last visited on 17 May 2009).

[65] Examples include attorneys, mental health professionals, and physicians. The list also includes barbers, contractors, and even realtors.

maintain a license or register is a criminal offense and can include significant monetary fines.

10.3.15 Opt-in

DPSIP 3.0 laws and regulations must require an opt-in approach standard similar to the AU standard.[66] The UK All Party Parliamentary Communications Group has also recommended an opt-in approach.[67]

The German Privacy Agency[68] has approved an opt-in approach in some situations. The agency has worked with Google for an opt-in in its *Find my Face* program option. Facebook has yet to comply.[69]

10.3.16 Privacy by Design—Privacy by Default

Privacy by default and privacy by design standards apply to device manufacturers, application developers, and designers. The standards also apply to service providers like Cloud computing and ISPs. At a minimum, the principles include products and services that are "proactive not reactive; preventative not remedial approaches; privacy as the default setting; privacy embedded into design; full functionality—positive-sum, not a zero-sum strategy; end-to-end security—full lifecycle protection; visibility and transparency—keep it open; and respect for user privacy—keep it user-centric."[70]

---

[66] See § 4.11 of this work.

[67] All Party Parliamentary Communications Group, Can we keep our hands off the net? Report of an Inquiry by the All Party Parliamentary Communications Group. (2009), at http://www.apcomms.org.uk/uploads/apComms_Final_Report.pdf (last visited on 19 October 2009). The group is an open and independent organization of MPs and Lords from all political parties. The group encourages stakeholders to present evidence and testimony on communication issues. The stakeholders include the Government, Parliamentarians, industry, and consumer groups.

[68] Known as the Der Hamburgishche Beauftragte für Datenschutz und Informationsfreiheit.

[69] Kevin Shalvey, *Germany Privacy Agency OK With Google Facial Recognition* Click. (2011), at http://blogs.investors.com/click/index.php/home/60-tech/4045-germany-privacy-agency-ok-at-least-now-with-google-facial- (last visited on 21 December 2012).

[70] Ann Cavoukian, *Mobile Near Field Communications (NFC) "Tap 'n Go" Keep it Secure & Private*, Information and Privacy Commissioner of Ontario. (2011), at

By design and default, privacy protections must be included in all programs, practices, and technologies. The default must limit processing options to only those activities that the data subject has approved. Such data shall not be made available to an indefinite number of parties or other organizations.

10.3.17 Private Right of Action

DPSIP 3.0 establishes business organization and government agency CPOs and government agencies to monitor and regulate DPSIP legal standards. The gravity of the issues also requires that private partes must have a private right of action. Such a private right also includes the availability of class action litigations.[71]

10.3.18 Privacy Impact Assessment

Prior to using any DPSIP-related business or government methods or the government granting any intellectual property protection, the requesting party must conduct and gain approval of the proposal through a privacy impact study and approval.[72] A privacy impact study and approval must be conducted prior to any legislative or regulatory actions. The courts must consider, subject to review, the privacy impact on relevant cases.

AU and CA have established some impact assessment guidelines. The basic principles are sound and must be integrated into DPSIP 3.0 legislation and regulations.

The AU[73] guidelines address a project description, which included mapping the information flows and privacy framework, privacy impact analysis, and

---

http://www.ipc.on.ca/images/Resources/mobile-nfc.pdf (last visited on 12 December 2012).

[71] See § 8.3.7 of this work.

[72] See §§ 2.5.2 and 2.6 of this study.

[73] Office of the Australian Information Commissioner, *Privacy Impact Assessment Guide (Revised May 2010)*. (2010), at

privacy management practices. The final stage is a full report that included recommendations for future action.

The Treasury Board of Canada Secretariat issued a useful set of *Privacy Impact Assessment Guidelines*.[74] They establish a gold standard for partial compliance; unfortunately, they donot apply to business organizations. A further problem is that the CA Court ruled that the standards are not binding; however, standards do help interpret the legislation.[75] The CA Information Commissioner Office produced a stronger Privacy Impact Assessment document.[76] Under DPSIP 3.0 guidelines, the principles must apply to both business and government.

Privacy impact assessments relate to government agencies that address DPSIP issues, including the administration or executive branch, legislators or parliamentarians, and the court or judicial branches. In the private sector, privacy impact assessments are required by all personal data controllers and processors.

Natural living person risk data factors must be identified in the assessment to identify clear, effective, and valid protections that will be afforded. While following the established PII items, the impact assessment must also incorporate the biological risk factors including but not limited to: biometric data, genetic data, health care utilization, health status, infectious diseases,

---

http://www.oaic.gov.au/publications/guidelines/Privacy_Impact_Assessment_Guide.html (last visited on 20 June 2012).

[74] Treasury Board of Canada Secretariat, *Privacy Impact Assessment Guidelines: A Framework to Manage Privacy Risks*. (2002), at http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paipg-pefrld2-eng.asp (last visited on 20 July 2010).

[75] *Canada Post Corp. v. Canada (Minister of Public Works) (1995)*, [1995] F.C.J. No. 241, 60 C.P.R. (3d) 441, 91 F.T.R. 320 (note), (sub nom. Societe canadienne des postes v. Canada) [1995] 2 F.C. 110, 179 N.R. 350, 30 Admin. L.R. (2d) 242, 1995 CarswellNat 688, 1995 CarswellNat 652 (Fed. C.A.), (10 February 1995). (CA) See also *Canada (Information Commissioner) v. Canada (Minister of Citizenship & Immigration)*, 2002 CarswellNat 1476, 2002 FCA 270, 291 N.R. 236, 228 F.T.R. 319 (note), [2003] 1 F.C. 219, 21 C.P.R. (4th) 30, 1 Admin. L.R. (4th) 270, (21 June 2002). (CA)

[76] Information Commissioner Office, *Privacy Impact Assessment Handbook*. (2009), at http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/html/0-advice.html (last visited on 6 October 2012).

and mental disorders. Psychosocial risk factors shall include but not be limited to: creditworthiness, economic situation, legal activities, location, personal behavior, personal preferences, personal reliability, and work performance.

DPSIP 3.0 legal standards require that all government and business organizations perform a privacy impact assessment on all DPSIP-related policies, practices, and technologies prior to adoption and use. The assessment must include factors of compliance, information security procedures, and stakeholder management. The focus is on avoiding inadequate solutions, avoiding loss of recognition and trust, avoiding unnecessary costs, identifying and managing risks, informing communication strategies, and meeting and exceeding DPSIP legal requirements. If DPSIP risks exist, the assessment must provide an identification of less privacy-invasive alternatives, means to avoid negative impacts, and ways to eliminate the negative impact on privacy rights. The privacy right extends to personal information, the privacy of the person, one's personal behavior, and personal communications. The assessment must clearly establish privacy protections, means to avoid breaches, function creep,[77] and misuse. The assessment process is continual. Submission of the assessment includes an acknowledgement and acceptance of risks, impacts, as well as legal liabilities.[78]

The DPSIP 3.0 assessment must address all of the issues advocated by Salvatore Colletti, Divonne Smoyer, and Bernard Nash.[79] The assessment must address all existing and potentially new federal and state DPSIP laws and regulations. The task includes international laws and the impact of

---

[77] The subtle use of technology or systems to invade information privacy rights beyond the original intent of the data collection.

[78] See Information Commissioner Office of The UK, *Privacy Impact Assessment, Version 2*, Author. (2009), at http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/files/PIAhandbookV2.pdf (last visited on 3 March 2012).

[79] Salvatore Colletti, et al., *Top Ten Recommendations for Improving Your Company's Data Security Compliance*, Acc: Association of Corporate Counsel. (2009), at http://www.acc.com/legalresources/publications/topten/top-ten-recommendations-for-improving-your-company.cfm (last visited on 2 February 2012).

transferring data between countries and safe harbors. The assessment must include monitoring computer systems to detect any intrusions, vulnerabilities, and weaknesses (both personal and technological). The process must assess and reassess the data security policies and the sufficiency of the standards. The organization must be held responsible to the standard that all employees are trained and monitored on DPSIP policies and practices. The process must verify that the organization limits the amount of personal information that is collected, stored, and transferred. The organization must establish quality mechanisms for the timely disposal of personal information. The assessment must ensure that the data security practices of third-party contractors are adequate, both legally and technologically. The PIA must establish a sound incident response plan for preventing the loss of personal information and for reacting to any losses of personal data that occur. The assessment must document that it encrypts all private information. The PIA must document that the policies and practices apply to technological data and even paper records.

10.3.19 Reports

DPSIP 3.0 commissioners must issue periodic reports based on the CA practices. The office of the commissioner must also provide public education on the law, regulations, and acceptable practices.[80]

10.3.20 Right to be Forgotten

DPSIP 3.0 recognizes the right of data subjects to be forgotten.[81] A subject can object to a controller's processing of the subject's data and show that the data is no longer needed or warranted. The subject may withdraw any prior consent. In such situations, the data controller must permanently erase any such personal data.

---

[80] See § 5.9.2 of this work.
[81] See Chapter 3 section 3.4.3.2; Chapter 5. section 5.9.2; Chapter 6 section 6.5,

The principle of a right to be forgotten is relatively new based on CA's and proposed EU standards. A common charge is that the law is slow to respond to technology and business advances. The reality is that legal scholars often sound a beacon call for attention; however, legislatures and the judiciary are slow to heed the call. Each has its own self-serving set of assumptions and beliefs to justify inaction. During this assumption of belief error, business and government organizations take aggressive claim to rights while ignoring the law of unintended consequences. When confronted with their invasion of personal and property rights, governments and entrepreneurial business sources claim foul. The charge of foul ignores the existing spirit of previously established legal principles.

International corporations like Google, Facebook, and Linkedin will vigorously fight legal constraints to their theft, without consent, of DPSIP data. Such organizations may claim that the data subject freely participates in the activities; these organizations ignore the fact that the data subject has provided no written informed consent. Such organizations have a legal obligation make the data subject right – with appropriate redress.

Data subjects have the legal right to delete information posted online, even if one has given consent or release to make the data public. The data subject shall have the right to obtain erasure of any public Internet link to personal data. The right shall apply to any copy of or replication of personal data that is contained in any publicly available communication service.

10.3.21 Right to Data Portability

A data subject has the legal right to transfer personal data from one automated processing system to another. A data controller may not interfere with the subject's right by policy or technology. The controller may not charge a fee for any portability request.

10.3.22 Subject Rights

Similar to the UK standard, DPSIP 3.0 standards provide that a data subject must have a legal right of data corrections, prevention of processing, failure compensation, and rectification.[82] Individuals must have a legal right to access personal data that is held about them. Individuals must be able to legally block, erase, and rectify inaccurate data. Individuals must also have a legal right to block the processing of data not covered by the written informed consent.

10.3.23 Technology-Based Surveillance

Governments have an obligation to protect their citizens from criminal activities within strict parameters with legally justified checks and balances. The principle of the rule of law applies. At the same time, the government must also protect the innocent from unwarranted interference and even unwarranted surveillance.[83] The government has the right to develop technology that can aid its legitimate functions like facial recognition technology. However, the government does not have the right to allow development of or sale of such technology for private gain. Nor can the government circumvent its constraints by purchasing such technology or data from private sources. The government can restrictively license and monitor the development of DPSIP technology similar to activities restricted to certain medical research and weapons that could destroy the nature of civilization.

Private businesses and corporations—even powerful multinational corporations—do not have the same legal right or lawful justification. Arguments of providing wanted services or promoting sales do not justify the use of spying technologies. Without government constraints, far too many business organizations are more than willing to pillage and rape the DPSIP rights of the people.

---

[82] See Part 2 §§ 7-15.

[83] This basic legal principle has been forgotten in the UK and is being ignored in the US under the guise of fighting the so called war on terror.

Some business organizations have already started to use facial recognition technologies in a number of products and services with no legal constraints. Examples include digital billboards, mobile apps, and even social networks. Some companies want to automatically tag photographs of even strangers.[84] There is no informed consent or opt-in option. Such technology can be used by private individuals to take pictures of strangers anywhere to identify them and discover everything about them—including a full range of DPSIP data—without the person's awareness or consent. The data can be used for identity theft or even worse. The recent research conducted by Alessandro Acquisti at Carnegie Mellon University showed that the potential threat is not paranoia or science fiction.[85]

AU police claim that many businesses use biometric facial recognition technology without any public notice. Westfield, the international shopping mall corporation, has noted that it will use such technology in its malls for tracking all customer activities—without notice or consent.[86] Large international corporations like Wal-Mart are requiring their suppliers to provide RFID tags to products to track item movement.[87] The use of RFID and even smart meters can serve a useful purpose as long as the data is not linked to an individual consumer's DPSIP data.

---

[84] In the US the FTC is starting to investigate such practices. See Alysa Zeltzer Hutnik & Sharon Kim Schiavetti, *The FTC Offers Framework for Facial Recognition Technology*, Acc: Association of Corporate Counsel (2011), at http://www.lexology.com/library/detail.aspx?g=a93a9908-880c-48cf-b5c6-77b0002cb618 (last visited on 12 December 2012).

[85] Alessandro Acquisti & Richard Power, *New Study Co-Authored by CyLab Researcher: Face Recognition Software and Social Media Result in Increased Privacy Risks*, Cylab News: Carnegie Mellon University (2011), at http://www.cylab.cmu.edu/news_events/news/2011/acquisti-study-finds-face-recognition-software-social-media-increase-privacy-risks.html (last visited on 1 August 2012).

[86] Saffron Howden, *No Place For Crooks to Hide*, Sydney Morning Herald. (2009), at http://innovya.com/2009/12/10/no-place-for-crooks-to-hide/ (last visited on 9 December 2009).

[87] Katherine Albrecht & Liz Mcintyre, *Spychips: How Major Corporations and Government Plan to Track Your Every Move with RFID*, (Nelson Current ed. 2005).

DPSIP 3.0 standards require that invasive technologies similar to facial recognition software or hardware, NFC devices, RFID, and smart meters should not be sold to or used by private parties and business organizations because of the innate DPSIP, fraud, identify theft, and stalking issues. Possession and use of such technology is subject to civil and criminal sanctions for the manufacturer, distributor, seller, purchaser, and user, including corporations and executives. Sanctions shall include civil and criminal remedies. Intellectual protections shall not be afforded to such technologies, unless a successful privacy impact assessment is created and audited and the technology follows the quality standards of privacy by design.

10.3.24 Violations

Violations of DPSIP 3.0 laws and regulations must give rise to civil penalties [using a strict absolute liability principle], criminal penalties, and/or loss of the information processing license and registration. The cost of violation must be strong enough to function as a deterrent to deviant behavior.

10.4 Exemptions

DPSIP 3.0 acknowledges the rightful need for limited exemptions to the legal standard. When properly monitored and when warrants are obtained, the government's police powers must be an exemption. The function may include the investigation, indictment, and prosecution of crimes. Government agencies are allowed to investigate and prosecute ethical breaches of regulated professions. The state's power of taxation or duty collection may be exempted.

Traditional exemptions of artistic, historic, journalistic, literary, and research purposes are not to be presumed or seen as universal. Any such exemption must be within a strict standard of fulfilling the people's need to know and is subject to approval by the organization's CPO, government CPO office, or the courts. Prior consultation and authorization is recommended. Publication or use of DPSIP data without an acceptable privacy impact assessment shall be

considered ipso facto[88] proof of a material breach of the DPSIP law and regulations.

Some jurists have created and perpetuated the legal fiction of a "reasonable expectation of privacy" as it relates to informational DPSIP issues. When a person walks through a shopping center, one could expect that he or she will be seen by another person. However, people may not expect that facial recognition software and GPS technology may trace their every step, collect total personal data on every purchase, and even track purchased goods after purchase. Credit card data on purchased items must be limited to credit purchase data only. In such situations a reasonable expectation of privacy standard must apply.

A common exception in DPSIP legislation is national security. The rule allows governments to ignore DPSIP laws with a simple and even unsubstantiated claim. Historically, national security claims have been made to suspend civil and human rights. Claims of national security are not an automatic exemption; however, such issues can be processed using the checks and balances of the state's police powers. Perhaps Dr. Samuel Johnson addressed the issue best when he said that "patriotism is the last refuge of a scoundrel."[89] A few decades later, Ambrose Bierce offered a friendly amendment that "patriotism is the first refuge of a scoundrel."[90]

10.5 Alternative Legal Considerations

The adoption of DPSIP 3.0 legal standards will limit some assumed laisez-faire personal information business practices. Violations of basic civil and human rights, consumer protections, and international treaties justify regulatory constraints. Legal protections afforded to government agencies and business organizations must also be extended to DPSIP legal issues.

---

[88] Res ipso facto means "by the fact itself."

[89] James Boswell, *The Life of Samuel Johnson, LL.D.*, at 615 (Henry Baldwin for Charles Dilly ed. 1791).

[90] Ambrose Bierce, *The Collected Writings of Ambrose Bierce*, at 323. (The Citadel Press ed. 1946).

In response to the new DPSIP legal standards, business organizations that deal with personal data may seek insurance coverage to respond to the risk. Such a practice is standard in the business world. Business organizations may seek to establish international DPSIP 3.0 compliance standards and certification similar to International Standards for Business, Government, and Society.[91]

DPSIP issues will continue to exist. At the time of this writing, many states and countries have passed a range of approaches. In some regional groups like the EU and APEC, staffers are working on evolving regional standards. DPSIP 4.0 may include an international treaty based approach. Efforts at an international DPSIP treaty must begin now. A sound basis is the DPSIP 3.0 standards.

10.6 Limitations of the Current Study and Future Research Recommendations

The current study is an interdisciplinary analysis of modern DPSIP legal and regulatory issues. The focus has included perspectives from the history and current positions of the law, legal theory, human rights, business and government practices, information technology, psychosocial concerns, and psychological research. The study is a comparative law analysis using sociolegal and positive law principles. The study examines international legal

[91] *See International Standards for Business Government and Society,* Information Technology*. (2011), at http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_ics_browse.htm?ICS1=35 (last visited on 26 December 2012). See also standards 17799, 22307, ISO 27000 Standards Series.*

standards and guidelines with a major focus on the AU, CA, SA, UK, and US legal standards and approaches.

The approach reports the legal research and writings of distinguished legal authorities in each of the countries studied. Examples include Professors J. Neethling and Anneliese Roos in SA; Professor Ian Lloyd in the UK; Professor Lawrence Lessig in the US; Professor Michael Geist in CA; and the Honorable Justice Michael Kirby in AU.

The strengths of the study also reveal weaknesses in research. The study focuses on historic and current issues and practices. As the field develops, additional research will be needed to keep pace and even advance further prescriptive legal approaches.

The design of the current study is limited to five generally English-speaking countries. Future research could add to the list or focus on different countries. During the course of this study interesting developments have evolved in other countries like Mexico and India. Following the lead of the work of Anneliese Roos,[92] future work may focus on some European countries like France and Germany.

With the exception of the work of revisionist historians, the history of the law rarely changes. Historic insights can be revisited. As the technology and law advance, some of the current data may be changed or become footnotes. This is the nature of legal research.

10.7 The Need for DPSIP 3.0 Vigilance

DPSIP intrusions, surveillance, and violations are not victimless crimes or a civil law nuisance. DPSIP breaches damage and harm the body politic. Whether done by governments, business organizations, not-for-profit

[92] Anneliese Roos, *The Law of Data (Privacy) Protection: A Comparative and Theoretical Study* (LL.D. thesis, UNISA ed. 2003).

organizations, or even individuals, DPSIP violations damage basic legal and government principles.

Elaine Scarry writes that such violations repeal guarantees of privacy and political freedom. Such behaviors reverse the fundamental constitutional "requirement that people's lives be private and the work of government officials be public; instead it crafts a set of conditions in which our inner lives become transparent, and the workings of the government [or business] become opaque."[93]

The first parade-of-horribles[94] harm is that the countries in the study follow the UK lead in establishing a surveillance society, where all traditionally private behavior is monitored by faceless and non-accountable government bureaucrats. Few checks or balances on big brother exist, and the legal principle of obtaining a legal warrant is often ignored. Those who sanction such violations of basic legal rights attempt to justify the violations in the name of security. Violations of such principles are constitutional violations.

The second parade-of-horribles harm is that juristic organizations[95] violate DPSIP standards in the name of making profits. The theft of personal information is often framed as providing better services while it is in fact making profits that violate basic principles of distributive justice. A corollary is found when governments obtain, even pay for, and use little brother to obtain data, which is ordinarily illegal to possess.

The third parade-of-horribles harm claim is not popular with neo-conservative advocates: a claim of damages can be made on an individual and class action based on a behavioral basis.

From a psychological and psychosocial perspective, information privacy is an

---

[93] Elaine Scarry, *Rule of Law, Misrule of Men*, (A Boston Review Book, The MIT Press ed. 2010) at 9-10.
[94] Also known as the slippery slope principle or the parade-of-horrors objection.
[95] Known as Little Brother.

imperative. Information privacy has powerful consequential and meaningful impacts on personal and societal wellbeing.[96] "Privacy plays a central role in human affairs. Without some degree of privacy, civilized life would not be possible."[97] Research in anthropology, architecture, design professions, law, political science, psychology, and sociology supports the thesis.[98] "Respect for another's privacy is a legitimate expectation in all social relationships. As a value, privacy does not exist in isolation, but is part and parcel of the system and values that regulates action in society."[99]

Data protection and information privacy is more than a legal debate. The concepts, principles, and laws are based on legal standards and psychological–psychosocial realities. Information privacy laws recognize relevant psychological and psychosocial research findings.

> When procedures inhibit one's ability to control personal information, one may be forced to alter the image that one portrays to others. That is, one may be unintentionally forced to reveal information that he or she would like to keep private, as part of his or her personal identity. In a similar manner, the public self that one wishes to reveal may be threatened when privacy is impinged. Privacy ensures control of self-other boundaries.[100]

Data protection and information privacy are the focus of concern and study from a range of disciplines. Ideally, the law should culminate the theory, research, and data from legal history, business practices, political science, philosophy, psychology, and sociology. Eric Fromm, a famous psychoanalyst,

---

[96] See Charles T. Melton, *The significance of law in the everyday lives of children and families, 22 Georgia Law Review,* 851 (1988). James Rachels, Why Privacy is Important, 4 *Philosophical and Public Affairs* 4, 323 (1975). Charles R. Tremper & Mark A. Small, Privacy Regulation of Computer-Assisted Testing and Instruction, 63 *Washington Law Review* 3, 841 (1988).

[97] Louis W. Hodges, The Journalist and Privacy, 9 *Journal of Mass Media Ethics* 4, 97 (1994) at 200.

[98] Irwin Altman, Privacy: A Conceptual Analysis, 8 *Environment and Behavior* 1, 7 (1976) at 7.

[99] Arnold Simmel, Privacy Is Not An Isolated Freedom, in *Privacy (Nomos, XIII)* (J. Ronald Pennock & John W. Chapman eds., Atherton Press 1971) at 71.

[100] Bradley J. Alge, Effects of Computer Surveillance on Perceptions of Privacy and Procedural Justice, 86 *Journal of Applied Psychology* 4, 798 (2001) at 798.

wrote about issues of freedom and liberty. He offered a challenge to those concerned about both and information privacy. He declared as follows:

> We forget that, although each of the liberties which have been won must be defended with utmost vigor, the problem of freedom is not only a quantitative one, but a qualitative one; that we not only have to preserve and increase the traditional freedom, but we have to gain a new kind of freedom, one which enables us to realize our own individual self, to have faith in this self and in life.[101]

The research supports the position of Oscar Ruebhausen and O. G. Brim.[102] The authors maintained the following:

> The essence of privacy is no more, and certainly no less, than the freedom of the individual to pick and choose for himself the time and circumstances under which, and most importantly, the extent to which, his attitudes, beliefs, behavior, and opinions are to be shared with or withheld from others. The right to privacy is, therefore, a positive claim to a status of personal dignity—a claim for freedom, if you will, but freedom of a very special kind.[103]

Perhaps the best description of the psychological and psychosocial principle supporting information privacy was argued by Immanuel Kant. He explained that “Man is inclined to be reserved. ... We do not press our friends to come into our water-closet, although they know that we have one just like themselves. ... Everyone has a right to prevent others from watching and scrutinizing his actions."[104]

Writing from a legal perspective, Charles Fried expanded the Kantian view.

---

[101] Eric Fromm, *Escape from Freedom*,(Holt, Rinehart & Winston, Inc ed. 1941) at 126.
[102] Oscar M. Ruebhausen & O. G. Brim, Privacy and Behavioral Research, 65 *Columbia Law Review,* 1184 (1965).
[103] *Id*. at 1211.
[104] Kant, I. (1930). *Ethical duties toward others: Truthfulness* (L. Infield, Trans.). (Indianapolis, IN: Hackett Publishing Company) at 225.

He maintained as follows:

> Privacy is not just one possible means among others to insure some other value, but it is necessarily related to ends and relations of the most fundamental sort: respect, love, friendship and trust. Privacy is not merely a good technique for furthering these fundamental relations; rather without privacy they are simply inconceivable.[105]

Information privacy represents and performs a vital psychological and social function. Individuals are more than social and political entities. Individuals are discrete human beings with rights. Information privacy is a vital psychological aspect and an integral part of functional autonomy and self-development.

Abraham Maslow[106] wrote about human needs. The basic need, the one on which all other psychological needs are based, is security. Information privacy is an element of security. Julie Inness[107] wrote that privacy infringements result in a sense of "violation, harm, and loss of agency." Privacy allows people "to conduct ourselves... in a way that serves purely individual demands."[108] The "interpersonal spheres of privacy protected from the public gaze are essential for human emotional … life."[109] An essential issue is "What we can tolerate having out in the open between us depends on what we think we can handle jointly without crippling our relations for other purposes."[110]

---

[105] Charles Fried, Privacy (A Moral Analysis) in *Philosophical Dimensions of Privacy: An Anthology* (Ferdinand David Schoeman ed., Cambridge University Press 1984) at 205.
[106] Abraham H. Maslow, *Toward a Psychology of Being*, (John Wiley & Sons 3rd ed. 1999).
[107] Julie C. Inness, *Privacy, Intimacy and Isolation*, (Oxford University Press ed. 1992) at 3.
[108] Thomas Nagel, Concealment and Exposure, 27 *Philosophy and Public Affairs* 1, 3 (1998) at 17.
[109] *Id.* at 20.
[110] *Id.* at 16.

"Men and animals share several basic mechanisms for claiming privacy among their own fellows."[111] Robert Ardrey[112] established *The Territorial Imperative* as an accepted biological basis for different types of privacy. Louis Hodges argued that "Privacy plays a central role in human affairs. Without some degree of privacy, civilized life would not be possible."[113]

Charles Fried supported the psychological need for information privacy in social relations. Fried wrote about the "sharing of information about one's actions, beliefs, or emotions which one does not share with all, and which one has the right not to share with anyone. By conferring this right, privacy creates the moral capital which we spend in friendship and love."[114] Ruth Gavison takes the need for information privacy a step further. Information privacy allows for the "promotion of liberty, autonomy, human relations, and furthering the existence of a free society."[115]

The importance of and correlation of information privacy and psychological well-being has been the subject of scientific studies. The two principles and dynamics are connected. Judee Burgoon established the psychological and psychosocial significance of "the degree of control that the individual can exercise, not only over the initial release of the information but also over its subsequent distribution and use."[116] Irwin Altman clearly documented the need for information privacy as a psychological imperative for psychosocial well-being and functioning. Privacy involves a "selective control of access to the self or to one's group."[117]

Sandra Petronio showed the psychological importance of having control over one's personal information. She found the following:

---

[111] Alan F. Westin, *Privacy and Freedom*, (Atheneum ed. 1967) at 8.
[112] Robert Ardrey, *The Territorial Imperative*, (Atheneum ed. 1966).
[113] Louis W. Hodges, The Journalist and Privacy, 9 *Journal of Mass Media Ethics* 4, 97 (1994) at 200.
[114] Charles Fried, Privacy, 77 *Yale Law Journal,* 475 (1968) at 492.
[115] Ruth Gavison, Privacy and the Limits of Law, 89 *Yale Law Journal* 3, 421 (1980) at 423.
[116] Judee K. Burgoon, Privacy and Communication, in *Communication Yearbook 6* (Michael Burgoon & Noel E. Doran eds., Sage Publications 1982) at 230.
[117] Irwin Altman, *The Environment and Social Behavior: Privacy, Personal Space, Territory, Crowding*, (Brooks/Cole Publishing Company ed. 1975) at 18.

> Revealing private information is risky because there is a potential vulnerability when revealing aspects of the self. Receiving private information from another may also result in the need for protecting oneself. In order to manage both disclosing and receiving private information, individuals erect a metaphoric boundary to reduce the possibility of losing face and as a means of protection. Also, people use a set of rules or criteria to control the boundary and regulate the flow of private information to and from others.[118]

Sandra Petronio argued that privacy management is a demand–response between at least two people.[119] When given the right, disclosing people use five factors in deciding when to release data: "(1) need to tell, (2) predicted outcome(s), (3) riskiness of revealing the specific information, (4) privacy level of the specific information, and (5) degree of emotional self-control."[120]

Valerian Derlega and Alan Chaiken define privacy from a psychological and psychosocial perspective. The essential feature of information privacy is control over all aspects of self-disclosure. Control over "what one person tells another about himself/herself"[121] is a psychological imperative. The authors concluded as follows:

> Privacy represents control over the amount of interaction we choose to maintain with others. If one can choose how much or how little to divulge about oneself to another voluntarily, privacy is maintained. If another person can influence how much information we divulge about ourselves or how much information input we let in about others, a lower level of privacy exists.[122]

> Regulating access to the self in terms of self-disclosure outputs and inputs affects one's own vulnerability to control by others as well as one's ability to

---

[118] Sandra Petronio, Communication Boundary Management: A Theoretical Model of Managing Disclosure of Private Information Between Marital Couples, 1 *Communication Theory* 4, 311 (1991) at 311.
[119] *Id.* at 314.
[120] *Id.* at 316.
[121] Valerian J. Derlega & Alan L. Chaiken, Privacy and Self-Disclosure in Social Relationships, 33 *Journal of Social Issues* 3, 102 (1977) at 103.
[122] *Id.* at 102.

> influence other's outcomes (or to exercise power).[123]

Alan Westin summarized the importance of information privacy. He wrote:

> Psychologists and sociologists have linked the development and maintenance of this sense of individuality to the human need for autonomy—the desire to avoid being manipulated or dominated wholly by others. … The most serious threat to the individual's autonomy is the possibility that someone may penetrate the inner zone.[124]

Westin also noted cases where information privacy violations caused damages.

> The numerous instances of suicides and nervous breakdowns resulting from such exposures by government investigation, press stories, and even published research constantly remind a free society that only grave social need can ever justify destruction of the privacy which guards the individual's ultimate autonomy.[125]

Robert Laufer and Maxine Wolfe[126] maintain that information privacy involves information and interaction management. In the study, researchers found that individuals whose private data was violated reported significant levels of loss of control—not only of the information but in inter-action boundaries.

Ferdinand Schoeman[127] summarized the psychological and psychosocial research related to information privacy. He found:

> What makes information private or intimate for a person is not just a function

---

[123] *Id.* at 109.
[124] Alan F. Westin, *Privacy and Freedom*, (Atheneum ed. 1967) at 33.
[125] *Id.* at 33-34.
[126] Robert S. Laufer & Maxine Wolfe, Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory, 33 *Journal of Social Issues* 3, 22 (1977).
[127] Ferdinand D. Schoeman, Privacy and Intimate Information, in *Philosophical Dimensions of Privacy: An Anthology* (Ferdinand D. Schoeman ed., Cambridge University Press 1984).

> of the content of the information; it is also a function of the role the information plays for the person... their importance to our conceptions of ourselves and to our relationships with others. To entrust another with intimate information is not primarily to provide the other with an arsenal that could prove detrimental to ourselves if revealed to the world. Typically, this involves a trust that the other will not regard the information as inconsequential.[128]

In his 4 March 1837 Presidential Farewell Address, Andrew Jackson addressed one of the key issues of his time. DPSIP issues are the key legal, political, cultural, and psychosocial issues of this day. President Jackson's words apply to the issues of this study. He said:

> But you must remember, my fellow-citizens, that eternal vigilance by the people is the price of liberty, and that you must pay the price if you wish to secure the blessing. It behooves you, therefore, to be watchful in your States as well as in the Federal Government.[129]

Since the middle ages, advancements in civil and human rights have involved a struggle against those who hold power and authority however gained, even against those who want to maintain their power at all costs. Advancement in DPSIP protections is no different. Those who want to assert their economic and political powers of social control will not give up their advantage easily.

Strong DPSIP protections are justified by:

1. Research in the selected countries that shows that the majority of the people want DPSIP protections and the numbers are increasing over the years.

---

[128] Ferdinand D. Schoeman, Privacy and Intimate Information, in *Philosophical Dimensions of Privacy: An Anthology* (Ferdinand D. Schoeman ed., Cambridge University Press 1984) at 405-406.

[129] Andrew Jackson, *Presidential Farewell Address*. (1837 March 4), at ¶ 27 at http://www.presidentialrhetoric.com/historicspeeches/jackson/farewelladdress.html (last visited on 29 December 2012).

2. Basic psychological and psychosocial research
3. Enlightenment political theory
4. Historic legal theory and agreements
5. Basic modern legal checks and balances and consumer protections
6. Basic principles of corporate social responsibility.

SA has some options. SA can:

1. Ignore or reject the DPSIP advances of the international community and its trading partners.
2. Catch up to the standards of its various trading partners and the Western world.
3. Follow its Constitutional mandate and advance DPSIP standards for itself and the world.

Appendix A

International Treaties and Conventions

Declaration	AU	CA	SA	UK	US
International					
International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families	D	D	D	D	D
International Covenant on Civil and Political Rights	P	P	P	P	P
The Convention on the Rights of the Child	R	R	R	R	S
The Universal Declaration of Human Rights	P	P	Abstained	P	P
UN Guidelines for the Regulation of Computerized Personal Data Files Adopted by General Assembly resolution 45/95 on 14 December 1990 – no vote recorded [NV]	NV	NV	NV	NV	NV
Regional - Africa					
African Charter on Human and People's Rights	N/A	N/A	R	N/A	N/A
Declaration of Principles on Freedom of Expression in Africa	N/A	N/A	R	N/A	N/A
Regional – Asia					
Asia-Pacific Economic Cooperation Privacy Charter	S	S	N/A	N/A	S
Regional – European					
European Convention of Human Rights and Fundamental	N/A	N/A	N/A	P	N/A

Freedoms					
European Union Declaration	Seek	Seek	N/A	P	Seek
OECD Privacy Standards	R	R	N/A	P	R
Regional – Western Hemisphere					
American Declaration of the Rights and Duties of Man	N/A	S	N/A	N/A	S
Guidelines Concerning Personal Data Files	N/A	S	N/A	N/A	S

A – Accession
D – Did not support
N/A – Not Applicable
NV - No Vote Recorded [NV]
P - Party
R – Ratified
S - Signatory
Seek – Seeking compliance

Bibliography[1]

Books

Marc Abrams, *World Wide Web: Beyond the Basics* (Prentice Hall. 1998).

Alessanadro Acquisti, et al., *Digital Privacy: Theory, Technologies, and Practices* (Auerbach Publications. 2008).

John Emerich Acton & Edward Dalberg, *Essays on Freedom and Power* (Beacon Press ed. 1948).

African Commission on Human and Peoples' Rights, *African Charter on Human and Peoples' Rights* (Author. 1981).

Philip E. Agre & Marc Rotenberg, *Technology and Privacy: The New Landscape* (The MIT Press. 1998).

Katherine Albrecht & Liz Mcintyre, *Spychips: How Major Corporations and Government Plan to Track Your Every Move with RFID* (Nelson Current. 2005).

Ellen Alderman & Caroline Kennedy, *In Our Defense: The Bill of Rights in Action* (William Morrow and Company, Inc. 1991).

Ellen Alderman & Caroline Kennedy, *The Right to Privacy* (Knopf Publishing Group. 1995).

Irwin Altman, *The Environment and Social Behavior: Privacy, Personal Space, Territory, Crowding* (Brooks/Cole Publishing Company. 1975).

American Bar Association, *International Guide to Privacy* (Jody R. Westlby ed., Author. 2004).

American Law Institute, *Restatement of the Law, Torts.* (American Law Institute. 1939).

American Law Institute, *Restatement of the Law, Second, Torts* (The American Law Institute. 1977).

Lori Andrews, *Social Networds and the Death of Privacy: I know Who You are and I Saw What You Did* (Free Press. 2011).

[1] Bibliography format is based on the ALWD Citation Manual (4th ed.). Most recent access dates

Ann Cavoukian, et al., *SmartPrivacy for the Smart Grid: Embedding Privacy into the Design of Electricity Conservation* (Information and Privacy Commissioner of Ontario and The Future of Privacy Forum. 2009).

Robert Ardrey, *The Territorial Imperative* (Atheneum. 1966).

Australian Communications and Media Authority, *Privacy Guidelines for Broadcasters* (Australian Communications and Media Authority. 2005).

Australian Government Office of the Privacy Commissioner, *Guidelines on Workplace E-mail, Web Browsing and Privacy* (Australian Government Office of the Privacy Commissioner. 2000).

Australian Office of the Federal Privacy Commission, *Privacy and the Community* (Author. 2001).

Australian Office of the Federal Privacy Commission, *Community Attitudes towards Privacy 2004* (Author. 2004).

Australian Office of the Federal Privacy Commission, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (Author. 2005).

Australian Office of the Federal Privacy Commission, *Community Attitudes towards Privacy 2007* (Author. 2007).

Andre Bacard, *The Computer Privacy Handbook* (Peachpit Press. 1995).

Constance E. Bagley, *Winning Legally: How to Use the Law to Create Value, Marshal Resources, and Manage Risk* (Harvard Business School Press. 2005).

Dennis Bailey, *The Open Society Paradox: Why the 21st Century Calls for More Openess - Not Less* (Brassey's Inc. 2004).

Joel Bakan, *The Corporation: The Pathological Pursuit of Profit and Power* (Free Press. 2004).

Aharon Barak, *Judical Discretion* (Yale University Press. 1987).

Aharon Barak, *Purposive Interpretation in Law* (Princeton University Press. 2005).

Aharon Barak, *The Judge in a Democracy* (Princeton University Press. 2006).

---

are found in the relevant footnote.

Benjamin R. Barber, *Consumed: How Markets Corrupt Children, Infantilize Adults, and Swallow Citizens Whole* (W.W. Norton & Company. 2007).

Randall Bartlett, *Economics and Power: An Inquiry into Human Relations and Markets.* (Cambridge University Press. 1989).

David Beatty, *Talking Heads and the Supremes: The Canadian Production of Constitutional Review* (Carswell. 1990).

Tom L. Beauchamp & James F. Childress, *Principles of Biomedical Ethics (4th ed.)* (Oxford University Press. 1994).

Robert N. Bellah, et al., *Habits of the Heart: Individualism and Commitment in American Life* (University of California Press. 1985).

Thomas Bender, *A Nation among Nations: America's Place in World History* (HIll and Wang. 2006).

Yochai Benkler, *The Wealth of Networks: How Social Productin Transforms Markets and Freedom* (Yale University Press. 2006).

Colin J. Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (Cornell University Press. 1992).

Colin J. Bennett & Rebecca Grant, *Visions of Privacy: Policy Choice for the Digital Age* (University of Toronto Press. 1999).

Colin J. Bennett & Charles D. Raab, *The Governance of Privacy: Policy Instruments in Global Perspective* (Ashgate Publishing Company. 2003).

Jessica W. Berg, et al., *Informed Consent: Legal Theory and Clinical Practice* (Oxford University Press 2nd ed. 2001).

Henri Louis Bergson, *The Two Sources of Morality and Religion* (Doubleday. 1935).

Marver H. Bernstein, *Regulating Business by Independent Commission* (Princeton University Press. 1955).

Huw Beverley-Smith, et al., *Privacy, Property and Personality: Civil Law Perspectives on Commercial Appropriation* (Cambridge University Press. 2005).

Stuart Biegel, *Beyond Our Control? Confronting the Limits of Our Legal System in the Age of Cyberspace* (The MIT Press. 2003).

Ambrose Bierce, *The Collected Writings of Ambrose Bierce* (The Citadel Press 1946).

W.A. Bogart, *Courts and Country: The Limits of Litigation and the Social and Political Life of Canada* (Oxford University Press. 1994).

John C. Bogle, *The Battle for the Soul of Capitalism* (Yale University Press. 2005).

Sissela Bok, *Secrets: On the Ethics of Concealment and Revelation* (Pantheon. 1982).

Lee C. Bollinger, *The Tolerant Society* (Oxford University Press. 1988).

A. Alan Borovoy, *When Freedoms Collide: The Case for Our Civil Liberties* (Lester and Orpen Dennys. 1988).

James Boswell, *The Life of Samuel Johnson, LL.D.* (Henry Baldwin for Charles Dilly. 1791).

James Boyle, *Shamans, Software, & Spleens: Law and the Construction of the Information Society* (Harvard University Press. 1997).

Anne Wells Branscomb, *Who Owns Information? From Privacy to Public Access* (Basic Books. 1994).

Daniel L. Brenner, *Law and Regulation of Common Carriers in the Communications Industry* (Westview Press 2nd ed. 1998).

Stephen G. Breyer, *Regulation and its Reform* (Harvard University Press. 1982).

Stephen G. Breyer, *Breaking the Vicious Circle: Toward Effective Risk Regulation* (Harvard University Press. 1993).

David Brin, *The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?* (Basic Books. 1998).

British Standards Institution, *Code of Practice for Information Security Management.* (British Standards Institution (BS7799). 1995).

Johann Broodryk, *Ubuntu: Life lessons from Africa* (Ubuntu School of Philosophy 2nd ed. 2002).

William Henry Browne, *A Treatise on the Law of Trademarks* (Little, Brown. 1885).

Thomas Buergental, *International Human Rights* (West Publishing. 1995).

David Burnham, *The Rise of the Computer State* (Weidenfeld & Nicolson. 1983).

William C. Burton, *Legal Thesaurus* (Maxwell Macmillan 2nd ed. 1992).

Arthur A. Bushkin, *The Foundations of the United States Information Policy: A United States Government Submission to the High-level Conference on Information, Computer, and Communications Policy* (US Department of Commerce. 1980).

Ian Bushnell, *The Captive Court: A study of the Supreme Court of Canada* (McGill-Queen's University Press. 1992).

Lee A. Bygrave, *Data Protection Law: Approaching its Rationale, Logic and Limits* (P. Bernt Hugenholtz ed., Kluwer Law International. 2002).

Guido Calabresi, *The Costs of Accidents* (Yale University Press. 1970).

James Cannon, *Time and Chance: Gerald Ford's Appointment with History* (Harper Collins. 1994).

Benjamin N. Cardozo, *The Paradoxes of Legal Science* (Greenwood Publishing Group, Incorporated. 1970).

Benjamin N. Cardozo, *The Nature of the Judicial Process* (Yale University Press. 1985).

Timothy P Carney, *The Big Ripoff: How Big Business and Big Government Steal Your Money* (John Wiley & Sons, Inc. 2006).

Manuel Castells, *The Internet Galaxy: Reflections on the Internet, Business, and Society* (Oxford University Press. 2001).

Manuel Castells & Gustavo Cardoso, *The Network Society: From Knowledge to Policy* (Johns Hopkins Center for Transatlantic Relations. 2006).

Fred H Cate, *Privacy in the Information Age* (Brookings Institution Press. 1997).

Edward A. Cavazos & Gavino Morin, *Cyber Space and the Law, Your Rights and Duties in the On-line World (4th ed.)* (The MIT Press. 1996).

Ann Cavoukian & Claudiu Popa, *Privacy by ReDesign: A Practical Framework for Implementation* (Information & Privacy Commissioner Ontario. 2011).

Ann Cavoukian & Tyler J. Hamilton, *The Privacy Payoff: How Successful Businesses Build Customer Trust* (McGraw-hill Ryerson Ltd. 2002).

Ann Cavoukian & Don Tapscott, *Who Knows: Safeguarding your Privacy in a*

Networked World (Random House of Canada. 1995).

Zechariah Chafee, *Free Speech in the United States* (Harvard University Press. 1941).

Michael E. Chesbro, *Privacy for Sale: How Big Brother and Others are Selling Your Private Secrets for Profit* (Paladin Press. 1999).

Frank Church, *Senate Select Committee to Study Government Operations with Respect to Intelligence*

Activities, 94th Congress, Final Report on Intelligence Activities and the Rights of Americans (United State Printing Office. 1976, April 26).

Andrew Clapham, *Human Rights in the Private Sphere* (Clarendon Press. 2002).

Barkley Clark & Christopher Smith, *The Law of Product Warranties* (Warren Gorham & Lamont. 1994).

Richard Clayton & Hugh Tomlinson, *Privacy and Freedom of Expression* (Oxford University Press. 2001).

Jeffrey D. Clements, *Corporations Are Not People: Why They Have More Rights Than You and What You Can Do About it* (Berrett-Koehler Publishers, Inc. 2012).

Jean L. Cohen, *Regulating Intimacy: A New Legal Paradigm* (Princeton University Press. 2002).

David Cole & James X. Dempsey, *Terrorism and the Constitution: Sacrificing Civil Liberties in the Name of National Security* (The New Press 2nd ed. 2002).

Madeleine Colvin, *Developing Key Privacy Rights* (Hart Publishing. 2002).

Australian Law Reform Commission, *Australian Privacy Law and Practice* (Commonwealth of Australia. 2008).

New South Wales Law Reform Commission, *Privacy Principles: Report 123* (New South Wales Law Reform Commission. 2009, August).

Commission on Risk Assessment and Risk Management, *Risk Assessment and Risk Management in Regulatory Decision-Making: Final Report (Volume 2)* (Government Printing Office. 1997).

Communications Canada, *Telecommunications Privacy Principles* (Supply and

Services Canada. 1992).

Thomas Mcintyre Cooley, *Treatise of the Law of Torts: Or the Wrongs Which Arise Independent of Contract* (Callaghan. 1888).

Thomas Mcintrye Cooley, *A Treatise on the Law of Torts or the Wrongs Which Arise Independently of Contract* (Callaghan & Company 3rd ed. 1906).

Coopers & Lybrand Deloitte in Association with Cameron Markby Hewitt, *Dealing with Computer Misuse: Review of the Application of the Computer Misuse Act and the Associated Market for Information and Expert Advice* (Report Prepared for the Commercial IT Security Group, IT Division, Department of Trade and Industry. n.d.).

Lewis Corey, *The House of Morgan: A Social Biography of the Maters of Money* (G. Howard Watt. 1930).

Vita Cornelius, *Personal Privacy* (Novinka Books. 2002).

Terence Craig & Mary E. Ludloff, *Privacy and Big Data* (O'Reilly Media, Inc. 2011).

Samuel Dash, *The Intruders: Unreasonable Searches and Seizures from King John to Jophn Ashcroft* (Rutgers University Press. 2004).

John W. Dean, *The Rehnquist Choice: The Untold Story of the Nixon Appointment that Redefined the Supreme Court.* (The Free Press 2001).

John W. Dean, *Broken Government: How Republican Rule Destroyed the Legislative, Executive, and Judicial Branches* (Viking. 2007).

Judith Wagner Decew, *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology* (Cornell University Press. 1997).

Jacques Delarue, *The Gestapo: A History of Horror* (Mervyn Savill trans., Frontline Books. 2008).

Maurizio Passerin D'entreves & Ursula Vogel, *Public & Private: Legal. Political, and Philosophical Perspectives* (Routledge. 2000).

Lothar Determan, *Determann's Field Guide to International Data Privacy Law Compliance* (Edward Elgar. 2012).

Whitfield Diffie & Susan Landau, *Privacy on the Line: The Politics of Wiretapping and Encryption* (The MIT Press. 1998).

Association of Legal Writing Directors & Darby Dickerson, *ALWD Citation Manual: A Professional System of Citation* (Aspen Publishers 4th ed. 2010).

Byron L Dorgan, *Take this Job and Ship It: How Corporate Greed and Brain-Dead Politics are Selling out America* (Thomas Dunne Books / St. Martin Press. 2006).

James A. Douglas & Laurel Binder-Arain, *Computer and Information Law Digest* (Warren, Gorham & Lamont. 1994).

Dianne Louise Draper & Maureen G. Reed, *Our Environment: A Canadian Perspective* (Thompson Nelson. 2006).

Susan J. Drucker & Gary Gumpert, *Real Law @ Virtual Space: Regulation in Cybersapce* (Susan J. Drucker & Gary Gumpert eds., Hampton Press, Inc.).

Lee Drutman & Charlie Cray, *The People's Business: Controlling Corporations and Restoring Democracy* (Berrett-Koehler Publishers, Inc. 2004).

Gordon E. Duinker & Peter N. Beanlands, *An Ecological Framework for Environmental Impact Assessment in Canada* (Institute for Environmental Systems, Dalhousie University. 1983).

Daphine A. Dukelow & Betsy Nuse, *The Dictionary of Canadian Law* (Carswell 2 ed. 1995).

George T. Duncan, et al., *Private Lives and Public Policies: Confidentiality and Accessibility of Government Statistics* (National Academy Press. 1993).

Julian Dunster & Katherine Dunster, *Dictionary of Natural Resource Management* (University of British Columbia Press. 1996).

Soumitra Dutta & Irene Mia, *The Global Information Technology Report 2010–2011: Transformations 2.0* (World Economic Forum. 2011).

Terry Eastland, *BenchMarks: Great Constitutional Controversies in the Supreme Court* (Ethcis and Public Polcy Center and William B. Eerdmans Publishing Company. 1995).

John Ehrlichman, *Witness to Power: The Nixon Years* (Simon & Schuster. 1982).

Dwight D. Eisenhower, *Public Papers of the Presidents* (Government Printing Office. 1960).

Dwight D. Eisenhower, *Military-Industrial Complex Speech. Public Papers of the Presidents, Dwight D. Eisenhower (pp. 1035-1040)* (Government Printing Office. 1961).

Ekos Research Associates, *Privacy Revealed: The Canadian Privacy Survey* (Ekos Research Associates. 1993).

Electronic Privacy Information Center, *Surfer Beware: Personal Privacy and the Internet* (Author. 1997).

Electronic Privacy Information Center, *Privacy & Human Rights: An International Survey of Privacy Laws and Developments* (Author. 1999-2006).

Robert C. Ellickson, *Order Without Law: How Neighbors Settle Disputes.* (Harvard University Press. 1991).

Environment Canada, *Review and Evaluation of Adaptive Environmental Management* (University of British Columbia Press. 1982).

Michael Erbschloe & John Vacca, *Net Privacy: A Guide to Developing and Implementing an Ironclad ebusiness Privacy Plan* (McGraw-Hill. 2001).

Amitai Etzioni, *The Limits of Privacy* (Basic Books. 1999).

European Parliament, *Assessing the Technologies of Political Control. European Parliament Civil Liberties Committee and undertaken by the European Commission's Science and Technology Options Assessment office* (Author. 1997).

Executive Office of the President - Office of Science and Technology, *Privacy and Behavioral Research* (Government Printing Office. 1967).

Ruth Faden & Tom L Beauchamp, *A History and Theory of Informed Consent* (Oxford University Press. 1986).

Silvana Faja, *Influence of the Web Vendor's Level of Intervention with Regard to Privacy on Behavioral Intention in E-Commerce* § Ph.D. (University of Nebraska. 2004).

Greg Farrell, *Corporate Crooks: How Rogue Executives Ripped Off Americans .... and Congress Helped Them Do It!* (Prometheus Books. 2006).

Federation Nationale Des Associations De Consommateurs Du Quebec/Public Interest Advocacy Centre, *Surveying Boundaries: Canadians and their Personal Information* (Author. 1995).

Jay M. Feinman, *Un-Making Law: The Conservative Campaign to Roll Back the Common Law* (Beacon Press. 2004).

David H. Flaherty, *Privacy in Colonial New England* (University of Virginia Press. 1972).

David H. Flaherty, *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States* (University of North Carolina Press. 1989).

Nancy Flynn, *The Social Media Handbook: Policies and Best Practices to Effectively Manage your Organization's Social Media Presence, Posts, and Potential Risks* (Pfeiffer. 2012).

Herbert N. Foerstel, *Freedom of Information and the Right to Know: The Origins and Applications of the Freedom of Information Act* (Greenwood Press. 1999).

Ralph H. Folsom, *European Union Law* (West Publishing. 1995).

Andrew Frackman, et al., *Internet and Online Privacy: A Legal and Business Guide* (ALM Publishing. 2002).

Jerome Frank, *Courts on Trial: Myth and Reality in American Justice* (Princeton University Press. 1949).

Benjamin Franklin, *Pennsylvania Assembly: Reply to the Governor; Votes and Proceedings of the House of Representatives, 1755-1756* (Pennsylvania Assembly. 1756).

Franks Committee, *Report of the Committee on Administrative Tribunals and Enquiries* (H. M. Stationery Office 1957).

William C. Frederick, *Corporation be Good: The Story of Corporate Social Responsibility* (Dog Ear Publishing, LLC. 2006).

David D. Friedman, *Future Imperfect: Technology and Freedom in an Uncertain World* (Cambridge University Press. 2008).

Lawrence M. Friedman, *Total Justice* (Beacon Press. 1985).

Lawrence M. Friedman, *The Republic of Choice: Law, Authority, and Culture* (Harvard University Press. 1990).

Lawrence M. Friedman, *The Horizontal Society* (Yale University Press. 1999).

Lawrence M. Friedman, *Guarding Life's Dark Secrets: Legal and Social Controls over Reputation, Propriety, and Privacy* (Stanford University Press. 2007).

Milton Friedman, *Capitalism and Freedom* (University of Chicago Press. 1962).

Eric Fromm, *Escape from Freedom* (Holt, Rinehart & Winston, Inc. 1941).

Lon L. Fuller, *The Morality of Law* (Yale University Press Rev. ed. 1997).

James K. Galbraith, *The Predator State: How Conservatives Abandoned the Free Market and Why Liberals Should Too* (Free Press. 2008).

Oscar H. Gandy, *The Panoptic Sort: A Political Economy of Personal Information* (Westview Press. 1993).

Martin Garbus, *Courting Disaster: The Supreme Court and the Unmaking of American Law* (Henry Holt and Company. 2002).

Simson Garfinkel, *Database Nation: The Death of Privacy in the 21st Century* (O'Reilly. 2000).

Michael Geist, *Internet Law in Canada* (Captus Press 3rd. ed. 2002).

Robert Gellman & Pam Dixon, *Online Privacy* (Contemporary World Issues, ABC-CLIO. 2011).

Robert B. Gelman & Stanton Mccandlish, *Protecting Yourself Online* (HarperEdge. 1998).

Curt Gentry, *J. Edgar Hoover: The Man and the Secrets* (W. W. Norton & Company. 1991).

Mary Ann Glendon, *Right Talk: The Impoverishment of Political Discourse* (Free Press. 1991).

Mike Godwin, *Cyber Rights: Defending Free Speech in the Digital Age* (Times Books. 1998).

Mike Godwin, *Cyber Rights: Defending Free Speech in the Digital Age* (The MIT Press Rev. ed. ed. 2003).

Jack Goldsmith & T. Wu, *Who Controls the Internet? Illusions of a Borderless World* (Oxford University Press. 2006).

Australian Government, *Issues Paper: A Commonwealth Statutory Cause of Action for Serious Invasion of Privacy* (Australian Government 2011 September).

Gale L. Gran, *Understanding Digital Signatures: Establishing Trust Over the Internet and Other Networks* (Mc-Graw-Hill. 2009).

Mark Green, *Losing Our Democracy: How Bush, the Far Right and Big Business are Betraying Americans for Power and Profit* (Sourcebooks, Inc. 2006).

Andy Greenberg, *This Machine Kills Secrets: How Wikileakers.Cyberpunkis, and Hactivists Aim to Free the World's Information.* (Dutton. 2012).

Jan Crawford Greenburg, *Supreme Court: The Inside Story of the Struggle For Control of the United States Supreme Court* (The Penguin Press. 2007).

Davydd J. Greenwood & Morten Levin, *Introduction to Action Research: Social Research for Social Change* (Sage. 1998).

Wendy M. Grossman, *Net.wars* (New York University Press. 1997).

Laura J. Gurak, *Persuasion and Privacy in Cyberspace: The Online Protests over Lotus Marketplace and the Clipper Chip* (Yale University Press. 1997).

Kermit L Hall, *The Magic Mirror: Law in American history* (Oxford University Press. 1989).

Kermit L Hall, *The Oxford Companion to the Supreme Court of the United States* (Oxford University Press. 1992).

Kermit L Hall, *The Oxford Companion to the Supreme Court of the United States* (Oxford University Press 2nd. ed. 2005).

Cees J. Hamelink, *The Ethics of Cyberspace* (Sage. 2000).

Alexander Hamilton, et al., *The Federalist Papers* (Benjamin Fletcher Wright ed., Metro Books. 1787/1961).

Olivier Hance & Suzanne Dionne Balz, *Business and Law on the Internet.* (The Best of McGraw Hill. 1966).

Valerie P. Hans, *Business on Trial: The Civil Jury and Corporate Responsibility* (Yale University Press. 2000).

Harris Interactive, *Privacy On and Off the Internet: What Consumers Want (Study No. 15229)* (Author. 2002).

Louis Harris & Allen F. Westin, *The Dimensions of Privacy* (Sentry Insurance. 1979).

Lesley Ellen Harris, *Digital Property: Currency of the 21st Century* (McGraw-Hill Ryerson. 1998).

Richard A. Harris & Sidney M. Milkis, *The Politics of Regulatory Change: A Tale of Two Agencies* (Oxford University Press 2nd ed. 1996).

Thom Hartmann, *Unequal Protection: The Rise of Corporate Dominance and the Theft of Human Rights* (Rodale. 2002).

Louis Hartz, *The Liberal Tradition in America: An Interpretation of American Political Thought Since the Revolution* (Harcourt Brace Jovanovich, Publishers. 1955).

Harvard Law Review Association, *The BlueBook: A Uniform System of Citation* (The Harvard Law Review Association 18th ed. 2005).

David E Hawkins, *Corporate Social Responsibility: Balancing Tomorrow's Sustainability and Today's Profitability* (Palgrave Macmillan. 2006).

Friedrich A. Hayek, *The Constitution of Liberty* (The University of Chicago Press. 1960).

Health and Human Services, *Toward a National Health Information Infrastructure, Report to the Secretary, US Department of Health and Human Services, Workgroup on Computerization of Patient Records* (Author. 1993).

Dorothee Heisenberg, *Negotiating Privacy: The European Union, the United States, and Personal Data Protection* (Lynne Rienner Publishers. 2005).

Harry Henderson, *Privacy in the Information Age* (Facts on File Rev. ed. 2006).

Janine S. Hiller & Ronnie Cohen, *Internet Law & Policy* (Prentice Hall. 2002).

Christopher Hodder-Williams, *Fistful of Digits* (Hodder and Stoughton, Ltd. 1972).

Eric Hoffer, *The True Believer: Thoughts on the Nature of Mass Movements* (HarperCollins Publishers Rev. ed. 2002).

C. S. Holling, *Adaptive Environmental Assessment and Management* (John Wiley and Sons. 1978).

Oliver Wendell Holmes, *The Common Law* (Dover Publications 1881/1991).

Oliver Wendell Holmes, *Collected Legal Papers* (Harcourt Brace and Company. 1920).

David H. Holtzman, *Privacy Lost: How Technology is Endangering your Privacy* (Jossey-Bass. 2006).

House Committee on Government Operations, *Who Cares About privacy? Congressional Report Number 455 of the 98th Congress* (Government Printing Office. 1983).

Peter Huber, *Law and Disorder in Cyberspace: Abolish the FCC and Let Common Law Rule the Telecom.* (Oxford. 1997).

Arianna Huffington, *Pigs at the Trough: How Corporate Greed and Political Corruption are Undermining America* (Crown Publishing Group. 2004).

Elaine L. Hughes, et al., *Environmental Law and Policy* (Emond Montgomery 3rd ed. 2003).

Wilson Huhn, *The Five Types of Legal Argument* (Carolina Academic Press. 2002).

Will Hutton, *A Declaration of Interdependence: Why America Should Join the World* (W. W. Norton & Company, Inc. 2003).

Aldous Huxley, *Brave New World* (Harper & Brothers. 1946).

Michael S. Hyatt, *Invasion of Privacy: How to Protect Yourself in the Digital Age* (Regnery Publishing, Inc. 2001).

Industry Canada, *Privacy and the Information Highway Regulatory Options for Canada* (Author. 1996).

Information and Privacy Commissioner/Ontario, *Eyes on the Road: Intelligent Transportation Systems and Your Privacy* (Author. 1995).

Information Canada, *Privacy and Computers (A Report of a Task Force Established Jointly by Department of Communications/Department of Justice)* (Author. 1972).

Information Commissioner's Office, *Personal Information Online: Code of Practice* (Author. 2010).

Information Highway Advisory Council (Ihac), *Connection, Community, and*

Content: the Challenge of the Information Highway (Minister of Supply and Services Canada. 1995).

John Inness & Gweneth Norris, *Corporate Social Responsibility: A Case Study Guide for Management Accountants* (Elsevier Limited. 2005).

Julie C. Inness, *Privacy, Intimacy and Isolation* (Oxford University Press. 1992).

Stephen Isacc & William B. Michael, *Handbook in Research and Evaluation: A Collection of Principles, Methods, and Strategies Useful in the Planning, Design, and Evaluation of Studies in Education and the Behavioral Sciences* (Edits/ Educational and Industrial Testing Services 3rd ed. 1995).

Ravi K. Jain, et al., *Environmental Assessment* (McGraw-Hill 2nd ed. 1993).

Daniel S. Janal, *Risky Business: Protect Your Business from Being Stalked, Conned, or Blackmailed on the Web* (John Wiley & Sons, Inc. 1998).

Irving L. Janis, *Psychological Stress: Psychoanalytic and Behavioral Studies of Surgical Patients* (Wiley and Sons. 1958).

Marianne M. Jennings, *The Seven Signs of Ethical Collapse: How to Spot Moral Meltdowns in Companies ... Before It's Too Late* (St. Martin's Press. 2006).

Matthew Josephson, *The Robber Barons: The Great American Capitalists, 1861-1901* (Harcourt, Brace & World. 1962).

John J. Trinckes Jr, *The Definitive Guide to Complying with the HIPAA/HITECH Privacy and Security Rules* (CRC Press. 2013).

Vine Deloria Jr. & David E. Wilkins, *The Legal Universe: Observations on the Foundation of American Law* (Fulcrum Publishing. 2011).

Brian Kahin & Charles Nesson, *Borders in Cyberspace: Information Policy and the Global Information Infrastructure.* (The MIT Press. 1999).

David Kahn, *The Codebreakers: The Story of Secret Writing* (Scribner 2nd ed. 1996).

Robert G. Kaiser, *So Damn Much Money: The Triumph of Lobbying and the Corrosion of American Government* (Alfred A. Knopf. 2009).

Andrew Kakabadse & Mette Morsing, *Corporate Social Responsibility: A 21st*

Century Perspective (Palgrave Macmillan. 2006).

Cem Kaner & David Pels, *Bad Software: What to Do When Software Fails* (John Wiley & Sons. 1998).

Immanuel Kant, *Groundwork of the Metaphysics of Morals* (Mary Gregor trans., Cambridge University Press (1998). 1785).

Immanuel Kant, *The Metaphysics of Morals. (Originally published in two parts in 1797 as the Doctrine of right and the Doctrine of virtue)* (Mary Gregor trans., Cambridge University Press. 1797/1996).

Immanuel Kant, *Ethical Duties Toward Others: Truthfulness* (Louis Infield trans., Hackett Publishing Company. 1930).

Ethan M. Katsh, *The Electronic Media and the Transformation of Law* (Oxford University Press. 1989).

M. Ethan Katsh, *Law in a Digital World* (Oxford University Press. 1995).

Kevin M. Keenan, *Invasion of Privacy: A Reference Handbook* (ABC CLIO. 2005).

W. Page Keeton, et al., *Posser and Keeton on the Law of Torts* (West Publishing. 1984).

Mark S. Kende, *Constitutional Rights in Two Worlds: South Africa and the United States* (Cambridge University Press. 2009).

Joseph Migga Kizza, *Civilizing the Internet: Global Concerns and Efforts Toward Regulation* (McFarland & Company, Inc. 1998).

Rainer Knopff & F. L. Morton, *Charter Politics* (Nelson. 1992).

Philip Kotler & Nancy Lee, *Corporate social responsibility: Doing the most good for your company and your cause* (John Wiley & Sons. 2004).

Herbert M. Kritzer, *The English Experience with the English Rule: How 'Loser Pays' Works, What Difference It Makes, and What Might Happen Here* (University of Wisconsin, Institute for Legal Studies. 1992).

Paul R. Krugman, *The Great Unraveling: Losing Our Way in the New Century* (W. W. Norton & Company. 2003).

Christopher Kuner, *European Data Privacy Law and Online Business* (Oxford University Press. 2003).

Susan Landau, *Surveillance or Security? The Risks Posed by New Wiretapping Technologies* (The MIT Press. 2010).

Carole A. Lane, *Naked in Cyberspace: How to Find Personal Information Online* (Pemberton Press. 1997).

Frederick S. Lane Iii, *The Naked Employee: How Technology is Compromising Workplace Privacy* (American Management Association. 2003).

Cynthia J. Larose, et al., *State Data Breach Notification Laws* (Acc: Association of Corporate Counsel. 2011).

Pierre Larouche, *Competition Law and Regulation in European Telecommunications* (Hart Publishing. 2000).

Erik Larson, *The Naked Consumer: How Our Private Lives Become Public Commodities* (Henrey Holt and Company. 1992).

Norman Lee & Clive George, *Environmental Assessment in Developing and Transitional Countries* (John Wiley and Sons Ltd. 2000).

Orlan Lee, *Waiving Our Rights: The Personal Data Collection Complex and its Threat to Privacy and Civil Liberties* (Lexington Books. 2012).

Lawrence Lessig, *Code and Other Laws of Cyberspace* (Basic Books. 1999).

Lawrence Lessig, *Te Future of Idea: The Fate of the Commons in a Connected World* (Random House. 2001).

Lawrence Lessig, *Free Culture How Big Media Uses Technology and the Law to Lock Down Culture and Control Creativity* (The Penguin Press. 2004).

Lawrence Lessig, *Code: Version 2.0* (Basic Books. 2006).

Lawrence Lessig, *Republic, Lost: How Money Corrupts Congress - and a Plan to Stop It* (Twelve - Hachette Hook Group. 2011).

Leonard W. Levy, *Origins of the Bill of Rights* (Yale Nota Bene. 2001).

Joyce H-S Li, *The Center for Democracy and Technology and Internet Privacy in the U.S.: Lessons of the Last Five Years* (The Scarecrow Press, Inc. 2003).

David F. Linowes, *Privacy in America: Is Your Private Life in the Public Eye?* (University of Illinois Press. 1989).

Seymour Martin Lipset, *Continental Divide: The Values and Institutions of the*

United States and Canada (C.D. Howe Institute. 1989).

Karl N. Llewellyn, et al., *The Case Law System in America* (The University of Chicago Press. 1990).

Ian J. Lloyd, *A Guide to the Data Protection Act of 1998* (Butterworths. 1998).

Ian J. Lloyd, *Legal Aspects of the Information Society* (Butterworths. 2000).

Ian J. Lloyd, *Information Technology Law* (Oxford University Press 5th. ed. 2008).

Ian J. Lloyd & Moria Simpson, *Law on the Electronic Frontier* (The David Hume Institute, Edinburgh University Press. 1997).

David Lyon, *Surveillance Society: Monitoring Everyday Life* (Open University. 2001).

Rebecca Mackinnon, *Consent of the Networked: The Worldwide Struggle for Internet Freedom* (Basic Books. 2012).

Wayne Madsen, *Handbook of Personal Data Protection* (Stockton Press; Macmillian Publishers, Ltd. 1992).

Patrick Malcolmson & Richard Myers, *The Canadian Regime: An Introduction to Parliamentary Government in Canada* (University of Toronto 3rd ed. 2005).

Carolyn Marvin, *When Old Technologies Were New: Thinking About Electric Communication in the Late Eighteenth Century* (Oxford University Press. 1988).

Abraham H. Maslow, *Toward a Psychology of Being* (John Wiley & Sons 3rd ed. 1999).

Tim Mather, et al., *Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance* (O'Reilly Media, Inc. 2009).

Robert May, *Guidelines 2000: Scientific Advice and Policy Making* (UK Office of Science and Technology. 2000).

Jane Mayer, *The Dark Side: The Inside Story of How the War on Terror Turned into a War on American Ideals.* (Doubleday. 2008).

Viktor Mayer-Schonberger & Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think* (An Eamon Bolan

Book/Houghton Mifflin Harcourt ed. 2013).

Marshall Mcluhan, *The Gutenberg Galaxy: The Making of Typographic Man* (University of Toronto Press. 1962).

Arthur R. Miller, *The Assault on Privacy: Computer Data Banks and Dossiers* (University of Michigan Press. 1971).

Frederic P. Miller, et al., *Japanese Canadian Internment: World War II, Empire of Japan, Pearl Harbor, Brian Mulroney, Japanese American internment, Ukrainian Canadian internment, ... run internment camps during World War II* (Alphascript Publishing. 2009).

Richard Lawrence Miller, *Nazi Justice: Law of the Holocaust* (Praeger. 1995).

Steven E. Miller, *Civilizing Cyberspace: Policy, Power, and the Information Superhighway* (ACM Press. 1995).

Mark Minasi, *The Software Conspiracy: Why Companies Put Out Faulty Software, How They Can Hurt You and What You Can Do About It* (McGraw Hill. 1999).

Barry Minkow, *Cleaning Up: One Man's Redemptive Journey Through the Seductive World of Corporate Crime* (Thomas Nelson. 2005).

Prasad Modak & Asit K Biswas, *Conducting Environmental Impact Assessment in Developing Countries* (United Nations University Press. 1999).

Barrington Moore, Jr, *Privacy: Studies in Social and Cultural History* (M.E. Sharpe, Incorporated. 1984).

Evgeny Morozov, *The Net Delusion: The Dark Side of Internet Freedom* (PublicAffairs ed. 2011).

Evgeny Morozov, *To Save Everything, Click Here: The Folly of Technological Solutionism* (PublicAffairs ed. 2013).

Milton L. Mueller, *Ruling the Root: Internet Governance and the Taming of Cyberspace* (The MIT Press. 2002).

Ingo Müller, *Hitler's Justice: The Courts of the Third Reich* (Deborah Lucas Schneider trans., Harvard University Press. 1991).

Robert Edward Munn, *Environmental Impact Assessment: Principles and Procedures: Scope Report 5* (United Nations Environment Program;

Environment Canada; United Nations Educational, Scientific and Cultural Organization. 1985).

Bruce Allen Murphy, *Fortas: The Rise and Ruin of a Supreme Court Justice* (William Morrow. 1988).

John Naisbitt, *Megatrends - Ten New Directions Transforming Our Lives* (Warner Books. 1982).

National Commission on Terrorist Attacks Upon the United States, *Final Report of the National Commission on Terrorist Attacks upon the United States, the 9/11 Commission Report 394 (Authorized 1st ed.)* (Government Printing Office. 2004).

National Council for Science and the Environment (Ncse), *Recommendations for Improving the Scientific Basis for Environmental Decision-Making — A Report from the First National Conference on Science, Policy, and the Environment* (National Academy of Sciences. 2000).

National Research Council, *Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Assessment* (Committee on Technical and Privacy Dimensions of Information for Terrorism Prevention and Other National Goals. 2008).

J Neethling, et al., *Neethling's Law of Personality* (Butterworths. 1996).

J Neethling, et al., *Neethling's Law of Personality* (LexisNexis 2nd ed. 2005).

Peter G. Neuman, *Computer Related Risks* (Addison-Wesley Publishing Company. 1995).

Abraham L. Newman, *Protectors of Privacy: Regulating Personal Data in the Global Economy* (Cornell University Press. 2008).

Daniel Neyland, *Privacy, Surveillance and Public Trust* (Palgrave Macmillan. 2006).

Raymond T. Nimmer, *Information Law* (Warren, Gorham & Lamond. 1966).

Stephen L. Nock, *The Cost of Privacy, Surveillance and Reputation in America* (Transaction Publishers. 1993).

David M. O'Brien, *Privacy, Law, and Public Policy* (Praeger. 1979).

Information Commissioner’s Office, *Personal Information Online: Code of*

Practice (Author. 2010).

Office of Technology Assessment (Ota), *The Electronic Supervisor: New Technology, New Tensions* (U.S. Government Printing Office. 1987).

Office of Technology Assessment (Ota), *Protecting Privacy in Computerized Medical Information* (U.S. Government Printing Office. 1993).

Office of the Federal Privacy Commissioner, *Privacy and Public Key Infrastructure: Guidelines for Agencies Using PKI to Communicate or Transact With Individuals* (Office of the Federal Privacy Commissioner. 2001).

Office of the Privacy Commissioner, *SPAM Act 2003 Review* (Office of the Privacy Commissioner. 2006).

Robert O'harrow, *No Place to Hide* (Free Press. 2006).

John V. Orth, *Due Process of Law: A Brief History* (University Press of Kansas. 2003).

John V. Orth, *How Many Judges Does It Take To Make A Supreme Court? And Other Essays on Law and the Constitution* (University Press of Kansas. 2006).

George Orwell, *Nineteen Eighty-Four* (Harcourt, Brace. 1949).

David Osborne & Ted Gaebler, *Reinventing Government* (Plume. 1992).

Thomas Paine, *Common Sense* (Author. 1776, February 14).

John Palfrey & Urs Gasser, *Interop: The Promise and Perils of Highly Interconnected Systems* (Basic Books. 2012).

Christian Parenti, *The Soft Cage: Surveillance in America from Slavery to the War on Terror* (Basic Books. 2003).

Donn B. Parker, *Fighting Computer Crime: A New Framework for Protecting Information* (John Wiley & Sons. 1998).

Nikos Passas & Neva R. Goodwin, *It's Legal but It Ain't Right: Harmful Social Consequences of Legal Industries* (University of Michigan Press. 2004).

Michael Quinn Patton, *Qualitative Research & Evaluation Methods* (Sage 3rd ed. 2001).

Michael Perelman, *Manufacturing Discontent: The Trap of Individualism in*

Corporate Society (Pluto Press. 2005).

William Peterson, *Japanese Americans: Oppression and Success* (Random House 1st ed. 1971).

Ithiel De Sola Pool, *Technologies of Freedom: On Free Speech in an Electronic Age* (Harvard University Press. 1983).

Karl R Popper, *The Open Society and its Enemies: The Spell of Plato* (Harper & Row, Publishers. 1962a).

Karl R. Popper, *The Open Society and its Enemies: The High Tide of Prophecy: Hegel, Marx, and the Aftermath* (Harper & Row, Publishers. 1962b).

Richard A. Posner, *The Right to Privacy* (University of Chicago, Center for Study of the Economy and the State. 1978).

Richard A. Posner, *How Judges Think* (Harvard University Press. 2008).

Virginia Postrel, *The Future and its Enemies: The Growing Conflict Over Creativity, Enterprise, and Progress* (The Free Press. 1998).

Lucas A. Powe Jr, *American Broadcasting and the First Amendment* (University of California Press. 1987).

A. Paul Pross, *Group Politics and Public Policy* (Oxford University Press 2nd ed. 1992).

Alan Charles Raul, *Privacy and the Digital State: Balancing Public Information and Personal Privacy* (Kluwer Academic Publishers. 2002).

Diane Ravitch, *The Language Police: How Pressure Groups Restrict What Students Learn* (Alfred A. Knopf. 2003).

John Rawls, *A Theory of Justice* (The Belknap Press of Harvard University Press rev. ed. 1999).

Pricilla M. Regan, *Legislating Privacy: Technology, Social Values, and Public Policy* (University of North Carolina Press. 1995).

Social and Market Strategic Research, *Report on Information Commissioner's Office Annual Track* (Author. 2006).

Social and Market Strategic Research, *Report on Information Commissioner's Office Annual Track* (Author. 2008).

Alasdair Roberts, *Blacked Out: Government Secrecy in the Information Age*

(Cambridge University Press. 2006).

Neil Robinson, et al., *Review of the European Data Protection Directive* (Rand Europe. 2009).

Colin Robson, *Real World Research: A Resource for Social Scientists and Practitioner-Researchers* (Blackwell 2nd ed. 2002).

Anneliese Roos, *The Law of Data (Privacy) Protection: A Comparative and Theoretical Study* § LL.D. ((LL.D. thesis, UNISA. 2003).

Lance Rose, *Netlaw: Your Rights in the Online World* (Osborne McGraw-Hill. 1995).

Jeffrey Rosen, *The Unwanted Gaze: The Destruction of Privacy in America* (Random House. 2000).

Jeffrey Rosen, *The Naked Crowd: Reclaiming Security and Freedom in an Anxious Age* (Random House. 2004).

Jeffrey Rosen, *The Supreme Court: The Personalities and Rivalries that Defined America* (Times Books Henry Holt and Company. 2006).

Jeffrey Rosen & Benjamin Wittes, *Constitution 3.0: Freedom and Technological Change* (eds., Brookings Institution Press. 2011).

Sheera Rosenfeld, et al., *Privacy, Security, and the Regional Health Information Organization* (California Health Care Foundation. 2007).

Jonathan Rosenoer, *CyberLaw: The Law of the Internet* (Springer. 1997).

Beate Rössler, *The Value of Privacy* (R. D. V. Glasgow trans., Polity Press. 2005).

David Rothkopf, *Power, Inc.: The Epic Rivalry Between Big Business and Government - The Reckoning That Lies Ahead,* (Farrar, Straus and Giroux. 2012).

Wade Rowland, *Greed, Inc: Why Corporations Rule Our World* (Arcade Publishing. 2006).

Doris Rubenstein, *The Good Corporate Citizen: A Practical Guide* (John Wiley & Sons. 2004).

James B. Rule, *Private Lives and Public Surveillance: Social Control in the Computer Age* (Schocken Books. 1974).

James B. Rule, *Privacy in Peril: How We Are Sacrificing a Fundamental Right in Exchange for Security and Convenience* (Oxford University Press. 2007).

James B. Rule, et al., *The Politics of Privacy: Planning for Personal Data Systems as Powerful Technologies* (Elsevier. 1980).

Michael Salter & Julie Mason, *Writing Law Dissertations: An Introduction and Guide to the Conduct of Legal Research* (Pearson Longman. 2007).

Dianne Saxe, *Environmental Offences: Corporate Responsibility and Executive Liability* (Canada Law Book. 1990).

Elaine Scarry, *Rule of Law, Misrule of Men* (A Boston Review Book, The MIT Press. 2010).

Elaine Scarry, *Thinking in an Emergency* (W.W. Norton & Company, Inc. 2011).

Madeleine Schachter, *Informational and Decisional Privacy* (Carolina Academe Press. 2003).

Bruce Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C* (John Wiley & Sons, Inc. 1994).

Bruce Schneier, *Secrets and Lies: Digital Security in a Networked World* (John Wiley & Sons, Inc. 2000).

Bruce Schneier & David Banisar, *The Electronic Privacy Papers: Documents on the Battle for Privacy in the Age of Surveillance* (Wiley. 1997).

Ferdinand David Schoeman, *Privacy and Social Freedom* (Cambridge University Press. 2008).

Stephen J. Schulhofer, *Rethinking the Patriot Act: Keeping America Safe and Free* (The Century Foundation. 2005).

Stephen J. Schulhofer, *More essential Than Ever: The Fourth Amendment in the Twenty-First Century* (Oxford University Press. 2012).

David Sciulli, *Corporate Power in Civil Society: An Application of Societal Constitutionalism* (New York University Press. 2001).

Stefano Scoglio, *Transforming Privacy: A Transpersonal Philosophy of Rights* (Praeger. 1998).

Gini Graham Scott, *The Death of Privacy: The Battle for Personal Privacy in the Courts, The Media, and Society* (Changemakers Publishing and Writing.

2011).

Scottish Law Commission, *Report on Computer Crime. (Scottish Law Commission, No 106)* (H.M.S.O. 1987).

Senate Judiciary Committee Hearing, *Nomination of William H. Rehnquist and Lewis F. Powell, Jr (291).* (Washington, DC: U.S. Government Printing Office. 1971).

Andrew L. Shapiro, *The Control Revolution: How the Internet is Putting Individuals in Charge and Changing the World We Know* (A Century Foundation Book. 1999).

Martin Shapiro, *Courts: A Comparative and Political Analysis.* (The University of Chicago Press. 1986).

Ibrahim F I Shihata, *Complementary Reform: Essays on Legal, Judicial and Other Institutional Reforms Supported by the World Bank* (Kluwer Law International. 1997).

David K. Shipler, *The Rights of the People: How our Search for Safety Invades our Liberties* (Alfred A. Knopf. 2011).

David K. Shipler, *Rights at Risk: The Limits of Liberty in Modern America* (Alfred A. Knopf. 2012).

Robert Shogan, *A Question of Judgment: The Fortas Case and the Struggle for the Supreme Court* (The Bobbs Merrill Company. 1972).

Adam Shostack & Andrew Strewart, *The New School of Information Security* (Addison-Wesley. 2008).

J. Gregory Sidak & Daniel F. Spulber, *Deregulatory Talkings and the Regulatory Contract: The Competitive Transformation of Network Industries in the United States.* (Oxford University Press. 1998).

David Sirota, *Hostile Takeover: How Big Money and Corruption Conquered Our Government--And How We Take It Back* (Crown Publishers. 2006).

Amy E. Sloan, *Basic Legal Research: Tools and Strategies* (Aspen Law & Business. 2000).

Christopher Slobogin, *Privacy at Risk: The New government Surveillance and the Forth Amendment* (The University of Chicago Press. 2007).

Pauk Slovic, *The Perception of Risk* (Earthscan Publisher. 2000).

Thomas J. Smedinghoff, *Online Law: The Software Publishers Association's Legal Guide to Doing Business on the Internet* (Thomas J. Smedinghoff ed., Addison-Westley. 1996).

Jeff Smith, *Managing Privacy: Information Technology and Corporate America* (The University of North Carolina Press. 1994).

L. Graham Smith, *Impact Assessment and Sustainable Resource Management* (Longman Scientific and Technical. 1993).

Robert Ellis Smith, *Ben Franklin's Web Site: Privacy and Curiosity from Plymouth Rock to the Internet* (Privacy Journal. 2004).

Rodney A. Smolla, *Free Speech in an Open Society* (Vintage Books. 1992).

James G. Snell & Frederick Vaughan, *The Supreme Court of Canada: History of the Institution* (University of Toronto Press. 1985).

Daniel J. Solove, *The Digital Person: Technology and Privacy in the Information Age* (New York University Press. 2004).

Daniel J. Solove, *Understanding Privacy* (Harvard University Press. 2008).

Daniel J. Solove, *Nothing to Hide: The False Tradeoff between Privacy and Security* (Yale University Press. 2011).

Daniel J. Solove, et al., *Privacy, Information, and Technology* (Aspen Publishers 2nd ed. 2006).

John T. Soma, *Computer Technology and the Law* (Shepard's/McGraw-Hill. 1983).

South African Law Reform Commission, *Privacy and Data Protection Report: Project 124* (South African Law Reform Commission. 2009).

Richard A. Spinello, *Ethical Aspects of Information Technology* (Prentice Hall. 1995).

Guido Stempel & Thomas Hargrove, *Public Attitudes About Media Invasion of Privacy* (AEJMC Conference Papers 1998).

Clifford Stoll, *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage* (Pocket Books. 1990).

Michael Stolleis, *The Law under the Swastika: Studies in Legal History in Nazi*

Germany (Thomas Dunlap trans., The University of Chicago Press. 1998).

Jane Stromseth, et al., *Can Might Make Rights?: Building the Rule of Law after Military Interventions* (Cambridge University Press. 2006).

Cass R. Sunstein, *Free markets and social justice* (Oxford University Press. 1997).

Cass R. Sunstein, *Designing Democracy: What Constitutions Do* (Oxford University Press. 2001).

Cass R. Sunstein, *Why Societies Need Dissent* (Harvard University Press. 2003).

Cass R. Sunstein, et al., *Are Judges Political? An Empirical Analysis of the Federal Judiciary* (Brookings Institution Press. 2006).

Richard E. Susskind, *The Future of Law: Facing the Challenges of Information Technology* (Clarendon Press Rev. ed. 1998).

Peter P. Swire & Robert E. Litan, *None of Your Business: World Data Flows, Electronic Commerce and the European Privacy Directive* (Brookings Institution Press. 1998).

Charles J. Sykes, *The End of Privacy: Personal Rights in the Surveillance Society* (St. Martin's Press. 1999).

Don Tapscott, *The Digital Economy: Promise and Peril In The Age of Networked Intelligence* (McGraw-Hill. 1995).

Don Tapscott & David Ticoll, *The Naked Corporation: How the Age of Transparency Will Revolutionize Business* (Free Press. 2003).

Don L. Teeter & Dwight L. Le Duc, *Law of Mass Communications: Freedom and Control of Print and Broadcast Media* (Foundation Press 7th ed. 1992).

Steven M. Teles, *The Rise of the Conservative Legal Movement: The Battle for Control of the Law* (Princeton University Press. 2008).

Richard H. Thaler & Cass R. Sunstein, *Nudge: Improving Decisions About Health, Wealth, and Happiness* (Yale University Press. 2008).

The Center for Democracy and Technology, *Preliminary e-Government Policy, Law and Regulation Survey Report: South Africa* (The Center for

Democracy and Technology. 2006).

R. Murray Thomas & Dale L. Brubaker, *Theses and Dissertations: A Guide to Planning, Research, and Writing* (Bergin & Garvey. 2000).

Lawrence H. Tribe, *The Invisible Constitution* (Oxford University Press. 2008).

Joseph Turow, *Americans and Online Privacy: The System is Broken* (Annenberg Public Policy Center, University of Pennsylvania. 2003).

Nick Turse, *The Complex: How the Military Invades Our Everyday Lives* (Metopolita Books - Henry Holt and Company. 2008).

Tom R. Tyler, *Why People Obey the Law* (Princeton University Press. 2006).

United Kingdom Department of the Environment, *Environmental Assessment, Circular 15/1988* (FaLSO. 1988).

United States Department of Health and Human Services, *Toward a National Health Information Infrastructure, Report to the Secretary, US Department of Health and Human Services, Workgroup on Computerization of Patient Records* (Government Printing Office. 1993).

United States Department of War, *Final Report: Japanese Evacuation from the West Coast 1942* (Wartime Civil Control Administration, Western Defense Command and Fourth Army, Press Release No. 1, March 14, 1942. 1943).

United States Environmental Protection Agency, *Science Policy Council Handbook: Risk Characterization* (Government Printing Office. 2000).

United States Privacy Protection Study Commission, *Personal Privacy in an Information Society* (U.S. Privacy Protection Study Commission. 1977).

United States Privacy Protection Study Commission, *Personal Privacy in an Information Society, 502 (1977) – US Privacy Act of 1974 Future* (Author. 1994).

United States Senate, *USA S. Rep. No. 515, 100th Cong., 2d Sess. 1, 4 (1988), reprinted in 1988 U.S.C.C.A.N. (102 Stat. 3935) 5577, 5580* (US Government Printing Office. 1988).

United States Senate, *Report on Ratification of the International Covenant on Civil and Political Rights* § Exec. Rep. No. 102-123, 15 (US Government Printing Office. 1992).

Wim Van Grembergen, *Strategies for Information Technology Governance* (Idea Group Publishing. 2004).

John J. Vargo & Ray Hunt, *Telecommunications in Business: Strategy and Application* (Irwin. 1996).

Privacy Victoria, *Privacy Audit Manual* (Author. 2007).

Norman J. Vig & Herbert Paschen, *Parliaments and Technology: The Development of Technology Assessment in Europe* (State University of New York Press. 2000).

David Vogel, *The Market for Virtue: The Potential And Limits of Corporate Social Responsibility* (Brookings Institution Press. 2005).

Raymond Wacks, *Personal Information: Privacy and the Law* (Oxford University Press. 1993).

Raymond Wacks, *Law, Morality, and the Private Domain* (Hong Kong University Press. 2000).

E. D. Warfield *The Kentucky Resolution of 1799* (Putnam 2nd ed. 1894).

Alan Watson, *Law Out of Context* (University of Georgia Press. 2000).

Peter Wayner, *Digital Copyright Protection* (AP Professional. 1997).

Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* (United States Institute of Peace. 2006).

Gary Weiss, *Ann Rand Nation: The Hidden Struggle for America's Soul* (St. Martin's Press. 2012).

Alan F. Westin, *Privacy and Freedom* (Atheneum. 1967).

Allen F. Westin & Michael A. Baker, *Databanks in a Free Society: Computers, Record-Keeping & Privacy. National Academy of Sciences. Washington. D.C. Project on Computer Databanks* (Quadrangle Books. 1972).

David B. Whittle, *Cyberspace: The Human Dimension* (W. H. Freeman and Company. 1997).

Lauren Ruth Wiener, *Digital Woes: Why We Should Not Depend on Software* (Addison-Wesley Publishing Company. 1994).

Wik-Consult/Rand Europe/Clip/Crid/Glocom, *Comparison of Privacy and Trust Policies in the Area of Electronic Communications: Final Report* (Authors.

2007).

Valerie Plame Wilson, *Fair Game: My Life as a Spy, My Betrayal by the White House* (Simon & Schuster. 2007).

Benjamin Wittes, *Law and the Long War: The Future of Justice in the Age of Terror* (The Penguin Press. 2008).

Bob Woodward & Scott Armstrong, *The Brethren: Inside the Supreme Court* (Simon & Schuster. 1979).

World Bank, *Initiatives in Legal and Judicial Reform* (World Bank 2002).

Christopher G. Wren & Jill R. Wren, *The Legal Research Manual: A Game Plan for Legal Research and Analysis* (Adams & Ambrose Publishing 2nd ed. 1986).

Benjamin Wright & Jane K. Winn, *Law of Electronic Commerce: Edi, Fax, and E-Mail : Technology, Proof and Liability* (Aspen Law & Business 3rd ed. 2001).

David Wright & Paul. De Hert, *Privacy Impact Assessment* (Springer 2012).

Robert K. Yin, *Case Study Research: Design and Methods* (Sage Publications 4th ed. 2009).

Kenneth Younger, *Report of the Committee on Privacy, Chairman: The Right Hon Kenneth Younger* (Home Office. 1972, July).

Fareed Zakaria, *The Future of Freedom: Illiberal Democracy at Home and Abroad* (W.W. Norton & Company. Rev. ed. 2007).

Jonathan Zittrain, *The Future of the Internet and How to Stop It* (Yale University Press. 2008).

Books: Edited

Seymour Bosworth, et al., *Computer Security Handbook* § 1 (John Wiley & Sons 5th ed. 2009a).

Seymour Bosworth, et al., *Computer Security Handbook* § 2 (John Wiley & Sons 5th ed. 2009b).

Bryan A. Garner, *Black's Law Dictionary* (Bryan A. Garner ed., West Group 17

ed. 1990).

Madeleine Colvin, *Developing Key Privacy Rights: The Impact of the Human Rights Act of 1998* (Madeleine Colvin ed., Hart Publishing 2002).

Ronald Deibert, et al., *Access Denied: The Practice and Policy of Global Internet Filtering* (Ronald Deibert, et al. eds., The MIT Press 2008).

Denis J. Galligan, *Socio-Legal Studies in Context: The Oxford Centre Past and Future (Journal of Law and Society Special Issues)* (Denis J. Galligan ed., Wiley-Blackwell 1995).

Serge Gutwirth, et al., *Reinventing Data Protection?* (Serge Gutwirth, et al. eds., Springer 2009).

Sven Ove Hansson & Elin Palms, *The Ethics of Workplace Privacy* (Sven Ove Hansson & Elin Palms eds., P.I.E.-Peter Lang S.A. 2005).

Rikke Frank Jergensen, *Human Rights in the Global Information Society* (Rikke Frank Jergensen ed., The MIT Press 2006).

Andrew T. Kenyon & Megan Rischardson, *New Dimensions in Privacy Law: International and Comparative Perspectives* (Andrew T. Kenyon & Megan Rischardson eds., Cambridge University Press 2006).

Phaedon John Kozyris, *Regulating Internet Abuses: Invasion of Privacy* (Phaedon John Kozyris ed., Kluwer Law International 2007).

The National Council for Civil Liberties. Liberty, *Liberating Cyberspace: Civil Liberties, Human Rights and the Internet* (Liberty ed., Pluto Press 1999).

Brian D. Loader, *The Governance of Cyberspace: Politics, Technology and Global Restructuring* (Brian D. Loader ed., Routledge 1997).

Brian D. Loader, *Cyberspace Divide: Equality, Agency and Policy in the Information Society* (Brian D. Loader ed., Routledge 1998).

David Lyon, *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination* (David Lyon ed., Routlegde 2003).

Reinhardt Buys, *Cyberlaw@SA: The Internet and the Law in South Africa* (Reinhardt Buys ed., J. L. Van Schaik Publishers 2000).

Reinhardt Buys & Francis Cronjé, *Cyberlaw@SA II: The Internet and the Law in South Africa* (Reinhardt Buys ed., J. L. Van Schaik Publishers 2nd ed.

2004).

Ferdinand David Schoeman, *Philosophical Dimensions of Privacy: An Anthology* (Ferdinand David Schoeman ed., Cambridge University Press 2007).

Paul L. C. Torremans, *Copyright and Human Rights: Freedom of Expression - Intellectual Property - Privacy* (Paul L. C. Torremans ed., Kluwer Law International 2004).

David Wright, et al., *Safeguards in a World of Ambient Intelligence* (David Wright, et al. eds., Springer Science 2008).

David Wright & Paul De Hert, Privacy Impact Assessment (David Wright & Paul De Hert ed., Springer 2012).

Katja S. Ziegler, *Human Rights and Private Law: Privacy as Autonomy* (Stefan Wogenauer ed., Hart Publishing 2007).

Book: Sections

Anita L. Allen, *Privacy in American Law*, in *Privacies: Philosophical Evaluations* (Beate Rossler ed. Stanford University Press 2004).

J Baker, *A Practical Framework for EIA Follow-up*, in *Assessing Impact: Handbook for EIA and SEA Follow-up* (A. Morrison-Saunders & J. Arts eds., Earthscan 2004).

Jack M. Balkin, *The Constitution in the National Surveillance State*, in *The Constitution in 2020* (Jack M. Balkin & Reva B. Siegel eds., Oxford University Press 2009).

Kenneth A. Bamberger & Deirdre K. Mulligan, *PIA Requirements and Privacy Decision-Making in US Governmental Agencies*, in *Privacy Impact Assessment* (David Wright & Paul De Hert eds., Springer 2012).

David W Barron, *People, Not Computers*, in *Privacy* (J. B. Young ed. John Wiley & Sons 1978).

Robin M. Bayley & Colin J. Bennett, *Privacy Impact Assessments in Canada*, in *Privacy Impact Assessment* (David Wright & Paul De Hert eds., Springer 2012).

William M Beaney, *The Constitutional Right to Privacy in the Supreme Court, 1962*, in *The Supreme Court Review, 1963* (Philip B. Kurland ed. The University of Chicago Press 1963).

Stanley. I. Benn & G. F. Gaus, *The Public and the Private: Concepts and Action*, in *Public and Private in Social Life* (Stanley. I. Benn & G. F. Gaus eds., Croon Helm, Ltd 1983).

Colin J. Bennett, *Convergence Revisited: Toward a Global Policy for the Protection of Personal Data?* in *Technology and Privacy: The New Landscape* (Philip Agre & Marc Robinson eds., The MIT Press. 1998).

Francis Bennion, *Teaching Law Management*, in *Reviewing Legal Education* (Peter Birks ed. Oxford University Press 1994).

Jeremy Bentham, *The Panopticon*, in *The Panopticon Writings* (Miran Bozovic ed. Verso 1995).

Edward J. Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, in *Philosophical Dimensions of Privacy: An Anthology* (Ferdinand D. Schoeman ed. Cambridge University Press 1984).

Anne Wells Branscomb, *Property Rights in Information*, in *Information Technologies and Social Transformation* (Bruce R Guile ed. National Academy Press 1985).

N. Bratza, *The Treatment and Interpretation of the European Convention on Human Rights: Aspects of Incorporation*, in *European Convention on Human Rights: Aspects of Incorporation* (J. P. Gardner ed. British Institute of Comparative Law 1992).

Alan Brinkly, *A Familiar Story: Lessons from Past Assaults on Freedom*, in *The War on Our Freedoms: Civil Liberties in an Age of Terrorism* (Richard C. Leone & Greg Anrig eds., Public Affairs 2003).

Judee K. Burgoon, *Privacy and Communication*, in *Communication Yearbook 6* (Michael Burgoon & Noel E. Doran eds., Sage Publications 1982).

Roger V. Clarke, *Situational Crime Prevention*, in *Building a Safer Society: Strategic Approaches to Crime Prevention* (Michael H. Tonry & David P. Farrington eds., University of Chicago Press 1995a).

Roger V. Clarke, *PIAs in Australia: A Work-In-Progress Report*, in *Privacy Impact Assessment* (David Wright & Paul De Hert eds., Springer 2012).

Grover Cleveland, *Fourth Annual Message to Congress, 3 Dec. 1888*, in *Messages and Papers of the Presidents* (James D. Richardson ed. Government Printing Office 1888).

T. J Cottle, *Is Privacy Possible?* in *The Right to Privacy* (Grant S. Mcclellan ed. H. W. Wilson 1976).

Mary J. Culnan & Sandra J. Milberg, *Consumer Privacy*, in *Information Privacy: Looking Forward, Looking Back* (M. Culnan, et al. eds., Georgetown University Press 1999).

Richard A Epstein, *Deconstructing Privacy: And Putting It Back Together Again*, in *The Right to Privacy* (Ellen Krankel Paul, et al. eds., Cambridge University Press 2000).

Frank H. Esterbrook, *Intellectual Property is Still Property*, in *Information Ethics: Privacy, Property, and Power* (Adam D. Moore ed. University of Washington Press 2005).

Charles Fried, *Privacy (A Moral Analysis)* in *Philosophical Dimensions of Privacy: An Anthology* (Ferdinand David Schoeman ed. Cambridge University Press 1984).

Phil George, *McSpotlight: Freedom of Speech and the Internet*, in *Liberating Cyberspace: Civil Liberties, Human Rights & the Internet* (Liberty ed. Pluto Press 1999).

Rutherford Birchard Hayes, *Diary and Letters of Rutherford Birchard Hayes*, in *U.S. President. Diary and Letters of Rutherford Birchard Hayes: Nineteenth President of the United States* (Charles Richard Williams ed. The Ohio State Archaeological and Historical Society 1888).

Michelle Hough, *The Decline of Privacy: How the Loss of Privacy Impacts Our Lives and Our Livelihoods*, in *Privacy: Management, Legal Issues and Security Aspects* (Tobias K. Buckner & Betram L. Knowles eds., Nova Publishers 2012).

Thomas Jefferson, *Letter to George Logan*, in *The Writings of Thomas Jefferson*

(Paul Leicester Ford ed. G. P. Putnam's Sons 1816).

Abraham Lincoln, *Letter to Colonel William F. Elkins, November 21, 1864*, in *The Lincoln Encyclopedia* (1950) (Archer H. Shall ed. Macmillan 1864).

Duncan A. Macdonald, *Privacy, Self-Regulation, and the Contractual Model: A Report from Citicorp Credit Services, Inc.*, in *Privacy and Self-Regulation in the Information Age* (U.S. Department of Commerce ed. Government Printing Office 1997).

V. Macha & R. Makaramba, *The Development and Harmonization of EIA Regulations —Tanzania Country Report*, in *The Development and Harmonization of Environmental Laws in East Africa: Development and Harmonization of EJA regulations* (Joint Project on Environmental Law and Institutions In Africa ed. The African Sub Regional Project Nairobi 1999).

M. Mendes, *Privacy and Computer-Based Information Systems*, *in Issues in New Information Technology* (Benjamin M. Compaine ed. Ablex Publishing 1988).

Adam D. Moore, *Intangible Property: Privacy, Power, and Information Control*, in *Information Ethics: Privacy, Property, and Power* (Adam D. Moore ed. University of Washington Press 2005).

Angus Morrison-Saunders & Jos Arts, *Introduction to EIA Follow-Up*, in *Assessing Impact: Handbook of EIA and SEA Follow-Up* (Angus Morrison-Saunders & Jos Arts eds., Earthscan 2004).

Deidre K. Mulligan & Janlori Goldman, *The Limits and the Necessity of Self-Regulation: The Case for Both*, in *Privacy and Self-Regulation in the Information Age* (U.S. Department of Commerce ed. Government Printing Office 1997).

Hanno N Olinger, et al., *Western Privacy and Ubuntu - Influences in the Forthcoming Data Privacy Bill* in *Ethics of New Information Technology - Proceedings of the Sixth International Conference of Computer Ethics: Philosophical Enquiry* (CEPE2005), P Brey, F Grodzinsky and L Introna (eds), Enschede, The Netherlands, 291-306, July 2005 (Philip Brey, et al.

eds., 2005).

Bruce Phillips, *Foreword*, in *The Personal Information Protection and Electronic Documents Act: An Annotated Guide* (Stephanie Perrin, et al. eds., Irwin 2001).

William Pitt, *Speech on the Excise Bill*, in (1839). *Historical Sketches of Statesmen Who Flourished in the Time of George III* (Henry Peter Brougham ed. Charles Knight & Co 1762).

Richard A. Posner, *An Economic Theory of Privacy*, in *Philosophical Dimensions of Privacy: An Anthology* (Ferdinand Schoeman ed. Cambridge University Press 1984).

Alexander Rosenberg, *Privacy as a Matter of Taste and Right*, in *The Right to Privacy* (Ellen Krankel Paul, et al. eds., Cambridge University Press 2000).

James Rule, et al., *Preserving Individual Autonomy in an Information-Oriented Society*, in *Computers, Ethics, and Social Values* (Deborah G. Johnson & Helen Nissenbaum eds., Prentice Hall 1995).

Peter H. Russell, *The Growth of Canadian Judicial Review and the Commonwealth and American Experiences*, in *Comparative Judicial Review and Public Policy* (Donald W. Jackson & C. Neal Tate eds., Greenwood Press 1992).

Ferdinand D. Schoeman, *Privacy and Intimate Information*, in *Philosophical Dimensions of Privacy: An Anthology* (Ferdinand D. Schoeman ed. Cambridge University Press 1984).

Arnold Simmel, *Privacy Is Not An Isolated Freedom*, in *Privacy* (Nomos, XIII) (J. Ronald Pennock & John W. Chapman eds., Atherton Press 1971).

Cass R. Sunstein, *Introduction: Behavioral Law & Economics*, in *Behavioral Law & Economics* (Cass R. Sunstein ed. Cambridge University Press 2000).

John Swaigen & Richard E. Woods, *A Substantive Right to Environmental Quality*, in *Environmental Rights in Canada* (John Swaigen ed. Butterworths 1991).

Michael A. Tomasulo & Scott N. Godes, *Helping Clients Evaluate Their Cyber*

Risks, in *Understanding Developments in Cyberspace Law: Leading Lawyers on Analyzing Recent Trends, Case Law, and Legal Strategies Affecting the Internet Landscape* (Thomas Reuters Aspatore ed. Thomas Reuters / Aspatore 2012).

Hal R. Varian, *Economic Aspects of Personal Privacy*, in *Privacy and Self-Regulation in the Information Age* (U.S. Department of Commerce ed. U.S. Department of Commerce 1996).

Kristen Walker, *Treaties and the Internationalisation of Australian Law* in *Courts of Final Jurisdiction: The Mason Court in Australia (*Cheryl Saunders ed. Federation Press 1966).

Willis H. Ware, *Privacy and Information Technology — The Years Ahead*, in *Computers and Privacy in the Next Decade* (Lance J. Hoffman ed. Academic Press 1980).

Adam Warren & Andrew Charlesworth, *Privacy Impact Assessments in the UK*, in *Privacy Impact Assessment* (David Wright & Paul De Hert eds., Springer 2012).

Journal Articles[2]

Bradley J. Alge, Effects of Computer Surveillance on Perceptions of Privacy and Procedural Justice, 86 *Journal of Applied Psy*chology, 4, 798 (2001).

Catherine Allan & Allan Curtis, Nipped in the Bud: Why Regional Scale Adaptive Management is Not Blooming, 36 *Environmental Management,* 414 (2005).

Anita L Allen, Privacy as Data Control: Conceptual, Practical, and Moral Limits of the Paradigm, 32 *Connecticut Law Review*, 861 - 75 (2000).

Irwin Altman, *Privacy: A Conceptual Analysis*, 8 Environment and Behavior, 1, 7(1976).

Alexander Alvaro, Why Property Rights Were Excluded from the Canadian Charter of Rights and Freedoms, 24 *Canadian Journal of Political*

[2] ALWD places article titles in italics. UNISA prefers journal name in italics.

Science, 309(1991).

Akhil Reed Amar, Intratextualism, 112 *Harvard Law Review*, 747 (1999).

Margo Anderson & William Seltzer, Federal Statistical Confidentiality and Business Data: Twentieth Century Challenges and Continuing Issues, 1 *The Journal of Privacy and Confidentiality*, 1, 7 (2009).

James M. Assey & Demetrios A. Eleftheriou, The EU-U.S. Privacy Safe Harbor: Smooth Sailing or Troubled Waters? 9 *CommLaw Conspectus: Journal of Commercial Law & Policy*, 145 (2001).

David Bainbridge & Graham Pearce, Tilting at Windmills - Has the New Data Protection Law Failed to Make a Significant Contribution to Rights of Privacy, 2000 *Journal of Information, Law and Technology*, 2 (2000).

Jack M. Balkin, The Constitution in the National Surveillance State, 93 *Minnesota Law Review,* 1, 1 (2008).

Kenneth A. Bamberger, Regulation as Delegation: Private Firms, Decision-making, and Accountability in the Administrative State, 5*6 Duke Law Journal*, 2, 377 (2006).

Kevin Bankston & Megan E. Gray, Government Surveillance and Data Privacy Issues: Foundations and Developments, 3 *The Privacy & Information Law Reporter*, 8, 1 (2003).

Yochai Benkler, Internet Regulation: A Case Study in the Problem of Unilateralism, 2000 *European Journal of International Law*, 1, (2000).

Francis Bennion & Kay Goodall, A New Skill? Law-Text Analysis, 3 *Web Journal of Current Legal Issues* (2006).

Jerry Berman & Deirdre Mulligan, The Internet and the Law: Privacy in the Digital Age: Work in Progress, 23 Nova Law Review, 549 (1999).

George A Bermann, The Discipline of Comparative Law in the United States, 51 *Ruevu Internationale De Droit Compare'*, 4, 1041 (1999).

Biometric Technology Today, Privacy, 1 *Biometric Technology Today*, 7 (1993, November).

Michael D. Birnhack, *The EU Data Protection Directive: An Engine of a Global Regime,* 24 *Computer Law & Security Report*, 6, 508 (2008).

Vincent Blasi, The Checking Value in First Amendment Theory, 1997 *American Bar Foundation Research Journal*, 521 (1997).

M. D. Blecher, Aspects of Privacy in the Civil Law, 43 *Tijdschrift voor Rechtsgeschiedenis*, 279 (1975).

Frederic Block, Civil Liberties During National Emergencies: The Interactions Between the Three Branches of Government in Coping with Past and Current Threats to the Nation's Security, 29 *New York University Review of Law and Social Change*, 3, 459 (2005).

Edward J. Bloustein, Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser, 39 *New York University Law Review*, 1003 (1964).

A. Brunel, Bills Registered, But No Rules: The Scope of Trademark Protection for Internet Domain Names, 7 *Journal of Proprietary Rights*, 2 (1994).

James L. Buckley, Joint Statement in Explanation of Buckley/Pell Amendment, 120, *Congressional Record, Record* 13991, 13 December 1974 (1974).

Kattrin Schartz Byford, Privacy in Cyberspace: Constructing a Model of Privacy for the Electronic Communications Environment, 24 *Rutgers Computer & Technology Law Journal*, 1 (1998).

L. Jean Camp, Web Security and Privacy: An American Perspective, 15 *The Information Society*, 4, 249 (1999).

Thomas Carothers, The Rule of Law Revival, 77 *Foreign Affairs,* 95 (1998, March/April).

Roger V. Clarke, Computer Matching by Government Agencies: The Failure of Cost/Benefit Analysis as a Control Mechanism, 4 *Information Infrastructure and Policy, 1*, 29 (1995).

Richard Clayton, et al., Ignoring the Great Firewall of China, 3 *I/S: A Journal of Law and Policy for the Information Society*, 2, 273 (2007).

Marie Clear, Comment, Falling into the Gap: The European Union's Data Protection Act and its Impact on U.S. Law and Commerce, 18 *John Marshall Journal of Computer and Information Law,* 4, 981 (2000).

John B Clutterbuck, Karl Llewellyn and the Intellectual Foundations of Enterprise Liability Theory, 97 *Yale Law Journal*, 1114 (1988).

David Cole, Enemy Aliens, 54 *Stanford Law Review,* 951 (2005).

Sandra Day O' Connor, Federalism of Free Nations, 28 *New York University Journal of International Law and Politics*, 1-2, 35 (1996).

Roger Cotterrell, Subverting Orthodoxy, Making Law Central; A View of Socio-Legal Studies, 29 *Journal of Law and Society*, 4, 675 (2002).

John D. R. Craig, Invasion of Privacy and Charter Values: The Common-Law Tort Awakens 42 *McGill Law Journal,* 355 (1997).

Susan Crawford, The Ambulance, the Squad Car, and the Internet, 21 *Berkeley Technology Law Journal*, 2, 873 (2006).

Frank Cross & Emerson Tiller, Judicial Partisanship and Obedience to Legal Doctrine, 107 *Yale Law Journal*, 7, 2155 (1998).

Mary J. Culnan, Protecting Privacy Online : Is Self-Regulation Working, 19 *Journal of Public Policy and Marketing,* 1, 20 (2000).

Judith Wagner Decew, The Scope of Privacy in Law and Ethics, 5 *Law and Philosophy,* 32 (1986).

James X. Dempsey & Lara M. Flint, Commercial Data and National Security, 72 *George Washington Law Review*, 1459 (2004).

Valerian J. Derlega & Alan L. Chaiken, *Privacy and Self-Disclosure in Social Relationships,* 33 *Journal of Social Issues*, 3, 102 (1977).

Gurpreet S. Dhillon & Trevor T. Moores, Internet Privacy: Interpreting Key Issues, 14 *Information Resources Management Journal*, 4, 33 (2001).

Ben Dipper, et al., Monitoring and Post Auditing in Environmental Impact Assessment: A Review, 41 *Journal of Environmental Planning and Management,* 731 (1998).

Tim Dixon, Communications Law Centre wants IPPs revised in line with Australian Privacy Charter, 3 *Privacy Law and Policy Reporter*, 9, 171 (1997).

William Orville Douglas, The Dissent, A Safeguard of Democracy, 32 *Journal of the American Judicial Society,* 104 (1948).

S. P Duffy, Ruling may help curb cybersquatters, *The Legal Intelligencer*, April 29 (1999).

Ronald Dworkin, Hard Cases, 88 *Harvard Law Review,* 1057 (1975).

Jonathan I. Edelstein, *Anonymity and International Law Enforcement in Cyberspace,* 7 *Fordham Intellectual Property Media & Entertainment Law Journal,* 231 (1996).

Julia A. Ekstrom, et al., Gauging Agency Involvement in Environmental Management Using Text Analysis of Laws and Regulations, 6 *I/S: A Journal of Law and Policy for the Information Society*, 2, 189 (2010).

Julia A. Ekstrom, et al., A Tool to Navigate Overlaps in Fragmented Ocean Governance 33 *Marine Policy,* 3, 532 (2009).

Richard H. Fallon, The Rule of Law as a Concept in International Discourse, 97 *Columbia Law Review*, 1, 7 (1997).

Jan Fernback & Zizi Papacharissi, Online Privacy as Legal Safeguard: The Relationship Among Consumer, Online Portal, and Privacy Policies, 9 *New Media & Society,* 5, 715 (2007).

Richard L. Field, 1996: Survey of the Year's Development in Electronic Cash Law and the Laws Affecting Electronic Banking in the United States, 46 *American University Law Review,* 967 (1997).

David H. Flaherty, On the Utility of Constitutional Rights to Privacy and Data Protection, 41 *Case Western Law Review*, 831 (1991).

David H. Flaherty, Some Reflections on Privacy and Technology, 26 *Manitoba Law Journal,* 2, 219 (1999).

Jeremy D. Fraiberg & Michae J. Trebilcock, Risk Regulation: Technocratic and Democratic Tools for Regulatory Reform, 43 *McGill Law Journal*, 4, 835 (1998).

Charles Fried, Privacy, 77 *Yale Law Journal,* 475 (1968).

A. Michael Froomkin, The Essential Role of Trusted Third Parties in Electronic Commerce, 75 *Oregon Law Review*, 49 (1996).

Candace Cummins Gauthier, Privacy Invasion by the News Media: Three Ethical Models, 17 *Journal of Mass Media Ethics,* 1, 26 (2002).

Ruth Gavison, Privacy and the Limits of Law, 89 *Yale Law Journal,* 3, 421 (1980).

Tom Gerety, Redefining Privacy, 12 *Harvard Civil Rights–Civil Liberties Law Review,* 233 (1977).

Robert B. Gibson, Environmental Assessment Design: Lessons from the Canadian Experience, 15 *The Environmental Professional,* 1, 2 (1993).

Susan M. Gilles, Promises Betrayed: Breach of Confidence as a Remedy for Invasion of Privacy, 43 *Buffalo Law Review,* 1, 1 (1995).

E.S Glass, Restructuring Informed Consent: Legal Therapy for the Doctor-Patient Relationship, 179 *Yale Law Journal,* 1533 (1970).

Cathy Goodwin, Privacy: Recognition of a Consumer Right, 10 *Journal of Public Policy and Marketing*, 1, 149 (1991, Spring).

Ken Gormley, One Hundred Years of Privacy, 1992 *Wisconsin Law Review,* 1335 (1992).

Graham Greenleaf, Reps Committee Protects the 'Privacy- Free Zone", 7 *Privacy Law and Policy Reporter*, 1 (2000).

James Grimmelmann, The Structure of Search Engine Law, 93 *Iowa Law Review,* 1, 2 (2007).

Chris Guthrie, et al., Inside the Judicial Mind, 86 *Cornell Law Review*, 4, 1 (2001).

John Hagel, The Coming Battle for Customer Information, 75 *Harvard Business Review*, 53 (1997).

R.Grant Hammond, The Misappropriation of Commercial Information in the Computer Age, 64 *Canadian Bar Review*, 342 (1986).

Trotter Hardy, The Proper Legal Regime for "Cyberspace", 55 *University of Pittsburgh Law Review*, 993 (1994).

Robert Harvie & Hamar Foster, Ties that bind? The Supreme Court of Canada, American jurisprudence, and the revision of Canadian criminal law under the Charter, 28 *Osgoode Hall Law Review*, 729 (1990).

Robert Harvie & Hamar Foster, Different Drummers: The Supreme Court of Canada, American Jurisprudence and the Continuing Revision of Criminal Law Under the Charter, 24 *Ottawa Law Review,* 39 (1992).

Stephen E Henderson, Nothing New Under the Sun? A Technologically Rational

Doctrine of Fourth Amendment Search, 56 *Mercer Law Review,* 507 (2005).

Susan N. Herman, The USA Patriot Act and the submajoritarian Fourth Amendment, 41 *Harvard Civil Rights - Civil Liberties Law Review*, 1, 67 (2006).

Janine Hiller, et al., *Privacy and Security in the Implementation of Health Information Technology (Electronic Health Records): U.S. and EU Compared,* 17 *Boston University Journal of Science & Technology Law,* 1, 1 (2011 Winter*).*

Sameer Hinduja, Theory and Policy in Online Privacy, 17 *Knowledge, Technology, & Policy,* 1, 38 (2004).

Jack Hirshleifer, Privacy: Its Origin, Function and Future, 9 *Journal of Legal Studies,* 4, 649 (1980).

Louis W. Hodges, The Journalist and Privacy, 9 *Journal of Mass Media Ethics*, 4, 97 (1994).

Chris Jay Hoofnagle, *Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement,* 29 *North Carolina Journal of International Law and Commercial Regulation,* 4, 595 (2004).

House of Lords, Practice Statement 119661 1, 58 *Weekly Law Reports*, 1234 (1966).

Marsha Cope Huie, et al., The Right of Privacy in Personal Data: The EU Prods the U.S. and Controversy Continues, 9 *Tulsa Journal of International and Comparative Law,* 391 (2002).

Jeffery Hutchings, et al., Is Scientific Inquiry Incompatible with Government Information Control? 54 *Canadian Journal of Fisheries and Aquatic Sciences*, 5, 1198 (1997).

Jacob Jacoby, et al., Corrective Advertising and Affirmative Disclosure Statements: Their Potential for Confusing and Misleading the Consumer, 46 *Journal of Marketing*, 61 (1982).

J. T Johnson, The Private I, You, They, 9 *Journal of Mass Media Ethics*, 4, 223

(1994).

Christine Jolls, et al., A Behavioral Approach to Law and Economics, 50 *Stanford Law Review,* 5, 1471 (1998).

D. Marvin Jones, Unrightable Wrongs: The Rehnquist Court, Civil Rights, and An Elegy for Dreams, 25 *University of San Francisco Law Review*, 1, 2 (1990).

Owen D. Jones, Time-Shifted Rationality and the Law of Law's Leverage: Behavioral Economics Meets Behavioral Biology, 95 *Northwestern University Law Review,* 4, 1141 (2001).

Anne Kandra, The Myth of Secure E-Shopping, 19 *PC World*, 7, 29 (2001).

B. Jerry Kang, Information Privacy In Cyberspace Transactions, 50 *Stanford Law Review,* 1193 (1998).

Stan Karas, Privacy, Identity, Databases, 52 *American University Law Review*, 393 (2002).

Alan F. Karr, et al., Data Quality: A Statistical Perspective, 3 *Statistical Methodology,* 137 (2006).

James E. Katz & Annette R. Tassone, Public Opinion Trends: Privacy and Information Technology, 54 *Public Opinion Quarterly*, 125 (1990).

The Hon Justice Michael D Kirby, Privacy in Cyberspace, *21 University of New South Wales Law Journal,* 2, 323 (1998).

Jacqueline Klosek, The Development of International Police Cooperation Within the EU and Between the EU and Third Party States: A Discussion of the Legal Bases of Such Cooperation and the Problems and Promises Resulting Thereof, 14 *American University International Law Review*, 3, 599 (1999).

David M. Kristol, HTTP Cookies: Standards, Privacy, and Politics, 1 *ACM Transactions Internet Technology*, 2, 151 (2001).

P. G. Kuehl & R. F Dyer, Applications of the Normative Belief Techniques for Measuring the Effectiveness of Deceptive and Corrective Advertisements, 4 *Advances in Consumer Research*, 204 (1976).

Christopher Kuner, Beyond Safe Harbor: European Data Protection Law and

Electronic Commerce, 35 *International Lawyer*, 79 (2001).

Dale Kunkel & Ursula Goette, Broadcasters' Response to the Children'sTelevision Act, 2 *Communication Law and Policy,* 3, 289 (1997).

Nkonko M Kwamwangamalu, Ubuntu in South Africa: a Sociolinguistic Perspective to a Pan-African Concept 13 *Critical Arts Journal*, 2, 24 (1999).

Namhee Kwon, et al., Multidimensional Text Analysis for eRulemaking, 57 *Administrative Law Review*, 2, 411 (2005).

Kenneth C. Laudon, Markets and Privacy, 39 *Communications of the Association for Computing Machinery,* 9, 92 (1996, September).

Robert S. Laufer & Maxine Wolfe, Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory, 33 *Journal of Social Issues,* 3, 22 (1977).

Patrick J. Leahy, New Laws for New Technologies: Current Issues Facing the Subcommittee on Technology and the Law 5 *Harvard Journal of Law and Technology,* 1, 1 (1992).

Mark A. Lemley, Intellectual Property and Shrinkwrap Licenses, 68 *Southern California Law Review,* 1239 (1995).

Avner Levin & Mary Jo Nicholson, Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground, 2 *University of Ottawa Law & Technology Journal,* 2, 357 (2005).

Lissa L. Broome & Jerry W. Markham, Banking and Insurance: Before and after the Gramm-Leach-Bliley Act, 25 *Journal of Corporation Law,* 4 (2000).

Maria Chiara Malaguti, Private-Law Instruments for Reduction of Risks on International Financial Markets: Results and Limits of Self-Regulation, 11 *Open Economies Review*, 1, 247 (2000).

Ross Marshall, et al., International Principles for Best Practice EIA Follow-up, 23 *Impact Assessment and Project Appraisal*, 3, 175 (2005).

Richard O. Mason, Four Ethical Issues for the Information Age, 7 *MIS Quarterly,* 2, 4 (1986).

Hiroyuki Matsuda, Challenges Posed by the Precautionary Principle and

Accountability in Ecological Risk Assessment, 14 *Environmetrics,* 245 (2003).

John W. Maxwell, et al., Self-Regulation and Social Welfare: The Political Economy of Corporate Environmentalism, 43 *Journal of Law and Economics*, 583 (2000).

Thomas S. Mayer, Privacy and Confidentiality Research and the U.S. Census Bureau Recommendations Based on a Review of the Literature, *Survey Methodology #2002-01*, 1 (2007).

Michael B. Mazis & Janice E. Adkinson, An Experimental Evaluation of a Proposed Corrective Advertising Remedy, 13 *Journal of Marketing Research,* 178 (1976).

Andrew J. Mcclurg, Bringing Privacy Law Out of the Closet: A Tort Theory of Liability for Intrusions in Public Places, 73 *North Carolina Law Review*, 989 (1995).

Andrew J. Mcclurg, A Thousand Words are Worth a Picture: A Privacy Tort Response to Consumer Data Profiling, 98 *Northwestern University Law Review,* 1, 63 (2003).

Charles T. Meadow, Online Database Industry Timeline, 11 *Database Magazine*, 5, 23 (1988).

Charles T. Melton, The significance of law in the everyday lives of children and families, 22 *Georgia Law Review,* 851 (1988).

Gary B. Melton, *Minors and Privacy: Are Legal and Psychological Concepts Compatible?*, 62 Nebraska Law Review, 455-93 (1983).

Gary B. Melton, The Significance of Law in the Everyday Lives of Children and Families, 22 *Georgia Law Review,* 851 (1988).

Douglas C. Michael, Cooperation Implementation of Federal Regulations, 13 Yale Journal on Regulation, 542 (1996).

Sandra. J. Milberg, et al., Values, Personal Information Privacy Concerns, and Regulatory Approaches, 38 *Communications of the ACM,* 12, 65 (1995).

Arthur R Miller, Personal Privacy in the Computer Age: The Challenge of a New Technology in an Information-Oriented Society, 67 *Michigan Law Review,*

1089 (1969).

R.T Mills & D.S Krantz, Information, Choice, and Reactions to Stress: A Field Experiment in a Blood Bank with Laboratory Analogue, 37 *Journal of Personality and Social Psychology*, 4, 608 (1979).

Mats Millson, Comment: Is There Room for Environmental Self-Regulation in the Mining Sector? 22 *Resources Policy,* 87 (1996).

George Milne & Mary J. Culnan, Strategies for Reducing Online Privacy Risks: Why Consumers Read [Or don't Read] Online Privacy Notices, 18 *Journal of Interactive Marketing*, 3, 15 (2004).

George R. Milne & Andrew J. Rohm, Consumer Privacy and Name Removal Across Direct Marketing Channels: Exploring Opt-in and Opt-out Alternatives, 19 *Journal of Public Policy and Marketing,* 2, 238 (2000).

A. D Miyazaki & A Fernandez*, Internet privacy and security: An examination of online retailer disclosures,* 19 *Journal of Public Policy and Marketing,* 1, 54 (2000).

James T. Moore, Sexual Predators Can't Hide Thanks to Public Safety Information Act, 6 *Community Policing Exchange, Phase V*, 21, 8 (1998).

Gillian S. Morris, Fundamental Rights: Exclusion by Agreement*?* 30 *Industrial Law Journal,* 1, 49 (2001).

Richard S. Murphy, Property Rights in Personal Information: An Economic Defense of Privacy, 84 *Georgetown Law Journal,* 2381 (1996).

Patrick J. Murray, The Adequacy Standard Under Directive 95/46/EC: Does U.S. Data Protection Meet This Standard? 2*1 Fordham International Law Journal,* 932 (1998).

Thomas Nagel, Concealment and Exposure, 27 *Philosophy and Public Affairs*, 1, 3 (1998).

Caroline B Ncube, Watching the Watcher: Recent Developments in Privacy Regulation and Cyber-Surveillance in South Africa, 3 *SCRIPTed - A Journal of Law, Technology & Society*, 4, 344 (2006).

Hano N. Olinger, et al., Western Privacy and/or Ubuntu? Some Critical Comments on the Influences in the Forthcoming Data Privacy Bill in South

Africa, 39 *The International Information & Library Review,* 1, 31 (2007).

Carl Oppedahl, Remedies in Domain Name Lawsuits: How Is a Domain Name Like a Cow? 15 *John Marshall Journal of Computer & Information Law*, 3, 437 (1997).

Leonard Ortolano & Anne Shepherd, *Environmental Impact Assessment: Challenges and Opportunities,* 13 *Impact Assessment,* 1, 3 (1995).

Stephen A. Oxman, Exemptions To The European Union Personal Data Privacy Directive: Will They Swallow The Directive? 24 *Boston College International and Comparative Law Review,* 1, 191 (2000).

Martin J. Packer, Hermeneutic Inquiry in the Study of Human Conduct, 40 *American Psychologist,* 10, 1081 (1985).

Zizi Papacharissi & Jan Fernback, Online Privacy and Consumer Protection: An Analysis of Portal Privacy Statements, 49 *Journal of Broadcasting & Electronic Media,* 3, 259 (2005, October).

William A. Parent, A New Definition of Privacy for the Law, 2 *Law and Philosophy,* 305 - 71 (1983).

Richard B. Parker, A Definition of Privacy, 27 *Rutgers Law Review,* 1, 275 (1974).

Elizabeth Paton-Simpson, Privacy and the Reasonable Paranoid: The Protection of Privacy in Public Places, 50 *University of Toronto Law Journal,* 3, 305 (2000).

Paul J. Polking & Scott A. Cammarn, Overview of the Gramm-Leach-Bliley Act, 4 *North Carolina Banking Institute,* 1, 1 (2000).

Graham Pearce & Nicholas Platten, Orchestrating Transatlantic Approaches to Personal Data Protection: A European Perspective, 22 *Fordham International Law Journal,* 5, 2024 (1999).

Henry H. Perritt Jr., Tort Liability, the First Amendment, and Equal Access to Electronic Networks, 5 *Harvard Journal of Law and Technology*, 65 (1992).

Henry H. Perritt Jr., Jurisdiction in Cyberspace, 41 *Villanova Law Review,* 1, 100 (1996).

Sandra Petronio, Communication Boundary Management: A Theoretical Model of Managing Disclosure of Private Information Between Marital Couples, 1 *Communication Theory,* 4, 311 (1991).

Owen R. Phillips, Negative Option Contracts and Consumer Switching Costs, 60 *Southern Economic Journal*, 2, 304 (1993).

John D. Podesta & Raj Goyle, Lost in Cyberspace? Finding American Liberties in a Dangerous Digital World, 23 *Yale Law and Policy Review,* 2, 509 (2005).

Neil A. F. Popovic, The Right to Participate in Decisions That Affect the Environment, 10 *Pace Environmental Law Review*, 2, 683 (1993, Spring).

Richard A. Posner, The Economics of Privacy, 71 *The American Economic Review,* 2, 405 (1981).

Roscoe Pound, The Scope and Purpose of Sociological Jurisprudence. Part 1, 2, & 3, 24, 25 *Harvard Law Review,* 591, 140, 489 (1911-1922).

Margot Priest, The Privatization of Regulation: Five Models of Self-Regulation, 29 *Ottawa Law Review*, 2, 233 (1997).

William Lloyd Prosser, Privacy, 48 *California Law Review,* 3, 383 (1960).

Christopher Patrick Raab, Fighting Terrorism in an Electronic Age: Does the Patriot Act Unduly Compromise Our Civil Liberties? 2006 *Duke Law and Technology Review,* 3, 26 (2006).

James Rachels, Why Privacy is Important, 4 *Philosophical and Public Affairs*, 4, 323 (1975).

Joseph Reagle & Lorrie Faith Cranor, The Platform for Privacy Preferences, 42 *Communications of the ACM*, 2, 48 (1999).

Priscilla M. Regan, Ideas or Interests: Privacy in Electronic Communications, 21 *Policy Studies Journal,* 3, 450 (1993).

William H. Rehnquist, Is an Expanding Right of Privacy Consistent with Fair and Effective Law Enforcement, 1 *Nelson Timothy Stephens Lectures, University of Kansas Law School*, 1-13 (1974, September 26 -27).

Charles A. Reich, *The New Property*, 73 *The Yale Law Journal*, 5, 733 (1964).

Joel R. Reidenberg, Privacy in the Information Economy-- A Fortress or Frontier for Individual Rights? 44 *Federal Communications Law Journal,* 2, 195

(1992).

Joel R. Reidenberg, Restoring Americans' Privacy in Electronic Commerce, 14 *Berkeley Technology Law Journal*, Spring, 771 (1999).

Joel R. Reidenberg, E-commerce and Trans-Atlantic Privacy, 38 *Houston Law Review,* 717 (2001).

Judith Resnik, Managerial Judges, 96 *Harvard Law Review*, 374 (1982).

Oscar M. Reubhausen & O. G. Brim, Privacy and Behavioral Research, 65 *Columbia Law Review,* 1184 (1965).

Richard L. Revesz, Environmental Regulation, Ideology, and the DC Circuit, 83 Virginia Law Review, 1717 (1997).

David A. J. Richards, Liberalism, Public Morality, and Constitutional Law: Prolegomenon to a Theory of the Constitutional Right to Privacy, 5*1 Law and Contemporary Problems*, 1, 123 (1988).

Neil M. Richards, Reconciling Data Privacy and the First Amendment, 52 *UCLA Law Review*, 4, 1149 (2005).

Alice Robbin, The Loss of Personal Privacy and Its Consequences for Social Research, 28 *Journal of Government Information,* 5, 493 (2001).

Jeffrey Rothfeder, No Privacy on the Net, *PC World,* 223 (1997, February).

Therese Marie Sacco, Social Exclusion: Experiences of Some of Apartheid's Victims of Human Rights Violations Post The Truth And Reconciliation Commission, 2003 *IUC Journal of Social Work: Theory and Practice*, 6.2 (2003).

Mark Sagoff, Economic Theory and Environmental Law, 79 *Michigan Law Review*, 7, 1393 (1981).

Steven R. Salbu, The European Union Data Privacy Directive and Internal Relations, 35 *Vanderbilt Journal of Transnational Law*, 655 (2002).

Jeremy Sarkin, The Effect of Constitutional Borrowings on the Drafting of South Africa's Bill of Rights and Interpretation of Human Rights Provisions, 1 *University of Pennsylvania Journal of Constitutional Law*, 2, 176 (2008).

Kurt M. Saunders, The Regulation of Internet Encryption Technologies: Separating the Wheat from the Chaff, 17 *John Marshall Journal of*

Computer & Information Law, 3, 945 (1999).

Walter V Schaefer, Precedent and Policy, 34 *University of Chicago Law Review*, 3, 23 (1966).

Rudolf B. Schlesinger, The Past and Future of Comparative Law, 43 *American Journal of Comparative Law,* 477 (1995).

Timothy D Schoechle, Privacy on the Information Superhighway: Will My House Still Be My Castle? 19 *Telecommunication Policy,* 6, 435 (1995).

Stephen J. Schulhofer, The New World of Foreign Intelligence Surveillance, 17 *Stanford Law & Policy Review,* 531 (2006).

Gary Schuman, Trademark Protection of Container and Package Configurations--A Primer, 59 *Chicago - Kent Law Review*, 779 (1983).

Paul M Schwartz, Privacy and Democracy in Cyberspace, 52 *Vanderbilt Law Review,* 6, 1609 (1999).

Paul M. Schwartz, Internet Privacy and the State, 32 *Connecticut Law Review,* 815 (2000).

Paul M. Schwartz, Property, Privacy, and Personal Data, 117 *Harvard Law Review,* 7, 2055 (2004).

Francis Reginald Scott, The Consequences of the Privy Council Decisions, 15 *Canadian Bar Review,* 485 (1937).

Gregory Shaffer, Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards, 25 *Yale Journal of International Law*, 1, 1 (2000).

Manu Sharma & Bryan G. Norton, A Policy Decision Tool for Integrated Environmental Assessment, 8 *Environmental Science and Policy,* 4, 356 (2005, August).

John Shattuck, Computer Matching is a Serious Threat to Individual Rights, 27 *Communications of the ACM,* 6, 538 (1984).

William R. Sheate, *Public Participation: The Key to Effective Environmental Assessment,* 21 *Environmental Policy and Law,* 3/4, 156 (1991).

Anna Shimanek, Note, Do You Want Milk with Those Cookies? Complying with the Safe Harbor Privacy Principles, 26 *Iowa Journal of Corporate Law*, 2,

455 (2001).

Spiros Simitis, Reviewing Privacy in an Information Society, 135 *University of Pennsylvania Law Review* 3, 707 (1987, March).

Spiros Simitis, From the Market to the Polis: The EU Directive on the Protection of Personal Data, 80 *Iowa Law Review*, 445 (1995, March).

H. Jeff Smith, et al., Information Privacy: Measuring Individuals' Concerns About Organizational Practices, 20 *Management Information Systems - MIS Quarterly,* 2, 167 (1996, June).

Jeff Smith, Privacy Policies and Practices: Inside the Organizational Maze, 36 *Communications of the ACM*, 12, 105 (1993).

J. C Smith, Machine Intelligence and Legal Reasoning, 73 *Chicago-Kent Law Review,* 1, 277 (1998).

Stephen A. Smith, Communication and the Constitution in Cyberspace, 43 *Communication Education,* 2, 87 (1994).

Daniel J. Solove, Privacy and Power: Computer Databases and Metaphors for Information Privacy, 53 *Stanford Law Review*, 6, 1393 (2001).

Daniel J. Solove, Access and Aggregation: Public Records, Privacy, and the Constitution, 86 *Minnesota Law Review*, 6, 1137 (2002).

Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy,* 75 *Southern California Law Review,* 1083 (2002a).

Daniel J. Solove, Conceptualizing Privacy, 90 *California Law Review*, 1087 (2002b).

Herbert Spencer, Progress: Its Law and Causes, 67 The Westminster Review, 445 (1857).

Aaron P. Stevens, Arresting Crime: Expanding the Scope of DNA Databases in America, 79 *Texas Law Review*, 921 (2001).

George J. Stigler, An Introduction to Privacy in Economics and Politics, 9 *Journal of Legal Studies*, 4, 623 (1980).

Robert S. Summers, A Formal Theory of the Rule of Law, 6 *Ratio Juris: An International Journal of Jurisprudence and Philosophy of Law,* 2, 127 (1993).

Domingo R. Tan, Personal Privacy in the Information Age: Comparison of Internet Data Protection Regulations in the United States and European Union, 21 *Loyola of Los Angeles International & Comparative Law Journal*, 7, 661 (1999).

Phillip Thomas, Curriculum Development in Legal Studies, 20 *Law Teacher*, 110 (1986).

Judith Jarvis Thomson, The Right to Privacy, 4 *Philosophy and Public Affairs*, 4, 295 (1975).

Paul D. Tolchinsky, et al., Employee Perceptions of Invasion of Privacy: A Field Experiment, 66 *Journal of Applied Psychology*, 3, 308 (1981).

Chris Tollefson, Strategic Lawsuits Against Public Participation: Strategic Lawsuits Against Public Participation, 73 *Canadian Bar Review,* 2, 200 (1994).

Charles R. Tremper & Mark A. Small, Privacy Regulation of Computer-Assisted Testing and Instruction, 63 *Washington Law Review*, 3, 841 (1988).

David Trezise*, Alternative Approaches to Legal Control of Environmental Quality in Canada*, 21 McGill Law Journal, 404 (1975).

Laurence H. Tribe, The Constitution in Cyberspace: Law and Liberty Beyond the Electronic Frontier, The Humanist, 15-39 (1991, September-October).

Eric C. Turner & Subhasish Dasgupta, *Privacy on the Web: an Examination of User Concerns, Technology, and Implications for Business Organizations and Individuals,* 20 *Information Systems Management*, 1, 8 (2003).

Maxine Van De Wetering, The Popular Concept of 'Home' in Nineteenth Century America, 18 *Journal of American Studies,* 1, 5 (1984).

David T. Vernon & Douglas.A. Bigelow, Effects of Information About a Potentially Stressful Situation on Responses to Stress Impact, 29 *Journal of Personality and Social Psychology,* 1, 50 (1974).

Alan B. Vickery, Breach of Confidence: An Emerging Tort, 82 *Columbia Law Review,* 1426 (1982).

Eugene Volokh, Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People From Speaking About You, 52

Stanford Law Review, 5, 1049 (2000).

Adam Warren, et al., Privacy Impact Assessments: International Experience as a Basis for UK Guidance, 24 *Computer Law & Security Report,* 3, 233 (2008).

Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, 4 *Harvard Law Review,* 5, 193 (1890).

Charles Weiss, The Coming Technology of Knowledge Discovery: A Final Blow to Privacy Protection, 2004 *University of Illinois Journal of Law, Technology and Policy,* 2, 253 (2004).

John W. Whitehead & Steven H. Aden, Forfeiting "Enduring Freedom" for "Homeland Security": A Constitutional Analysis of the USA PATRIOT Act and the Justice Department's Anti-Terrorism Initiatives, 61 *American University Law Review*, 6, 1081 (2002).

G. S Wood, Thomas Jefferson, Equality and the Creation of a Civil Society, 64 *Fordham Law Review*, 5, 2133 (1996).

Ulrich U. Wuermeling, Harmonisation of European Union Privacy Law, 14 *John Marshall Journal of Computer & Information Law*, 411 (1996).

Frederick H. Zemans, Legal Aid and Advice in Canada, 16 *Osgoode Hall Law Journal,* 663 (1978).

Rachel K. Zimmerman, The Way the "Cookies" Crumble: Internet Privacy and Data Protection in the Twenty-First Century, 4 *New York University Journal of Legislation and Public Policy*, 2, 439 (2000).

Newspaper Articles

Edmund L. Andrews, *European Law Aims to Protect Privacy of Data*, New York Times (1998, October 25), at A1.

Tom Daschle, *Power We Didn't Grant*, Washington Post (2005, December 23), at A21.

S. Davies, *Forget the Passport, Let's See Your Hand*, The Independent, London (1994, August 15), at A1.

James Davison, *Feingold Visits UW, Speaks on Patriot Act*, University of Wisconsin Badger (2004, April 5), at 38, p. 1.

A. Dowd, *Canada Judge Rules Kiddy Porn Possession Protected*, Vancouver (Reuters) (1999, January 15), at A1.

Elizabeth Fernandez, *6,000 UCSF Patients' Data Got Put Online*, San Francisco Chronicle (2008, May 2), at A1.

Rufus Hatch, *Hatch on Vanderbilt*, Chicago Daily Tribune (1882, October 17), at 12.

Audrey Hudson, *Librarians Dispute Justice's Claim on the Use of Patriot Act*, Washington Times (2003, September 19), at A10.

Tim Jackson, *This Bug in Your PC is a Smart Cookie*, Financial Times (1996, February 12), at A1.

Anick Jesdanun, *Internet Privacy Concerns Rising, Study Suggests: Findings Come Amid a Record Number of Data Breaches in 2007*, Associated Press (2008, January 16), at A1.

Jonathan Krim, *FTC Will Not Seek New Privacy Laws*, Washington Post (2001, October 5), at E1.

June Kronholz, *Patriot Act Riles an Unlikely Group: Nation's Librarians*, Wall Street Journal (2003, October 23), at A1-A6

B. Lambert, *Rise of Secret Surveillance Cameras Criticized*, NewYork Times (Wash.ed.) (1998, December 13), at 55.

George Lardner & Al Kamen, *1971 Rehnquist Account is Challenged by 3 Mem; Ballot Security Role in '60's Called Active* The Washington Post (1986. July 25), at A-4.

P Lewis, *Technology: Online*, New York Times (1995, August 14), at D5.

Tamara Loomis, *A Few Companies Have Complied with EU Law*, New York Law Journal (2001, August 30), at 5.

Audra Mahlong, *High Costs of Privacy Bill: Government will Spend R35 Million to Pilot Systems, But No Further Funding has been Secured*, IT Web Business 3 November. (2009), at.

John Markoff, *Growing Compatibility Issue: Computers and User Privacy*, New

York Times (1993, March 3), at A1.

John Markoff, *U.S. Data Code Is Unscrambled In 56 Hours*, New York Times (1998, July 17), at D1.

Haya El Nasser, *Papers Show Census Role in WWII Camps*, USA Today 30 March 2007. (2007), at http://www.usatoday.com/news/nation/2007-03-30-census-role_N.htm.

New York Herald – World, *Giants of Wall Street, in Fierce Battle Over Mastery, Precipitate Crash that Brings Ruins to Hordes of Pygmies* New York Herald – World (1901, May 11), at 22.

John M. Poindexter, *Security with Privacy*, New York Times (2003, September 10), at A25.

Theodore Roosevelt, *Roosevelt in the Kansas City Star*, Kansas City Star (1918, May 7), at 149.

Edmund Sanders, *FTC Nominee Sails Through Senate Confirmation Hearing*, Los Angeles Times (2001, May 17), at 3.

John Schwartz, *DoubleClick Takes It On The Chin; New Privacy Lawsuit Looms; Stock Price Drops*, The Washington Post E1 (2000, February 18), at A1.

L Williams, *Web of Intrigue*, *Sydney Morning Herald* (2000, April 29), at 1.

World News, *Guyana Lifts Restrictions on Sex-Related Internet Content*, *World News* (1999, January 11), at 545.

Electronic Sources

American Medical Association (A.M.A.), *HIPAA Violations and Enforcement*, Author. (2011), at http://www.ama-assn.org/ama/pub/physician-resources/solutions-managing-your-practice/coding-billing-insurance/hipaahealth-insurance-portability-accountability-act/hipaa-violations-enforcement.page (accessed 14 June 2011).

A.C.L.U. Of Northern California, *Google's Privacy Policy: What Would be the Real Impact of APEC?* (2007), at http://www.aclunc.org/issues/technology/blog/asset_upload_file251_6206.

pdf (accessed 3 November 2011).

Abantika Ghosh, *Right to Privacy May Become Fundamental Right*, The Times of India. (2011), at http://articles.timesofindia.indiatimes.com/2011-06-04/india/29620422_1_privacy-law-ministry-confidentiality (accessed 4 June 2011).

Jenn Abelson, *Breach of Data at TJX is Called the Biggest Ever*. (2007, March 29), at http://www.boston.com/business/articles/2007/03/29/breach_of_data_at_tjx_is_called_the_biggest_ever/ (accessed 5 December 2011).

ACM - Association for Computing Machinery, *Association for Computing Machinery Opposes Adoption of Uniform Computer Transactions Act (UCITA): UCITA Could Negatively Impact the Quality and Robustness of Mass Market Software*. (1999), at http://www.acm.org/announcements/ucita.html (accessed 15 November 2011).

Byron Acohido, *Theft of Personal Data More Than Triples This Year*. (2007, December 9), at http://www.usatoday.com/money/industries/technology/2007-12-09-data-theft_N.htm?POE=click-refer (accessed 2 January 2011).

Alessandro Acquisti & Richard Power, *New Study Co-Authored by CyLab Researcher: Face Recognition Software and Social Media Result in Increased Privacy Risks*, Cylab News: Carnegie Mellon University (2011), at http://www.cylab.cmu.edu/news_events/news/2011/acquisti-study-finds-face-recognition-software-social-media-increase-privacy-risks.html (accessed 1 August 2011).

Acrod/Cofa Police Certificate Working Party, *A Resource Manual for the Use of Police Certificates*. (2005), at http://www.ideaswa.net/Resources/Other/documents/ACRODCOFAPoliceCertificateResourceManualVersion2.pdf (accessed 23 January 2012).

Administrative Office of the U.S. Courts, *Privacy - Wiretap*. (1996), at http://www.epic.org/privacy/wiretap/stats/wiretap_stats.html (accessed 10

June 2011).

Jacquie Mcnish and Omar El Akkad, *Facebook Users Risk Blackmail, Privacy Czar Warns* Globe and Mail (2010), at http://www.theglobeandmail.com/news/technology/facebook-users-risk-blackmail-privacy-czar-warns/article1545444/ (accessed 26 April 2011).

Alexandre Deslongchamps, *Canada Banks, Agency, May Violate Clients' Privacy, Report Says* Bloomberg Press. (2009), at http://www.bloomberg.com/apps/news?pid=newsarchive&sid=aT_A.1ec0oKY (accessed 17 November 2011).

Margret Amatayakul & Michael R. Cohen, *Is HIPAA Now Spelled Apathy?* (2008), at http://health-care-it.advanceweb.com/editorial/content/editorial.aspx?CC=89534%20 (accessed 24 July 2011).

America on Line Sucks, *Rules of the Road*. (1997), at http://www.aolsucks.org/censor/tos/rules_of_road.html, http://www.aolsucks.org/censor/tos/online_conduct.html, http://www.aolsucks.org/censor/tos/usenet.html (accessed 27 May 2011).

America Online (AOL), *Assurance of Voluntary Compliance*. (1997), at http://www.wa.gov/ago/releases/agreement_aol.html (accessed 10 November 2011).

American Bar Association, *Business Law Section, Committee on the Law of Cyberspace, Subcommittee on Electronic Commerce Report*. (1999), at http://www.webcom.com/legaled/docs/jbmb699.html (accessed 15 June 2011).

American Medical Association (A.M.A.), *Guidelines for Medical and Health Information Sites on the Internet*. (2000), at http://jama.ama-assn.org/issues/v283n12/full/jsc00054.html (accessed 21 May 2011).

American Research Libraries, *UCITA*. (1999), at http://www.arl.org/info/frn/copy/ucita.html (accessed 1 October 2011).

Ross Anderson, et al., *Database State: A Report Commissioned by the Joseph Roundtree Reform Trust Ltd*. (2009), at

http://www.jrrt.org.uk/uploads/Database%20State.pdf (accessed 23 March 2011).

Sarah Anderson & John Cavanagh, *Top 200: The Rise of Global Corporate Power*, Global Policy Forum. (2000), at http://www.globalpolicy.org/component/content/article/221/47211.html (accessed 15 June 2011).

Angus Reid Global Monitor, *Five Countries Review Privacy, Technology*. (2006), at http://www.angus-reid.com/polls/view/11915 (accessed 31 March 2011).

Annenberg Public Policy Center of the University of Pennsylvania, *Free Gift Could Entice Children into Revealing Personal Family Information Online*. (2000), at http://appcpenn.org/final_release_fam.pdf (accessed 19 May 2011).

Anthony J. Degidio Jr, *Internet Domain Names and the Federal Trademark Dilution Act: A Law for the Rich and Famous 1997*. (1997), at http://www.lawoffices.net/tradedom/sempap.htm (accessed 14 July 2011).

Jim Armitage, *Web Users Angry at ISPs' Spyware Tie-Up*. (2008, June 3), at http://www.thisislondon.co.uk/standard-home/article-23449601-details/Web+users+angry+at+ISPs%27+spyware+tie-up/article.do (accessed 3 June 2011).

Antonella Artuso, *New ID Card Threatens our Privacy: Commissioner Raises Concerns*. (2008, October 21), at http://www.torontosun.com/news/canada/2008/10/21/7151421-sun.html (accessed 22 October 2011).

Warwick Ashford, *Mandatory Data Breach Notifications: An Opportunity For Change*, Computer Weekly. (2010), at http://www.computerweekly.com/Articles/2010/07/21/242043/Mandatory-data-breach-notifications-an-opportunity-for.htm (accessed 20 July 2011).

Assises, *Motion of the Participants at the Second Forum on an Internet that Promotes Non-Commercial Interests and Solidarity*. (1999), at http://www.assises.sgdg.org/motion-assises99-en.html (accessed 14 April

2011).

Associated Press, *Anti-Spam Law Ruled Unconstitutional*, Cnet.com. (2000, March 14), at http://news.cnet.com/news/0-1007-200-1572322.html?tag=st.ne.1002.bgif.1007-200-1572322 (accessed 15 March 2011).

Associated Press, *Judge Allows Start-Ups to Link to Big Rivals*, CNET News.com. (2000, March 29), at http://news.cnet.com/news/0-1005-200-1597146.html?pt.salon (accessed 29 March 2011).

Associated Press, *Doctor Reprimanded for Web Sales*, Las Vegas Sun. (2000, March 31), at http://www.lasvegassun.com/sunbin/stories/tech/2000/mar/31/033100648.html (accessed 31 March 2011).

Associated Press, *Britain Plans Cyber-Center to Spy on the Internet.* (2000, May 11), at http://www.mercurycenter.com/svtech/news/breaking/merc/docs/006527.htm (accessed 29 May 2011).

Associated Press, *Bush's Statement Opens Up Mail Privacy Debate*. (2007, January 7), at http://www.sptimes.com/2007/01/07/Worldandnation/Bush_s_statement_open.shtml (accessed 2 December 2011).

Canadian Marketing Association, *Consumer Protection*. (2010), at http://www.the-cma.org/public/?WCE=C=47|K=224338 (accessed 27 July 2011).

World Wide Legal Information Association, *Legal Resources*. (2010), at http://www.wwlia.org/LegalResources.aspx (accessed 4 July 2011).

Eric Auchard, *Google Says World Could Use Asian Privacy Approach*, Reuters. (2008, September 14), at http://mobile.reuters.com/mobile/m/FullArticle/CTECH/ntechnologyNews_uUSN1340110220070914 (accessed 14 September 2011).

Melissa August, et al., *Numbers*, Time. (2000), at http://www.time.com/time/archive/preview/0,10987,997618,00.html

(accessed 16 April 2011).

Australian Direct Marketing Association *The ADMA Direct Marketing Code of Practice*. (2007), at http://www.adma.com.au/asp/index.asp?pgid=1985&cid=10887&id=2196 (accessed 6 January 2011).

David Banisar, *Big Brother Goes Hi-Tech*, Covert Action Quarterly. (2003), at http://mediafilter.org/caq/CAQ56brother.html (accessed 11 June 2011).

Lisa Banks, *Commissioner Launches Privacy Guide* IDG News Service (2010), at http://www.networkworld.com/news/2010/051110-commissioner-launches-privacy.html (accessed 11 May 2011).

Diane Bartz, *Analysis: Google's Private Data Grab Means Big Legal Trouble*, Reuters. (2010), at http://www.reuters.com/article/idUSTRE6604YG20100701 (accessed 1 July 2011).

BBC News, *Cyber Libel Ruling Threatens UK ISPs*. (2000, May 2), at http://news.bbc.co.uk/hi/english/uk/newsid_733000/733432.stm (accessed 2 May 2011).

BBC News, *Google Ranked 'Worst' on Privacy*. (2007, June 11), at http://news.bbc.co.uk/2/hi/technology/6740075.stm (accessed 11 June 2011).

R. Beck, *Death of Online Retailing*. (2000), at http://abcnews.go.com/sections/business/DailyNews/eretailstudy_000412.html (accessed 4 June 2011).

Bellman, *Linux Standards Groups Combine*, IT-Director.com. (2000, May 10), at http://www.it-director.com/business/content.php?cid=803 (accessed 5 May 2011).

Colin J. Bennett, *The Protection of Personal Financial Information: An Evaluation of the Privacy Codes of the Canadian Bankers Association and the Canadian Standards Association*. (1997), at http://web.uvic.ca/polisci/bennett/research/cba.htm (accessed 31 December 2011).

Paul Schiff Berman, *Cyberspace and the State Action Debate: The Cultural Value of Applying Constitutional Norms to "Private" Regulation*, 71 University of Colorado Law Review 1263. (2000), at http://lsr.nellco.org/uconn/ucwps/papers/9 (accessed 28 December 2011).

Jon Bing, *Data Protection in Norway*. (2006), at http://www.jus.uio.no/iri/forskning/lib/papers/dp_norway/dp_norway.html (accessed 20 August 2011).

Natasha Bita, *Australian Police Get Access to Tax Data for Trials*, The Australian. (2010), at http://www.sott.net/articles/show/204287-Australian-Police-get-access-to-tax-data-for-trials (accessed 8 March 2011).

Bizcommunity.Com, *Consumer Protection Act Made Easy* (2010, March 15), at http://www.bizcommunity.com/Article/196/307/45701.html (accessed 24 April 2011).

Martin H. Bosworth, *Starbucks Data Loss No Laughing Matter: Company Loses Laptops Containing 60,000 Employees' Information*. (2006, November 6), at http://www.consumeraffairs.com/news04/2006/11/starbucks_data.html (accessed 1 January 2011).

Jan Bouckaert & Hans Degryse, *Opt In Versus Opt Out: A Free-Entry Analysis of Privacy Policies (The Fifth Workshop on the Economics of Information Security (WEIS 2006). Robinson College, University of Cambridge, England 26-28 June 2006)*. (2006), at http://weis2006.econinfosec.org/docs/34.pdf (accessed 24 July 2011).

Christopher Bowe, *Internet Fraud Faces Worldwide Crackdown*. (2000), at http://news.ft.com/ft/gx.cgi/ftc?pagename=View&c=Article&cid=FT39J44276C&live=true&tagid=ZZZAN4NOD0C&Collid=Any (accessed 15 June 2011).

Mike Bracken, *Parliamentary Procedure*, Wired News. (1998), at http://www.wired.com/news/politics/0,1283,16778,00.html (accessed 10 May 2011).

Peter Bradwell, *Private Lives A People's Inquiry Into Personal Information*, Demos. (2010), at http://www.demos.co.uk/files/Private_Lives_-

_web.pdf?1269213706 (accessed 5 September 2011).

Hiawatha Bray, *Injunction Bars Bidder's Edge from Indexing eBay Auction Data*, Boston Globe. (2000, May 26), at http://www.boston.com/dailyglobe2/147/business/Injunction_bars_Bidder_s_Edge_from_indexing_eBay_auction_data+.shtml (accessed 22 March 2011).

Kenneth Bredemeier, *A Close Look at a New Medium*, Washington Post. (2000), at http://www.washingtonpost.com/wp-dyn/articles/A2613-2000Mar13.html (accessed 14 March 2011).

Bill Brenner, *The Pros and Cons of Data Breach Insurance*. (2008, March 19), at http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1306207,00.html (accessed 20 March 2011).

Bridge News, *Oftel: Not Necessary for Cable Groups to Open Their Networks*. (2000, April 28), at http://www.individual.com/servlet/BuildIssue?mode=topics&content_src=/frames/story.shtml%3fstory=b0427040.5rg%26level3=139960%26date=20000428%26inIssue=TRUE (accessed 28 April 2011).

Ted Bridis, *Internet Body Finds Problems Collecting Funds from Nations*, WSJ.com. (2000, June 1), at http://interactive.wsj.com/articles/SB959807167398038843.htm (accessed 15 June 2011).

British Gas Trading Limited and the Data Protection Registrar, *Data Protection.* (1998), at http://www.open.gov.uk/dpr/bgtl.htm (accessed 28 April 2011).

Anne Broache, *RIAA: No Need to Force ISPs by Law to Monitor Piracy*. (2008, January 30), at http://news.cnet.com/8301-10784_3-9861460-7.html (accessed 30 January 2011).

Jon Brodkin, *Shoppers Willing to Pay Extra for Privacy Confidence, Study Finds*. (2007, June 6), at http://www.networkworld.com/news/2007/060607-privacy-confidence-survey.html (accessed 2 January 2011).

D. Brown, *The Truth is the Same, Even for Ads on the Internet*, ZD Net. (2000, May 1), at

http://www.zdnet.com/intweek/stories/news/0%2C4164%2C2557584%2C00.html?chkpt=zdnnp1ms (accessed 1 May 2011).

Internet Advertising Bureau, *IAB UK Unveils Good Practice Principles for Online Behavioural Advertising*. (2009), at http://www.iabuk.net/en/1/behaviouralbestpractice030309.html (accessed 4 March 2011).

Lynn Burke, *Huge Kid Porn Ring Busted*. (2000, April 14), at http://www.wired.com/news/politics/0%2C1283%2C35684%2C00.html (accessed 13 May 2011).

Peter Burrows, *AT&T To Get Tough on Piracy*. (2007, November 7), at http://www.businessweek.com/technology/content/nov2007/tc2007116_145984.htm (accessed 15 November 2011).

George H. W. Bush, *Inaugural Address of George H. W. Bush*. (1989), at http://www.yale.edu/lawweb/avalon/presiden/inaug/bush.htm (accessed 29 June 2011).

George W. Bush, *President Signs Class-Action Fairness Act of 2005*. (2005, February 18), at http://www.whitehouse.gov/news/releases/2005/02/20050218-11.html (accessed 1 June 2011).

George W Bush, *National Security and Homeland Security Presidential Directive*. (2007, May 9), at http://www.whitehouse.gov/news/releases/2007/05/20070509-12.html (accessed 2 June 2011).

Dan Bustillos, *Privacy and Consent Concerns in International Genetic Databanks*. (2005), at http://www.law.uh.edu/healthlaw/perspectives/August2005/(DB)GeneticDatabanks.pdf (accessed 7 September 2011).

Cambridge Dictionary of American English, *Govern - Influence*. (2003), at http://www.cup.cam.ac.uk/esl/dictionary/default.asp?String=govern*2%2B0&ACT=SELECT (accessed 4 June 2011).

Melissa Campanelli, *Privacy, Security Top Consumer Worries Online: Consumer*

Reports at FTC Forum. (2006, November 7), at http://www.dmnews.com/Privacy-security-top-consumer-worries-online-Consumer-Reports-at-FTC-forum/article/93362/ (accessed 1 January 2011).

Adam Carey, *Fine Breaches of Privacy: Keating* The Sydney Morning Herald. (2010), at http://www.watoday.com.au/national/fine-breaches-of-privacy-keating-20100804-11fny.html (accessed 5 August 2011).

Caslon Analytics, *Privacy Guide*. (2004), at http://www.caslon.com.au/privacyguide14.htm (accessed 26 December 2011).

Thomas Catán, *AOL to Settle $3.5m Suit*, Ft.com. (2000, May 16), at http://news.ft.com/ft/gx.cgi/ftc?pagename=View&c=Article&cid=FT39TDNJA8C&live=true&tagid=ZZZ2H6COD0C&Collid=Any (accessed 16 May 2011).

Fred H. Cate, *Global Information Policy Making and Domestic Law*. (1999), at http://www.law.indiana.edu/glsj/vol1/cate.html (accessed 1 May 2011).

Damien Cave, *Can Hyperlinks be Outlawed?*, Salon.com. (2000, April 6), at http://www.salon.com/tech/log/2000/04/06/decss/index.html (accessed 6 April 2011).

Ann Cavoukian, *What is Privacy by Design?* Information & Privacy Commissioner Ontario. (2010), at http://www.privacybydesign.ca/ (accessed 6 July 2011).

Ann Cavoukian, *Mobile Near Field Communications (NFC) "Tap 'n Go" Keep it Secure & Private*, Information and Privacy Commissioner of Ontario. (2011), at http://www.ipc.on.ca/images/Resources/mobile-nfc.pdf (accessed 12 December 2011).

Ann Cavoukian, *Privacy by Design and the Emerging Personal Data Ecosyste*. (2012), at http://www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=1244 (accessed 31 October 2012).

CBC News, *Credit Scores Can Hike Home Insurance Rates: Insurance*

Companies Say Credit Scores are a Good Indicator of Risk. (2010), at http://www.cbc.ca/consumer/story/2010/04/08/consumer-insurance-credit-score.html (accessed 6 July 2011).

CBC News, *Sask. Patient Privacy Rule Changes Slammed*. (2010), at http://www.cbc.ca/canada/saskatchewan/story/2010/05/03/sask-privacy-dickson-heath-information.html (accessed 3 May 2011).

CBC News, *Sask. Needs Privacy Upgrade: Report*. (2010), at http://www.cbc.ca/canada/saskatchewan/story/2010/06/30/sk-dickson-privacy-upgrade.html?ref=rss (accessed 30 June 2011).

Center for Democracy and Technology, *Recent Crypto Developments Underscore Futility of US Export Controls*. (1999), at http://www.cdt.org/ (accessed 20 January 2011).

Center for Democracy and Technology, *Privacy Basics: Generic Principles of Fair Information Practices*. (2008), at http://www.cdt.org/privacy/guide/basic/generic.html (accessed 28 July 2011).

University of Queensland Social Research Centre, *Australians Concerned for Online Privacy: Study*. (2012), at http://www.uq.edu.au/news/?article=24504 (accessed 15 March 2012).

Winnie Chung & John Paynter, *Privacy Issues on the Internet*. (2002), at http://csdl2.computer.org/comp/proceedings/hicss/2002/1435/07/14350193b.pdf (accessed 10 June 2011).

Thomas Claburn, *Most Bank Sites Are Insecure*, Information Week. (2008, July 23), at http://www.informationweek.com/news/internet/security/showArticle.jhtml?articleID=209600041 (accessed 24 July 2011).

Roger V. Clarke, *Net-etiquette Mini Case Studies of Dysfunctional Human Behavior on the Net*. (1998), at http://www.anu.edu.au/people/Roger.Clarke/II/Netethiquettecases.html (accessed 3 August 2011).

Roger V. Clarke, *Introduction to Dataveillance and Information Privacy and*

Definition of Terms. (1999), at http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html#Intro (accessed 20 July 2011).

Roger V. Clarke, *Privacy Impact Assessment*. (2012), at http://rogerclarke.com/DV/PIA.html (accessed 8 March 2012).

Jeri Clausing, *Congressional Investigators Scrutinize Internet Oversight Group*, Capital Dispatch. (2000, May 2), at http://www.nytimes.com/library/tech/00/05/cyber/capital/02capital.html (accessed 2 May 2011).

Jeri Clausing, *In Hearing On 'Love Bug,' Lawmakers Go After Software Industry*, New York Times.com. (2000, May 11), at http://www.nytimes.com/library/tech/00/05/cyber/articles/11love.html (accessed 11 May 2011).

Jeri Clausing, *ICANN Runs Into More Trouble Over Election Plans*, New York Times.com (2000, May 16), at http://www.nytimes.com/library/tech/00/05/cyber/capital/16capital.html (accessed 16 May 2011).

Privacy Rights Clearinghouse, *Data Breaches: A Year in Review. The Top Half Dozen Most Significant Data Breaches in 2011* (2011), at https://www.privacyrights.org/top-data-breach-list-2011 (accessed 16 December 2011).

Privacy Rights Clearinghouse, *How to Use the Chronology of Data Breaches*. (2011), at https://www.privacyrights.org/data-breach-how-to (accessed 17 December 2011).

Dominique Clément, *Canada's Rights Movement: A History*. (2010), at http://www.historyofrights.com/ngo.html (accessed 25 June 2011).

Jay Cline, *530M Records Exposed, and Counting*, Computerworld (2008, September 9), at http://computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=Privacy&articleId=9114176&taxonomyId=84&pageNumber=1 (accessed 9 September 2011).

William J. Clinton & Albert Gore. *A Framework for Global Electronic Commerce*. (1997, July 1), at http://www.w3.org/TR/NOTE-framework-970706.html (accessed 1 August 2011).

CNET.News, *First Internet Insider Trading Case Filed*. (2000, March 14), at http://news.cnet.com/news/0-1005-200-1572664.html?tag=st.ne.1002.thed.1005-200-1572664 (accessed 14 March 2011).

CNN.Com, *Spy Court Rejects No Requests in 2006*. (2007, May 1), at http://www.cnn.com/2007/POLITICS/05/01/fisa.court/ (accessed 2 June 2011).

CNNFN, *Bad News for dot.coms: MicroStrategy Tanks on Earnings Restatement; Barron's Report Stings*. (2000), at http://www.cnnfn.com/2000/03/20/markets/techwrap/ (accessed 20 March 2011).

Code of Hammurabi, *Code of Hammurabi*. (1780 BCE), at http://www.fordham.edu/halsall/ancient/hamcode.html (accessed 24 September 2011).

Code of Justinian, *Codex Justinianus*. (529), at http://www.fordham.edu/halsall/basis/535institutes.html (accessed 26 September 2011).

Julie E. Cohen, *DRM AND Privacy*, Berkeley Technology Law Journal. (2003), at http://www.law.georgetown.edu/faculty/jec/drmandprivacy.pdf (accessed 25 July 2011).

Salvatore Colletti, et al., *Top Ten Recommendations for Improving Your Company's Data Security Compliance*, Acc: Association of Corporate Counsel. (2009), at http://www.acc.com/legalresources/publications/topten/top-ten-recommendations-for-improving-your-company.cfm (accessed 2 February 2011).

Committee of Experts on Crime in Cyber-Space (Pc-Cy), *Meeting of the Ministers' Deputies, 4 February 1997*. (1997), at http://www.cyber-

rights.org/documents/cybercrime24.htm (accessed 6 May 2011).

Committee of Ministers, *XVIII. Protection of Personal Data: Resolutions and Recommendations Adopted by the Committee of Ministers*. (2008), at http://www.coe.int/t/e/legal_affairs/about_us/treaties_and_recommendations/listall.asp#P389_25201 (accessed 22 August 2011).

Commonwealth Human Rights Initiative, *Comments Concerning the South Africa Privacy and Data Protection Bill*. (2006), at http://www.humanrightsinitiative.org/programs/ai/rti/international/laws_papers/southafrica/south_africa_privacy_bill_submission_feb06.pdf (accessed 27 February 2011).

Computer Industry Almanac, *PCs In-Use Surpassed 900M in 2005*. (2006), at http://www.c-i-a.com/pr0506.htm (accessed 23 January 2011).

Computer Professionals for Social Responsibility, *Computer Professionals for Social Responsibility*. (2003), at http://www.cpsr.org/ (accessed 20 August 2011).

Consumer Reports, *Consumers Alarmed About Online Privacy, 25% Provide Fake ID to View Sites*. (2008), at http://www.marketingcharts.com/interactive/consumers-alarmed-about-online-privacy-25-provide-fake-id-to-view-sites-6265/ (accessed 20 March 2011).

Clive Cookson, *UK Scientists Expect £100m to Build Super-Fast Internet.* . (2000), at http://news.ft.com/ft/gx.cgi/ftc?pagename=View&c=Article&cid=FT4QE4SFE5C&live=true&tagid=ZZZAN4NOD0C&Collid=Any (accessed 16 May 2011).

A. Creed, *Australian regulator reports net censorship progress.* (2000, May 1), at http://www.newsbytes.com/pubNews/00/148256.html (accessed 1 May 2011).

A. Creed, *Australians charged over spamming incident.* (2000, May 2), at http://www.Infowar.Com/ (accessed 2 May 2011).

Judith Crosbie, *Commission Seeks External Advice on Internet Privacy*. (2009,

April 28), at http://www.europeanvoice.com/article/2009/04/commission-seeks-external-advice-on-internet-privacy/64717.aspx (accessed 29 April 2011).

Christian Crumlish, *How Many People Use the Internet?* (2004), at http://x-pollen.com/many/2004/06/02/how_many_people_use_the_internet.html and http://www.internetworldstats.com/stats.htm (accessed 16 April 2011).

Mildred Cruz-Fridman, *ACLU Accuses Intel of Violating Free Speech*, Newsbytes. (2000), at http://www.newsbytes.com/pubNews/00/148994.html (accessed 12 May 2011).

CSO the Source for Security Executives, *e-Crime Congress Survey Reveals Jail Sentence for CEO a Fitting Punishment for Data Breach* (2009, April 9), at http://www.cso.com.au/article/211736/e-crime_congress_survey_reveals_jail_sentence_ceo_fitting_punishment_data_breach (accessed 29 April 2011).

John-Thor Dahlburg, *G-8 Seeks Unity on Policing Internet*, LATimes.com. (2000, May 18), at http://articles.latimes.com/2000/may/18/business/fi-31309 (accessed 18 May 2011).

Daten Schultz, *Agreement on Interterritorial Data Protection by and between Service Provider, Data Protection Company, USA and Client Company*. (1997), at http://www.datenschutz-berlin.de/sonstige/konferen/ottawa/alex1.htm (accessed 28 November 2011).

Caroline Davies & James Robinson, *Information Commissioner's Office 'Let Down' Over Illegal Snooping*, guardian.co.uk (2009), at http://www.guardian.co.uk/media/2009/sep/02/information-commission-illegal-phone-hacking (accessed 2 September 2011).

Karen Dearne, *Canberra Plans Unified Privacy Principles*. (7 October 2008), at http://www.australianit.news.com.au/story/0,24897,24456243-15319,00.html (accessed 8 October 2011).

Karen Dearne, *Privacy Changes Put Data at Mercy of Scams* The Australian. (2009), at http://www.theaustralian.com.au/news/privacy-changes-put-data-at-mercy-of-scams/story-e6frgal6-1225788524304 (accessed 20 October 2011).

Karen Dearne, *Data Breach Costs $2m Per Incident* Australian IT. (2010), at http://www.theaustralian.com.au/australian-it/data-breach-costs-2m-per-incident/story-e6frgakx-1225851401246?from=marketwatch_rss (accessed 8 April 2011).

Deloitte, *Enterprise@Risk: Insights Into the Emerging Privacy and Data Protection Function*. (2007), at http://www.deloitte.com/dtt/cda/doc/content/us_risk_s%26P_2007%20Privacy10Dec2007final.pdf (accessed 26 December 2011).

Karen Deyoung, *Terrorism Database is Ballooning, Keepers Say*. (2007, March 26), at http://www.boston.com/news/nation/washington/articles/2007/03/26/terrorism_database_is_ballooning_keepers_say/ (accessed 2 January 2011).

Sam Diaz, *CNET: Justice Dept. to ask Congress for ISP Data Retention Law*, ZDNet. (2011), at http://www.zdnet.com/blog/btl/cnet-justice-dept-to-ask-congress-for-isp-data-retention-law/43969 (accessed 25 January 2011).

Direct Marketing Association, *Direct Marketing Association's Online Marketing Guidelines and DoTthe Right Thing Commentary*. (2006), at http://www.the-dma.org/guidelines/onlineguidelines.shtml (accessed 12 August 2011).

Lynley Donnelly, *The Right to Demand Answers*, Mail and Guardian. (2011), at http://mg.co.za/article/2011-04-29-the-right-to-demand-answers (accessed 4 May 2011).

Rodger Doyle, *Privacy in the Workplace*, Scientific American. (1999), at http://www.scientificamerican.com/article.cfm?id=privacy-in-the-workplace (accessed 1 June 2011).

DSV - the Department of Computer and Systems Sciences at Stockholm University and Kth, *Freedom of Speech, the EU Data Protection Directive*

and the Swedish Personal Data Act. (2002), at http://www.dsv.su.se/jpalme/society/eu-data-direcmltive-freedom.htm (accessed 12 May 2011).

Isaac Quinn Dupont, *Privacy in the Network Society: A Juri–Normative Case for "Public Privacy"* Textual Metanoia. (2007), at http://www.iqdupont.com/privacy-in-the-network-society/ (accessed 25 July 2011).

E-Commerce Law Weekly, *Attorneys General Target Web Sales of Imported Cigarettes to Minors*. (2000, January 7), at http://www.lawnewsnetwork.com/practice/techlaw/news/A12885-2000Jan6.html (accessed 6 January 2011).

Ecommerce.Gov, *Towards Digital Equality, The U.S. Government Working Group on Electronic Commerce*. (1999), at http://www.ecommerce.gov/bodytext.htm (accessed 3 May 2011).

London Economics, *Study on the Economic Benefits of Privacy Enhancing Technologies (PETs): Final Report to The European Commission DG Justice, Freedom and Security*. (2010), at http://ec.europa.eu/justice_home/fsj/privacy/docs/studies/final_report_pets_16_07_10_en.pdf (accessed 30 July 2011).

Nicholas Economides, *The Economics of Networks*. (1996), at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1719 (accessed 22 November 2011).

W. A. Drew Edmondson, *Letter by State Attorney Generals to UCITA Committee*. (1999), at http://www.badsoftware.com/aglet1.htm (accessed 7 June 2011).

Thomas B. Edsall, *Federalist Society Becomes a Force in Washington: Conservative Group's Members Take Key Roles in Bush White House and Help Shape Policy and Judicial Appointments*, Washington Post. (2001, April 18), at http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A30099-2001Apr17&notFound=true (accessed 8 August 2011).

Eibiz.Com, *Fraud on the Net*. (2000, April 3), at http://www.businessweek.com/2000/00_14/b3675017.htm (accessed 3 April 2011).

Electronic Financial Services Council, *On-line Financial Privacy: Current Legal Framework and Recent Developments*. (1999), at http://www.efscouncil.org/frames/Library/Privacy/EFSCPrivacyIssues.html (accessed 19 August 2011).

Electronic Privacy Information Center, *Public Opinion on Privacy*. (2008), at http://epic.org/privacy/survey/default.html (accessed 6 April 2011).

Emily Flitter, *Consumer Protection Debate Pits Theory Against Record*, American Banker. (2009), at http://www.americanbanker.com/issues/174_124/-383336-1.html (accessed 23 June 2011).

Leon Englebrecht, *Data Privacy Bill in Suspended Animation*. (2008, February 20), at http://www.itweb.co.za/sections/business/2008/0802201052.asp?S=Legal%20View&A=LEG&O=FRGN (accessed 21 February 2011).

Enlist, *Green Paper on the Security of Information Systems*. (1994), at http://www.ulapland.fi/home/oiffi/enlist/resources/ (accessed 30 August 2011).

Lori Enos, *Mobile Giants to Form E-Commerce Security*, E-Commerce Times. (2000, April 12), at http://www.ecommercetimes.com/news/articles2000/000412-1.shtml (accessed 12 April 2011).

Lori Enos, *Spam Strikes Back*, E-Commerce Times. (2000, March 17), at http://www.ecommercetimes.com/news/articles2000/000317-2.shtml (accessed 17 March 2011).

Lori Enos, *U.S. States Target Illegal Online Pharmacies*, E-Commerce Times. (2000, March 31), at http://www.ecommercetimes.com/news/articles2000/000331-5.shtml (accessed 31 March 2011).

Eocglobal, *EPCglobal Guidelines on EPC for Consumer Products*. (2005), at

http://www.epcglobalinc.org/public/ppsc_guide/ (accessed 10 April 2011).

Ernst & Young, *South African CEOs are Getting More Hands-On with Information Security Issues*, Tech News. (2004, November), at http://cbr.co.za/article.aspx?pklArticleId=3290&pklCategoryId=378 (accessed 22 March 2011).

Ernst & Young, *Risk at Home: Privacy and Security Risks in Telecommuting*. (2008), at http://www.cdt.org/privacy/20080729_riskathome.pdf (accessed 30 July 2011).

Europa, *Digital Agenda: Commission Refers UK to Court Over Privacy and Personal Data Protection*. (2010), at http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/1215&format=HTML&aged=0&language=EN&guiLanguage=en (accessed 30 September 2011).

Exitenew.Com, *French ISP Seeks Anti-Nazi Help*, News.Excite.com. (2000, May 25), at http://news.excite.com/news/r/000525/14/net-internet-nazi (accessed 25 May 2011).

Laura Falk, et al., *Analyzing Websites for User-Visible Security Design Flaws*. (2008), at http://cups.cs.cmu.edu/soups/2008/proceedings/p117Falk.pdf (accessed 24 July 2011).

Federalist Society, *The Federalist Society for Law and Public Policy Studies*. (2008), at http://www.fed-soc.org/ (accessed 9 August 2011).

Lowell Feld, *George W. Bush's Stealth War on the Environment*. (2003), at http://www.dailygusto.com/news/august/bush-082003.html (accessed 23 January 2011).

Scott Ferguson, *HP Settles Civil Complaint for $14.5M*, PCMAG.Com. (2006, December 8), at http://www.pcmag.com/article2/0,2704,2070117,00.asp (accessed 26 December 2011).

James W. Fiscus, *Caveat Scriptor: Proposed Law Helping Software Producers May Injure Writers*, The Bulletin. (1999), at http://www.sfwa.org/News/software.htm (accessed 13 May 2011).

Meagan Fitzpatrick, *Privacy Watchdog Probes Dating Site*, Canwest News

Service. (2010), at http://www.ottawacitizen.com/life/Privacy+watchdog+probes+dating+site/3223965/story.html (accessed 1 July 2011).

David H. Flaherty, *Reflections on Reform of the Federal Privacy Act*. (2008), at http://www.priv.gc.ca/information/pub/pa_ref_df_e.cfm (accessed 29 June 2011).

Ford Library Museum, *President Gerald R. Ford's Statement on Privacy Legislation*. (2001), at http://www.fordlibrarymuseum.gov/library/speeches/740125.htm (accessed 31 July 2011).

Fox New.Com, *U. S. Senators Write Agencies on Internet Fairness*. (2000), at http://www.foxnews.com/vtech/0511/t_rt_0511_20.sml (accessed 11 May 2011).

Susannah Fox & Oliver Lewis, *Fear of Online Crime: Americans Support FBI Interception of Criminal Suspects' Email and New Laws to Protect Online Privacy*, Pew Internet & American Life Project. (2001), at http://www.pewinternet.org/~/media//Files/Reports/2001/PIP_Fear_of_crime.pdf.pdf (accessed 24 May 2011).

Susannah Fox, et al., *Trust and Privacy Online: Why Americans Want to Rewrite the Rules*, Pew Internet & American Life Project. (2000), at http://www.pewinternet.org/~/media/Files/Reports/2000/PIP_Trust_Privacy_Report.pdf.pdf (accessed 7 June 2011).

Freedom Information, *POIB Protestors March in Cape Town; Hearing Set*, Freedom Information. (2010), at http://www.freedominfo.org/2010/10/poib-protestors-march-in-cape-town/ (accessed 14 October 2011).

Freedom Information, *South African Committee to Seek Extension of Time*, Freedom Information. (2011), at http://www.freedominfo.org/2011/01/south-african-committee-to-seek-extension-of-time/ (accessed 28 January 2011).

Batya Friedman, et al., *Informed Consent in the Mozilla Web Browser: Implementing Value-Sensitive Design*, Proceedings of the Thirty-Fifth

Annual Hawaii International Conference on System Science. (2002, January 7-10), at http://csdl2.computer.org/comp/proceedings/hicss/2002/1435/08/14350247.pdf (accessed 4 May 2011).

Manny Frishberg, *U.S. Confused About Privacy*, Wired.com. (2000, April 28), at http://www.wired.com/politics/law/news/2000/04/35979 (accessed 20 April 2011).

Fubar, *DNA Samples*. (1999), at http://pw2.netcom.com/~fubar4/BRO.html (accessed 22 May 2011).

Scott M. Fulton, *Consumer Privacy: Can the FTC Enforce a Voluntary Code of Conduct?*, Readwrite. (2012), at http://readwrite.com/2012/03/09/consumer-privacy-can-the-ftc-e (accessed 9 March 2012).

Fundamental Orders of Connecticut, *Fundamental Orders of Connecticut* (1639), at http://usinfo.state.gov/usa/infousa/facts/democrac/3.htm (accessed 24 September 2011).

Interview by Bill Moyers with James K. Galbraith. (2008, October 8), at http://www.pbs.org/moyers/journal/10242008/transcript2.html (accessed 8 October 2011).

James K. Galbraith, *Our New Corporate Republic*, Boston Globe. (2001), at http://www.commondreams.org/views01/0107-01.htm (accessed 20 February 2011).

L Gard, *Santa Clara's Yahoo Hit with Novel Privacy Suit*, Law.com. (2000, May 12), at http://www.callaw.com/stories/edt0512k.html (accessed 12 May 2011).

Frank Gardner, *Saudis 'Defeating' Internet Porn*, BBC News. (2000, May 10), at http://news.bbc.co.uk/hi/english/world/middle_east/newsid_742000/742798.stm (accessed 15 May 2011).

Sharon Gaudin, *Missing Hard Drive Holds Sensitive Data On 535K Vets, 1.3M Doctors*, Information Week: The Business Value of Technology. (2007, February 13), at

http://www.informationweek.com/news/showArticle.jhtml?articleID=197005769 (accessed 1 January 2011).

Michael Geist, *Canadian Privacy Rights Buried in the Fine Print*. (2009), at http://www.thestar.com/article/602772 (accessed 16 March 2011).

Michael Geist, *Standing on Guard for Privacy - Before Facebook*. (2009), at http://www.thestar.com/article/695147 (accessed 14 September 2011).

Barton Gellman, *The FBI's Secret Scrutiny; In Hunt for Terrorist, Bureau Examines Records of Ordinary Americans*, Washington Post. (2005, November 6), at http://www.washingtonpost.com/wp-dyn/content/article/2005/11/05/AR2005110501366_pdf (accessed 23 November 2011).

Geocities, *Truste*. (1998), at www.ftc.gov/opa/1998/9808/geocitie.htm (accessed 22 May 2011).

Subhendu Ghosh, *Source Code as Free Speech in Encryption Case*, GigaLaw.com. (2000), at http://www.gigalaw.com/articles/ghosh-2000-05-p1.html (accessed 17 May 2011).

Alorie Gilbert, *Supporters Back Away from Software Bill*, News.com. (2003, August 7), at http://news.com.com/2100-1028_3-5061061.html?tag=fd_top (accessed 26 November 2011).

Sharon Eisner Gillett & Mitchell Kapor, *The Self-Governing Internet: Coordination by Design*. (1996), at http://ccs.mit.edu/papers/CCSWP197/CCSWP197.html (accessed 19 May 2011).

Dan Gilmore, *Law Gives Firms License to Kill Your Computer*, Mercury News Technology. (1999), at http://www.mercurycenter.com/svtech/columns/gillmor/docs/dg060699.htm (accessed 15 November 2011).

Dan Gilmore, *Microsoft to Unveil Internet Initiative*, Silicon Valley News. (2000, May 27), at http://www.mercurycenter.com/svtech/news/indepth/docs/dg052800.htm (accessed 27 May 2011).

Sonia Giordani, *Judge Strikes Law Against Online Sex Info to Minors*, The Recorder/Cal Law. (2000, January 4), at http://www.lawnewsnetwork.com/practice/techlaw/news/A12649-2000Jan3.html (accessed 10 January 2011).

Charles Giordano, *Use Privacy to Build Customer Trust, Loyalty*, DM News. (2007, March 22), at http://www.dmnews.com/Use-privacy-to-build-customer-trust-loyalty/article/94933/ (accessed 2 January 2011).

Global Internet Liberty Campaign, *Privacy and Human Rights: An International Survey of Privacy Laws and Practice*. (2008), at http://www.gilc.org/privacy/survey/intro.html (accessed 16 July 2011).

Globelaw, *International and Transnational Law*. (2003), at http://www.globelaw.com/index.html (accessed 22 May 2011).

John Goddard, *Tenants' Private Data Available on Internet*, The Star. (2009), at http://www.thestar.com/article/596808 (accessed 5 March 2011).

Eric Goldman, *Cyberspace Law Table of Cases and Statutes*. (2000), at http://members.theglobe.com/ericgoldman/tablecase.html (accessed 18 May 2011).

Goldman Sachs, *Right Code for a Worldwide Web*, Financial Times. (2000, April 9), at http://news.ft.com/ft/gx.cgi/ftc?pagename=View&c=Article&cid=FT38COJ8V6C&live=true&tagid=ZZZ2H6COD0C&Collid=Any (accessed 23 April 2011).

Brian Gongol, *Privacy as a Property Right* (2006), at http://www.gongol.com/research/economics/privacypropertyright/ (accessed 1 November 2011).

Siobhan Gorman, et al., *Computer Spies Breach Fighter-Jet Project*, Wall Street Journal. (2009), at http://online.wsj.com/article/SB124027491029837401.html (accessed 21 April 2011).

GPS World, *Wayfinder Expands Coverage to Southeast Asia, Africa*. (2008, January 23), at http://lbs.gpsworld.com/gpslbs/LBS+News/Wayfinder-

Expands-Coverage-to-Southeast-Asia-Afric/ArticleStandard/Article/detail/486451?contextCategoryId=44174&searchString=countries (accessed 12 March 2011).

Jennifer Graham, *Saskatchewan Privacy Commissioner Cuts Services Citing Lack of Resources*, The Canadian Press. (2010), at http://www.chroniclejournal.com/includes/datafiles/CP_print.php?id=245484&title=Saskatchewanprivacycommissionercutsservicescitinglackofresources (accessed 22 February 2011).

Paul A Greenberg, *FTC Investigates Amazon, Yahoo!* , E-Commerce Times. (2000, March 31), at http://www.ecommercetimes.com/news/articles2000/000331-3.shtml (accessed 31 March 2011).

Paul A Greenberg, *U.S. Stymied in Online Drug War*, E-Commerce Times. (2000, May 26), at http://www.ecommercetimes.com/news/articles2000/000526-2.shtml (accessed 26 May 2011).

Paul A. Greenberg & Lori Enos, *FTC and DOJ Issue Joint Antitrust Guidelines*, E-Commerce Times. (2000, April 10), at http://www.ecommercetimes.com/news/articles2000/000410-2.shtml (accessed 15 April 2011).

Larry Greenemeier, *International Report: What Impact Is Technology Having on Privacy around the World?*, Scientific American. (2008, August 18), at http://www.scientificamerican.com/article.cfm?id=international-report-technology (accessed 21 July 2011).

Graham Greenleaf, *The European Privacy Directive - Completed*, 2 Privacy Law & Policy Reporter 5, 81-87. (1995), at http://www.austlii.edu.au/au/journals/PLPR/1995/52.html (accessed 3 March 2011).

Graham Greenleaf, *APEC Privacy Principles: More Lite with Every Version*. (2003), at http://www2.austlii.edu.au/~graham/publications/2003/APECv5_article.htm

l (accessed 1 August 2011).

Graham Greenleaf & Nigel Waters, *Direct Marketing Code of Practice Hits ACCC Snag*. (1998), at http://www.austlii.edu.au/au/journals/PLPR/1998/61.html (accessed 31 December 2011).

Alan Greenspan, *Greenspan Admits 'Mistake' that Helped Crisis*. (2008, October 23), at http://www.msnbc.msn.com/id/27335454/ (accessed 24 October 2011).

Chris Greenwood, *Data Protection Act Costs Country £53m Every Year*, The Independent. (2010), at http://www.independent.co.uk/news/uk/politics/data-protection-act-costs-country-pound53m-every-year-2019747.html (accessed 6 July 2011).

Grant Gross, *GAO: Most Sensitive Data on Government Laptops Still Unencrypted*, CompiterWorld. (2008), at http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyId=15&articleId=9110983&intsrc=hm_topic (accessed 30 July 2011).

Grant Gross, *Update: Court Bars Company from Online Sale of Phone Records* InfoWorld. (2008, January 28), at http://www.infoworld.com/article/08/01/28/Court-bars-company-from-online-sale-of-phone-records_1.html (accessed 28 January 2011).

All Party Parliamentary Communications Group, *Can we keep our hands off the net? Report of an Inquiry by the All Party Parliamentary Communications Group*. (2009), at http://www.apcomms.org.uk/uploads/apComms_Final_Report.pdf (accessed 19 October 2011).

Ben Grubb, *McAfee Keeps Leaked Details to Itself: Biggest Companies in Australia on List*, IT New for Australian Business. (2009), at http://www.itnews.com.au/News/151609,mcafee-keeps-leaked-details-to-itself.aspx (accessed 31 July 2011).

Ben Grubb, *Govt Wants ISPs to Record Browsing History*, ZDNet.com.au (2010), at http://www.zdnet.com.au/govt-wants-isps-to-record-browsing-history-

339303785.htm (accessed 12 June 2011).

Gtld-Mou, *Generic Top Level Domain Memorandum of Understanding*. (2003), at http://www.gtld-mou.org/ (accessed 12 June 2011).

Laura J. Gurak, *Logging in with Laura J. Gurak: Minnesota Professor Takes a Critical Look at Online-Privacy Issues*, The Chronicle of Higher Education. (2002 February 19), at http://chronicle.com/free/2002/02/2002021901t.htm (accessed 4 May 2011).

Angel Gurría, *Closing Remarks by Angel Gurría, OECD Ministerial Meeting on the Future of the Internet Economy*. (2008), at http://www.oecd.org/document/8/0,3343,en_2649_34487_40863240_1_1_1_1,00.html (accessed 7 September 2011).

GYU Center, *Most Important Issue Facing the Internet*. (2007), at http://www.why-not.com/company/stats.htm (accessed 23 January 2011).

Barry M. Hager, *Rule of Law*. (2003), at http://www.mcpa.org/rol/core_components.pdf (accessed 7 December 2011).

David P. Hamilton, *Intel Plans to Release Details of Microprocessor Via the Internet*, Wall Street Journal. (2000, May 10), at http://interactive.wsj.com/articles/SB957908075498923116.htm (accessed 1 May 2011).

Mark Hankins, *Ambulance Chasers on the Internet: Regulation of Attorney Web Pages*, 1 Journal of Technology Law and Policy 3 (1996), at http://journal.law.ufl.edu/~techlaw/1/hankins.html (accessed 8 May 2011).

Misty Harris, *The New Social Suicide: Facebook Users Jump Ship Over Privacy Concerns*, Canwest News Service. (2010), at http://www.vancouversun.com/socialsuicideFacebookusersjumpshipoverprivacyconcerns/3024192/story.html (accessed 9 July 2011).

Shane Harris, *TIA Lives On*, National Journal. (2006, February 23), at http://www.nationaljournal.com/about/njweekly/stories/2006/0223nj1.htm (accessed 8 June 2011).

Hawtalk, *UK Government Opposed to the Commission's Data Protection*

Regulation. (2012), at http://amberhawk.typepad.com/amberhawk/other-information-law/ (accessed 12 November 2012).

Jon Healey, *California Firm Develops Single ID for Users of Online Services*. (1999, November 2), at http://www.accessmylibrary.com/comsite5/bin/comsite5.pl?page=library&item_id=0286-5612708&override=Y&zip=92706&authtime= (accessed 9 September 2011).

Health & Human Services, *Code of Fair Information Practices* (1973), at http://aspe.hhs.gov/datacncl/1973privacy/Summary.htm (accessed 30 July 2011).

Helsinki Final Act, *Helsinki Final Act*. (1975), at http://www.hri.org/docs/Helsinki75.html (accessed 24 September 2011).

B. Hiawatha, *Europe's View of Online Privacy*, The Boston Globe. (1998), at http://www.law.wayne.edu/litman/classes/cyber/1998/nov5.html (accessed 22 July 2011).

Hippocrates, *The Classical Hippocratic Oath*. (2005), at http://www.mnsu.edu/emuseum/prehistory/aegean/culture/greekmedicine.html (accessed 20 August 2011).

Afua Hirsch, *Scotland and N Ireland Could Reject Bill of Rights: Proposals to Change the Human Rights Act Could Become a 'Legal and Political Nightmare,' Experts Have Said*, guardian.co.uk. (2010), at http://www.guardian.co.uk/uk/2010/feb/07/northern-ireland-bill-of-rights (accessed 10 August 2011).

Nils Homer, et al., *Resolving Individuals Contributing Trace Amounts of DNA to Highly Complex Mixtures Using High-Density SNP Genotyping Microarrays* 4 PLoS Genetics 8. (2008), at http://www.plosgenetics.org/article/info%3Adoi%2F10.1371%2Fjournal.pgen.1000167 (accessed 3 July 2011).

William E. Hornsby Jr, *The Ethical Boundaries of Selling Legal Services in Cyberspace*. (1996), at http://www.kuesterlaw.com/netethics/abawill.htm (accessed 17 August 2011).

Saffron Howden, *No Place For Crooks to Hide*, Sydney Morning Herald. (2009), at http://innovya.com/2009/12/10/no-place-for-crooks-to-hide/ (accessed 9 December 2011).

Reed E. Hunt, *The Internet: From Here to Ubiquity*. (1997), at http://www.fcc.gov/Speeches/Hundt/spreh742.html (accessed 9 May 2011).

Barry J. Hurewitz, *US - EU Privacy "Safe Harbor" Greeted with Skepticism*, Wilmer Hale. (2001), at http://www.wilmerhale.com/publications/whPubsDetail.aspx?publication=2367 (accessed 22 July 2011).

Alysa Zeltzer Hutnik & Sharon Kim Schiavetti, *The FTC Offers Framework for Facial Recognition Technology*, Acc: Association of Corporate Counsel. (2011), at http://www.lexology.com/library/detail.aspx?g=a93a9908-880c-48cf-b5c6-77b0002cb618 (accessed 12 December 2011).

IAPP, *EU officials discuss proposed data protection reform*. (2012), at https://www.privacyassociation.org/publications/2012_12_01_eu_officials_discuss_proposed_data_protection_reform (accessed 16 November 2012).

Industry Canada, *The Canadian Information Highway: Building Canada's Information and Communications Infrastructure / Privacy*. (1994), at http://www.ifla.org/documents/infopol/canada/cihac003.txt (accessed 1 August 2011).

Information Tribunal, *Tribunal Service: Information Rights*. (2010), at http://www.informationtribunal.gov.uk/aboutus.htm (accessed 14 August 2011).

National Advertising Initiative, *Helping You Protect Your Privacy Online*. (2009), at http://www.networkadvertising.org/ (accessed 16 August 2011).

International Chamber of Commerce, *ICC Report on Binding Corporate Rules for International Transfers of Personal Data*. (2004), at http://www.iccwbo.org/uploadedFiles/ICC/policy/e-business/pages/FINAL_ICC_BCRs_report_rev.pdf (accessed 26

December 2011).

International Chamber of Commerce, *ICC Task Force on Privacy and the Protection of Personal Data: Summary of the Workshop on the Distinction between Data Controllers and Data Processors*. (2007, October 25), at http://www.iccwbo.org/policy/ebitt/id17704/index.html (accessed 15 September 2011).

International Law Dictionary and Directory, *De Facto Government*. (2002), at http://august1.com/pubs/dict/g.htm (accessed 22 May 2011).

International Security Trust and Privacy Alliance, *Analysis of Privacy Principles: Making Privacy Operational*. (2007), at http://www.istpa.org/pdfs/ISTPAAnalysisofPrivacyPrinciplesV2.pdf (accessed 28 July 2011).

Internet Action Plan, *Call for Internet Action Plan*. (2000), at http://www.qlinks.net/iap/howto.html (accessed 5 May 2011).

Internet Corporation for Assigned Names and Numbers (Icann), *History.* (2003), at http://www.icann.org/ (accessed 18 June 2011).

Internet Engineering Task Force (Ietf), *History.* (2003), at http://www.ietf.cnri.reston.va.us/home.html (accessed 2 July 2011).

Internet Fraud Complaint Center, *Welcome to IFCC.* (2003), at https://www.ifccfbi.gov/ (accessed 17 August 2011).

Internet Genome Project, *Internet Genome*. (2000), at http://www.internetgenome.com/map/abridged.htm (accessed 27 May 2011).

Ipsos / Queen's University, *Interviews with 7,088 Adults in Brazil, Canada, France, Hungary, Mexico, Spain and the United States*. (2006), at http://www.angus-reid.com/polls/view/13849 (accessed 3 March 2011).

S Iskandar, *French Courts Curb Web Auctions*, Financial Times. (2000, May 3), at http://news.ft.com/ft/gx.cgi/ftc?pagename=View&c=Article&cid=FT3VYW2AT7C&live=true&useoverridetemplate=IXLZHNNP94C (accessed 7 May 2011).

ISO/IEC, *17799:2005 Information Technology - Security Techniques - Code of Practice for Information Security Management*. (2005), at http://www.iso.org/iso/support/faqs/faqs_widely_used_standards/widely_used_standards_other/information_security.htm (accessed 1 June 2011).

Andrew Jackson, *Presidential Farewell Address*. (1837 March 4), at http://www.presidentialrhetoric.com/historicspeeches/jackson/farewelladdress.html (accessed 29 December 2011).

Jaco Van Der Walt, *Trust and Privacy are the Cornerstones of Successful Relationships between Consumers and Business*. (2003, March 13), at http://www.ey.com/GLOBAL/content.nsf/South_Africa/15_May_03_Trust_And_Privacy (accessed 5 June 2011).

Jeffrey A. Jacobs, *Comparing Regulatory Models -- Self-Regulation vs. Government Regulation: The Contrast between the Regulation of Motion Pictures and Broadcasting may have Implications for Internet Regulation*. (1996), at http://journal.law.ufl.edu/~techlaw/1/jacobs.html (accessed 29 May 2011).

Patricia Jacobus, *Criminal Courts May Not Be the Place for High-Tech Cases*, CNET. (2000, May 1), at http://news.cnet.com/news/0-1005-200-1796137.html?tag=st.ne.1002.bgif.1005-200-1796137 (accessed 15 May 2011).

Jennifer Stoddart, *The Future of Privacy Regulation: Remarks at the 11th Annual Privacy and Security Conference*, Office of the Privacy Commissioner of Canada. (2010), at http://www.priv.gc.ca/speech/2010/sp-d_20100210_e.cfm (accessed 11 February 2011).

Charisse Jones, *States Name Sex Offenders on Net*, USA TODAY. (1999, January 19), at http://sige260.tripod.com/megnet.html (accessed 20 July 2011).

K. C. Jones, *Online Safety, Privacy Tops Parents' Concerns*, Information Week. (2008, July 22), at http://www.informationweek.com/news/security/client/showArticle.jhtml?articleID=209400624 (accessed 22 July 2011).

Bill Joy, *Quoted in Sun Co-founder, Top Scientist Sees Many Webs*, Tech Web. (2000, January 11), at http://www.techweb.com/wire/story/TWB20000111S0009 (accessed 15 May 2011).

UK Ministry Of Justice, *Government Response to the Joseph Rowntree Reform Trust Report: 'Database State'*. (2009), at http://www.justice.gov.uk/publications/docs/government-response-rowntree-illegal-databases-report.pdf (accessed 9 December 2011).

Margaret Kane, *MS Declares War on 'Cyber-Squatters'* ZDNN. (1998, December 30), at http://news.zdnet.com/2100-9595_22-101277.html (accessed 20 July 2011).

Cem Kaner, *Article 2B is Fundamentally Unfair to Mass-Market Software Customers*. (1997), at http://www.badsoftware.com/ali.htm (accessed 11 November 2011).

Carl S. Kaplan, *Governments Learn How to Censor the Internet, Report Says* Cyber Law Journal. (2000, May 5), at http://www.nytimes.com/library/tech/00/05/cyber/cyberlaw/05law.html (accessed 5 May 2011).

D Kelsey, *Colorado Lawmakers OK Anti-Spam Bill*. (2000), at http://www.ecommercetimes.com/news/articles2000/000320-nb2.shtml (accessed 6 June 2011).

Catherine Kelso, *Australia: A Step Towards Harmony in the Regulation of Privacy and Access to Government Information Legal Update*, Mondaq: Government & Public Sector. (2010 March 30), at http://www.mondaq.com/australia/article.asp?articleid=97214&email_access=on (accessed 1 April 2011).

Ross Kerber, *Cost of Data Breach at TJX Soars to $256m: Suits, Computer Fix Add to Expenses*. (2007, August 15), at http://www.boston.com/business/globe/articles/2007/08/15/cost_of_data_breach_at_tjx_soars_to_256m/ (accessed 15 August 2011).

Ross Kerber, *TJX Puts Cost for Breach at $25m So Far*. (2007, May 16), at

http://www.boston.com/business/personalfinance/articles/2007/05/16/tjx_puts_cost_for_breach_at_25m_so_far/ (accessed 2 January 2011).

Suzanna Kerridge, *G8 Nations Paralyzed by Indecision on Cyber Crime* Silicon.com (2000, May 18), at http://management.silicon.com/government/0,39024677,11017542,00.htm (accessed 19 May 2011).

Leo King, *U.K. Justice Agency Lost 45,000 Personal Records in Past Fiscal Year*. (2008, August 18), at http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=storage_security&articleId=9112864&taxonomyId=153&intsrc=kc_top (accessed 18 August 2011).

Leo King, *Call for Data Jail Sentences after Police Wrongly Hand Over Sensitive Information: Information Commissioner Says Fines are not Effective as a Deterrent*, ComputerworldUK. (2009), at http://www.computerworlduk.com/news/it-business/17776/call-for-data-jail-sentences-after-police-wrongly-hand-over-sensitive-information/ (accessed 30 November 2011).

Miya Knights, *Security Professionals Debate the Recommendations of Independent Research to Introduce Tough European Data Breach and Security Regulations*. (2008, October 9), at http://www.itpro.co.uk/606960/security-pros-call-for-data-breach-regulations (accessed 11 October 2011).

Lewis Z. Koch, *Cyberstalking Hype*, Inter@active Week. (2000, May 26), at http://www.lzkoch.com/column_05.html (accessed 26 May 2011).

Munir Kotadia, *ACMA Slams Retailers Over Spam Act Breaches*, SC Magazine For IT Security Professionals. (2009), at http://www.securecomputing.net.au/News/161769,acma-slams-retailers-over-spam-act-breaches.aspx (accessed 1 December 2011).

Brian Krebs, *Data Breaches Have Surpassed Level For All Of '07, Report Finds* Washington Post. (2008, August 26), at http://www.washingtonpost.com/wp-

dyn/content/article/2008/08/25/AR2008082502496.html (accessed 27 August 2011).

Herbert M. Kritzer, *Loser Pays Doesn't*, Legal Affairs. (2005, November), at http://www.polisci.wisc.edu/~kritzer/Research/Law_misc/LegalAffairs2005.pdf (accessed 20 August 2011).

Lucette Lagnado, *Judge Orders Online Laetrile Vendor To Close Shop, Signaling U.S. Stance*, Wall Street Journal. (2000, April 24), at http://interactive.wsj.com/articles/SB956527046745034154.htm (accessed 27 April 2011).

Rama Lakshmi, *India Data Privacy Rules May Be Too Strict for Some U.S. companies*, The Washington Post. (2011 May 23), at http://www.washingtonpost.com/business/india-data-privacy-rules-may-be-too-strict-for-some-us-companies/2011/05/18/AF9QJc8G_story.html (accessed 23 May 2011).

Jill Lawless, *Does DNA Database Unfairly Brand the Innocent?*, San Francisco Chronicle. (2009), at http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2009/09/12/MNDK19L6BK.DTL (accessed 13 September 2011).

Laws of Solon, *Laws of Solon* (594 BCE), at http://www.e-classics.com/solon.htm (accessed 26 September 2011).

D Lawsky, *Court Hands FCC Broadband Victory*, Znet.com. (2000, May 20), at http://www.zdnet.com/zdnn/stories/news/0%2C4586%2C2573296%2C00.html (accessed 5 May 2011).

Barry M. Leiner, et al., *A Brief History of the Internet*. (2003), at http://www.isoc.org/internet/history/brief.shtml (accessed 29 May 2011).

Rob Lemos, *Copyright Clash: Boundaries of Legality*, ZDNet.com. (2000, May 17), at http://www.zdnet.com/zdnn/stories/news/0%2C4586%2C2571669%2C00.html (accessed 29 May 2011).

Dan Lerner, *Internet Spreads its Web to Interactive E-Government*, Ft.com. (2000, May 25), at

http://news.ft.com/ft/gx.cgi/ftc?pagename=View&c=Article&cid=FT3B29BRO8C&live=true&tagid=ZZZ2H6COD0C&Collid=Any (accessed 20 May 2011).

Joe Lewis, *Digital Privacy a Shattered Utopia*. (2006, October 30), at http://www.webpronews.com/topnews/2006/10/30/digital-privacy-a-shattered-utopia (accessed 1 January 2011).

Liberty Alliance, *Privacy Summit*. (2007), at www.projectliberty.org/ liberty/ content/ download/ 3114/ 20838/ file/ Privacy-Summit-Final.pdf (accessed 9 July 2011).

P Lima, *Internet & Mobile Phones Begin to Coverage*, Themestream.com (2000, April 13), at http://www.themestream.com/gspd_browse/browse/view_article.gsp?c_id=42672&id_list=&cookied=T (accessed 1 April 2011).

Liz Tay, *Kirby Crowned International Privacy Champion*, SC Magazine for IT Security Professionals. (2010), at http://www.securecomputing.net.au/News/166776,kirby-crowned-international-privacy-champion.aspx (accessed 9 February 2011).

Dan Long, *Little Brother: How RFIDs in Everyday Objects Could Make Easy Targets for Hackers* SC Magazine for IT Professionals (2009), at http://www.securecomputing.net.au/Feature/150590,little-brother-how-rfids-in-everyday-objects-could-make-easy-targets-for-hackers.aspx (accessed 21 July 2011).

Jim Macdonald, *Alberta Data Hacked: Health, Drivers 'Licence Records Not Well Protected:Top Auditor*. (2008, October 3), at http://www.edmontonsun.com/News/Alberta/2008/10/03/pf-6962041.html (accessed 4 October 2011).

Andrew Macleod, *Sweeping New Powers Would Threaten Privacy: Watchdog*, The Tyee. (2010), at http://thetyee.ca/News/2010/03/25/NewPowers/ (accessed 25 March 2011).

Markle Foundation, *Creating a Trusted Information Network for Homeland Security*. (2003), at http://www.markletaskforce.org/ (accessed 11

January 2011).

Markle Foundation Task Force on National Security in the Information Age, *Mobilizing information to prevent terrorism: Accelerating development information sharing of a trusted environment.* (2006, July), at http://www.markle.org/downloadable_assets/2006_nstf_report3.pdf (accessed 1 December 2011).

Richard Martin, *Carriers Try to Avoid the Warrantless Eavesdropping Spotlight: The Telecoms, Including AT&T, Verizon, and Qwest, Face What AT&T Officials Have Called "A Maelstrom" of Civil Lawsuits Over the Eavesdropping Program*. (2007, November 19), at http://www.informationweek.com/security/showArticle.jhtml?articleID=203103309 (accessed 31 December 2011).

Gary T. Marx, *Privacy and Technology*. (1999), at http://web.mit.edu/gtmarx/www/privantt.html (accessed 9 July 2011).

Prisent Masons, *ICO Urges Clarity on Definition of Personal Data*, Author. (2010), at http://out-law.com/page-11422 (accessed 6 October 2011).

Merrill Matthews, *A Declaration of E-Freedoms*, E-freedom.org. (1999), at http://www.e-freedom.org/freedom/efreepub.nsf/da2f668c463fa9d4852568220030a4fb/bca32d088874987a86256824007412 08?OpenDocument (accessed 23 May 2011).

Suzie May, *A Picture's Worth a Thousand Words*, The Journal Online: The Member's Magazine of the Law Society of Scotland. (2010), at http://www.journalonline.co.uk/Magazine/55-7/1008393.aspx (accessed 19 July 2011).

Caroline E. Mayer, *Web Also Revolutionizing Fake ID*, Washington Post Online. (2000, May 19), at http://chronicle.augusta.com/stories/052000/tec_UX0869-9.shtml (accessed 1 May 2011).

A Mcchesney, *Press Minister Seeks to Regulate Internet*, MoscowTimes.com. (2000, May 24), at

http://www.themoscowtimes.com/stories/2000/05/24/041.html (accessed 20 May 2011).

Raymond Mcconville, *Telcos Show Their Google Envy*. (2008, April 8), at http://www.lightreading.com/document.asp?doc_id=150479&f_src=lightreading_FinancialC%20ontent. (accessed 10 April 2011).

Mccormick Tribune Foundation's Cantigny Conference on Counterterrorism Technology and Privacy, *The Cantigny Principles on Technology, Terrorism, and Privacy* 27 National Security Law Report 1, 14-16. (2005), at http://www.abanet.org/natsecurity/nslr/2005/NSL_Report_2005_02.pdf (accessed 22 September 2011).

Declan Mccullagh, *U.S. to Track Crypto Trails*, Wired News. (2000, May 4), at http://www.wired.com/news/politics/0%2C1283%2C36067%2C00.html (accessed 14 May 2011).

Declan Mccullagh, *COPPA Lets Steam Out of Thomas.*, Wired News. (2000, May 13), at http://www.wired.com/news/politics/0%2C1283%2C36325%2C00.html (accessed 7 May 2011).

Declan Mccullagh, *Filters Kowtowing to Hate?*, Wired News. (2000, May 27), at http://www.wired.com/news/politics/0%2C1283%2C36621%2C00.html (accessed 7 May 2011).

D Mcguire, *ICANN's Dyson Not Aware of GAO Investigation*, Newsbyte. (2000, May 2), at http://www.Infowar.Com/ (accessed 16 May 2011).

D Mcguire, *Another Case Goes Network Solutions' Way*, Newsbyte. (2000, May 9), at http://www.newsbytes.com/pubNews/00/148763.html (accessed 3 May 2011).

D Mcguire, *ICANN Nominating Process Draws Flak*, Newsbyte. (2000, May 12), at http://www.newsbytes.com/pubNews/00/149001.html (accessed 19 May 2011).

Paul Melle, *EC Sets Out Privacy Requirements for Smart RFID Tags*, Computer World. (2009, May 13), at http://computerworld.co.nz/news.nsf/scrt/5EA85E21103475EBCC2575B4

00729F86 (accessed 23 December 2011).

Memorandum of Understanding, *Between the U.S. Department Of Commerce and Internet Corporation for Assigned Names and Numbers*. (1979), at http://www.ntia.doc.gov/ntiahome/domainname/icann-memorandum.htm (accessed 24 November 2011).

Pamela Mendels, *Online Smut Law Heads Into Court*, The New York Times. (1999, January 17), at http://home.pacbell.net/pkykwan/kwanlaw2/reading/COPA.htm (accessed 3 June 2011).

Microsoft, *BackOffice to be Offered Via Rental Pilot Program*, IDG Net. (1998), at http://www.idg.net/crd_microsoft_75870.html (accessed 1 November 2011).

Microsoft, *Microsoft Hints at Windows Rental Again*, The Register. (1999), at http://193.122.103.82/990409-000025.html (accessed 10 November 2011).

H Mintz, *SCU Prof to Settle Fraud Suit in Online University Stock Offer*, SV.com. (2000, May 15), at http://www.mercurycenter.com/svtech/news/indepth/docs/sec051600.htm (accessed 29 May 2011).

Mirapoint.Com., *Mirapoint.* (2000), at http://www.mirapoint.com/company/index.asp (accessed 1 May 2011).

Brandon Mitchener, *European Union Ministers Fail to Resolve Copyright Battle*. (2000, May 26), at http://interactive.wsj.com/articles/SB959285982148008505.htm (accessed 29 May 2011).

William Mitting, *Data Privacy Debate to Come to the Fore, Experts Say*. (2009), at http://www.printweek.com/digital/news/915730/Data-privacy-debate-to-fore-experts-say/ (accessed 25 June 2011).

Model Laws, *Collection of Model Laws*. (2006), at http://www.law.upenn.edu/bll/ulc/ulc.htm (accessed 22 August 2011).

Gordon E. Moore, *Cramming More Components onto Integrated Circuits*, 38

Electronics, 8. (1965, April 19), at http://download.intel.com/research/silicon/moorespaper.pdf (accessed 6 June 2011).

Matt Moore, *ICANN Rejects Creation of '.xxx' Domain*. (2007), at http://www.usatoday.com/tech/news/techpolicy/2007-03-30-icann-xxx_N.htm (accessed 4 April 2011).

Asher Moses, *Web Snooping Policy Shrouded in Secrecy* Sydney Morning Herald. (2010), at http://www.smh.com.au/technology/technology-news/web-snooping-policy-shrouded-in-secrecy-20100617-yi1u.html (accessed 17 June 2011).

Asher Moses, *Google Exposes Government Takedown and Data Requests* Sydney Morning Herald. (2010), at http://www.smh.com.au/technology/technology-news/google-exposes-government-takedown-and-data-requests-20100421-stas.html (accessed 22 April 2011).

M Mosquera, *Feds Create Complaint Site for Internet Fraud*, TechWeb. (2000, May 8), at http://www.techweb.com/wire/story/TWB20000508S0011 (accessed 12 May 2011).

Phil Muncaster, *IE boss calls for more honesty about privacy*, V3.co.uk: All the latest UK technology news, reviews and analysis. (2009), at http://www.v3.co.uk/v3/news/2251656/ie-boss-calls-greater-honesty (accessed 20 October 2011).

N.S.W. Council for Civil Liberties, *Does Australia Violate Human Rights?* (2009), at http://www.nswccl.org.au/issues/hr_violations.php (accessed 1 January 2011).

Ellen Nakashima & Alec Klein, *New Profiling Program Raises Privacy Concerns*. (2007, February 28), at http://www.washingtonpost.com/wp-dyn/content/article/2007/02/27/AR2007022701542.html (accessed 3 December 2011).

National Telecommunications and Information Administration - Department of Commerce, *Elements of Effective Self Regulation for the Protection of*

Privacy and Questions Related to Online Privacy. (1998, June 5), at http://www.ntia.doc.gov/ntiahome/privacy/6_5_98fedreg.htm (accessed 1 June 2011).

Caroline B Ncube, *Watching the Watcher: Recent Developments in Privacy Regulation and Cyber-Surveillance in South Africa* 3 SCRIPTed - A Journal of Law, Technology & Society, 4. 344. (2006), at http://www.law.ed.ac.uk/ahrc/script-ed/vol3-4/ncube.asp (accessed 23 April 2011).

Network Advertising Initiative, *Self-Regulatory Principles for Online Preference Marketing by Network Advertisers*. (1999), at http://www.madmoneyrecap.com/NAI_principles.pdf (accessed 15 April 2011).

Media Awareness Network, *Your Guide to the CSA's Privacy Code*. (2010), at http://www.media-awareness.ca/english/resources/educational/handouts/privacy/csa_privacy_code_guide.cfm (accessed 5 July 2011).

H Newman, *Internet to go beyond home PCs.* (2000, May 11), at http://www.freep.com/money/tech/net11_20000511.htm (accessed 29 May 2011).

Newsedge Corporation, *China to Regulate Online News*, Individual.com. (2000, May 18), at http://www.individual.com/servlet/BuildIssue?mode=topics&content_src=/frames/story.shtml%3fstory=v0516586.6xi%26level3=181%26date=20000518%26inIssue=TRUE (accessed 22 May 2011).

Newsedge Corporation, *Beijing Regulates e-Commerce*, Individual.com. (2000, May 25), at http://www.individual.com/frames/story.shtml?story=v0524162.9xi&level3=181&date=20000525&inIssue=TRUE (accessed 15 May 2011).

Newsedge Corporation, *Access Ruling for British Telecom*, Individual.com (2000, May 29), at http://www.individual.com/servlet/BuildIssue?mode=topics&content_src=/fr

ames/story.shtml%3fstory=b0526125.900%26level3=181%26date=20000529%26inIssue=TRUE (accessed 12 May 2011).

James Niccolai, *AOL Class-Action Suits Pile Up*. (2000), at http://archives.cnn.com/2000/TECH/computing/03/03/aol.suits.idg/ (accessed 23 April 2011).

Jakob Nielsen, *Nielsen's Law of Internet Bandwidth*. (1998), at http://www.useit.com/alertbox/980405.html (accessed 6 June 2011).

Greg Nikolettos, *Kevin Rudd's e-Health Bill Paves the way for PositiveID Human Implantable RFID Microchips*, OEN: OpEdNews. (2010), at http://www.opednews.com/articles/Kevin-Rudd-s-e-Health-bill-by-Greg-Nikolettos-100408-839.html (accessed 26 June 2011).

Helen Nissenbaum, *Protecting Privacy in an Information Age: The Problem of Privacy in Public*, National Academy of Engineering. (2006), at http://onlineethics.org/CMS/computers/compessays/nissprivacy.aspx (accessed 25 July 2011).

Juliet M. Oberding & Terje Norderhaug, *A Separate Jurisdiction for Cyberspace? Emerging Law on the Electronic Frontier*. (1996), at http://jcmc.indiana.edu/vol2/issue1/juris.html (accessed 1 July 2011).

Ciara O'brien, *Data Protection Complaints Soar*. (2007 December 12), at http://www.electricnews.net/article/10123588.html (accessed 26 December 2011).

Kevin J. O'brien, *European Standoff Over Search Engine Data*. (2008, October 5), at http://www.iht.com/articles/2008/10/05/business/privacy06.php?page=1 (accessed 6 November 2011).

Kevin J. O'brien, *Cloud Computing Hits Snag in Europe*, The New York Times. (2010), at http://www.nytimes.com/2010/09/20/technology/20cloud.html?_r=1 (accessed 19 September 2011).

Office of Technology Assessment Act. (OTAA), *Public Law 92-484, 92d Congress, H.R. 10243, October 13, 197292-484.* (1972), at

http://www.ota.nap.edu/act.html (accessed 14 March 2011).

Office of the United States Courts, *Report of the Director of the Administrative Office of the United States Courts on Applications for Orders Authorizing or Approving the Interception of Wire, Oral, or Electronic Communications*. (2007), at http://www.uscourts.gov/wiretap06/2006WT.pdf (accessed 31 December 2011).

Keith Olbermann, *The Death of Habeas Corpus*. (2006), at http://www.msnbc.msn.com/id/15220450/ (accessed 19 May 2011).

Omni-Id, *Why RFID? The Reliability Problem*. (2009), at http://www.omni-id.com/technology/ (accessed 21 April 2011).

Onestat.Com, *Microsoft's Windows Dominates the OS Market on the Web According to OneStat.com*. (2008), at http://www.onestat.com/html/aboutus_pressbox46-operating-systems-market-share.html (accessed 18 August 2011).

On-Line Privacy Alliance, *Guidelines for Online Privacy Policies*. (2003), at http://www.privacyalliance.org/resources/ppguidelines.shtml (accessed 2 August 2011).

Open Government, *Data Protection Tracking Research*. (1997), at http://www.open.gov.uk/dpr/report/%21app.8.pdf (accessed 6 July 2011).

Open Water Solutions, *FCAPS - Is It Enough*. (2005), at http://www.openwatersolutions.com/fcaps.htm (accessed 10 July 2011).

Stephanie Overby, *Offshoring: Preparing for India's Proposed Privacy Rules*, PC Advisor. (2011), at http://www.pcadvisor.co.uk/news/security/3279814/offshoring-preparing-for-indias-proposed-privacy-rules/ (accessed 13 May 2011).

Terry Pedwell, *Academics Ask Privacy Watchdog to Probe Online Profiling Practices*, Canadian Press. (2008, July 28), at http://www.cbc.ca/cp/technology/080728/z072825A.html (accessed 29 July 2011).

M Pennington, *Fearing Dissent, Myanmar's Rulers Block Internet.*, Associated Press. (2000, April 24), at

http://www.techserver.com/noframes/story/0%2C2294%2C500196319-500268430-501373795-0%2C00.html (accessed 20 April 2011).

Nicholas Petreley, *UCITA Could Provide the License to Kill Those Companies that Support It*. (1999), at http://linux.idg.net/crd_software_76072.html (accessed 10 November 2011).

Eric Pfanner, *British Advertising Regulator Making Itself Felt Online*, The New York Times. (2010), at http://www.nytimes.com/2010/09/06/business/media/06cach.html (accessed 5 September 2011).

Pinsent Masons, *World's First Cybercrime Treaty Proposed*, Out-law.com. (2000, May 9), at from http://www.out-law.com/php/page.php3?page_id=worldsfirst957895058 (accessed 29 May 2011).

Pinsent Masons, *Lack of Law for Love Bug Case*, Out-law.com. (2000, May 18), at http://www.out-law.com/php/page.php3?page_id=lackoflawforlove958664327 (accessed 29 May 2011).

Pinsent Masons, *Hustinx: Nameless Data Can Still Be Personal*, Out-law.com. (2008, June 11), at http://www.out-law.com/page-9563 (accessed 12 June 2011).

Pinsent Masons, *Commission Takes UK to Court Over Alleged Privacy Law Failings*, Out-Law.com. (2010), at http://www.out-law.com/page-11409 (accessed 30 September 2011).

Pinsent Masons, *ICO Urges Clarity on Definition of Personal Data*, OUT-LAW News. (2010), at http://out-law.com/page-11422 (accessed 6 October 2011).

Ponemon Institute, *United Kingdom 2009 Annual Study: Cost of a Data Breach*. (2010), at www.encryptionreports.com/download/Ponemon_COB_2009_UK.pdf (accessed 7 February 2011).

Henry Porter, *My Ideal Queen's Speech*, guardian.co.uk. (2010), at

http://www.guardian.co.uk/commentisfree/henryporter/2010/may/05/ideal-queens-speech-manifesto-club (accessed 5 May 2011).

David G. Post, *Governing Cyberspace*, *43 Wayne Law Review,* 155. (1997), at http://www.temple.edu/lawschool/dpost/Governing.html (accessed 23 April 2011).

David G. Post, *Governing Cyberspace, or Where is James Madison When We Need Him*. (1999), at http://www.temple.edu/lawschool/dpost/icann/comment1.html (accessed 28 May 2011).

Chris Pounder, *Why the APEC Privacy Framework is Unlikely to Protect Privacy*. (2007), at http://www.out-law.com/page-8550 (accessed 1 August 2011).

Chris Pounder, *European Court Fines Finland for Data Breach*. (2008, July 25), at http://www.ehealtheurope.net/news/3992/european_court_fines_finland_for_data_breach (accessed 30 July 2011).

Erin Power, *Rethinking Privacy on the "Digital Street"*, Troy Media. (2009), at http://www.troymedia.com/?p=2185 (accessed 13 July 2011).

Canadian Press, *Do-Not-Call Fines Total $73,000; Only $250 Collected*, Metro News. (2010), at http://www.metronews.ca/toronto/local/article/572775--do-not-call-fines-total-73-000-only-250-collected--page0 (accessed 8 July 2011).

Chris Priestly, *United Kingdom: UK Told to Get Tougher on Data Protection Law* Mondaq: Intellectual Property. (2010), at http://www.mondaq.com/article.asp?articleid=106238&email_access=on (accessed 2 August 2011).

Privacy International, *A Race to the Bottom - Privacy Ranking of Internet Service Companies*. (2007), at https://www.privacyinternational.org/article/race-bottom-privacy-ranking-internet-service-companies (accessed 2 June 2011).

Privacy International, *Leading Surveillance Societies in the EU and the World 2007*. (2007, December 28), at

http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559597 (accessed 2 January 2011).

Privacy Protection Study Commission, *Personal Privacy in an Information Society*. (1977), at http://www.epic.org/privacy/ppsc1977report/ (accessed 29 July 2011).

Privacy Rights Clearinghouse, *A Review of the Fair Information Principles: The Foundation of Privacy Public Policy* (2004), at http://www.privacyrights.org/ar/fairinfo.htm (accessed 28 July 2011).

Prnewswire, *Teens have a license for the information superhighway 91% of teens use the internet to surf the web*. (2000), at http://www.individual.com/servlet/BuildIssue?mode=topics&content_src=/frames/story.shtml%3fstory=p0308154.100%26level3=2851%26date=20000309%26inIssue=TRUE (accessed 20 May 2011).

Scarlet Pruitt, *Users Seek Streamlined Online Security*, Network world. (2002), at http://www.networkworld.com/news/2002/0208jupiter.html (accessed 23 January 2011).

Chris Pulham, *United Kingdom: Prior Consent for Cookies - Amendments to the e-Privacy Directive*, Mondaq: IT and Telecoms. (2010), at http://www.mondaq.com/article.asp?articleid=104548 (accessed 5 July 2011).

John S. Quarterman, *Participatory Speech Wins*. (1996), at http://www.mids.org/mn/607/phila.html (accessed 4 December 2011).

Joshua Quittner, *Billions registered: Right now, there are no rules to keep you from owning a bitchin' corporate name as your own Internet address*, Wired. 54 (1994, October), at http://www.wired.com/wired/archive/2.10/mcdonalds_pr.html (accessed 2 July 2011).

Frank J. Ranelli, *Bush Nixes Public Access to EPA Libraries!* (2009), at http://www.opednews.com/articles/opedne_frank_j__060829_bush_nixes_public_ac.htm (accessed 20 January 2011).

Eric S Raymond, *Should Public Policy Support Open-Source Software*, The American Prospect. (2000), at http://www.prospect.org/controversy/open_source/raymond-e-2.html (accessed 9 May 2011).

Eric S. Raymond, et al., *Should Public Policy Support Open-Source Software?*, The American Prospect. (2000, April 3), at http://www.prospect.org/controversy/open_source/band-j-1.html (accessed 13 May 2011).

Viviane Reding, *Securing Personal Data and Fighting Data Breaches*. (2009, October 23), at http://ec.europa.eu/commission_barroso/reding/docs/speeches/2009/brussels-20091023.pdf (accessed 23 December 2011).

Keith Regan, *Yahoo! Blurs the Privacy Line*, E-Commerce Times. (2000, May 15), at http://www.ecommercetimes.com/news/viewpoint2000/view-000515-1.shtml (accessed 29 May 2011).

Robert Reich, *Corporate Power in Overdrive*, New York Times. (2001, March 18), at http://query.nytimes.com/gst/fullpage.html?res=9D04E2DA153DF93BA25750C0A9679C8B63&sec=&spon=&pagewanted=1 (accessed 20 August 2011).

Reporters without Borders, *South Africa*. (2004), at http://www.rsf.org/article.php3?id_article=10728 (accessed 15 January 2011).

Reuters, *SEC Charges Maine Day-Trading Site Operator With Fraud*. (2000), at http://www.digitalmass.com/news/daily/03/20/daytraders.html (accessed 27 May 2011).

Reuters, *Supreme Court Sides With ISP On Liability*. (2000), at http://www.zdnet.com/zdnn/stories/news/0%2C4586%2C2558957%2C00.html (accessed 27 May 2011).

Reuters, *Judge Won't Throw Out Charges Against Tokyo Joe*. (2000), at http://www.mercurycenter.com/svtech/news/breaking/merc/docs/044662.h

tm (accessed 27 May 2011).

Reuters, *France Rejects Nazi Web Suit*, Wired News, May 24. (2000), at http://www.wired.com/news/politics/0%2C1283%2C36554%2C00.html (accessed 27 May 2011).

Tim Richardson, *The Net Could Eat Us All - Archbishop of York*, The Register. (2000, April 10), at http://www.theregister.co.uk/000410-000008.html (accessed 22 May 2011).

James Risen, *Bush Signs Law to Widen Reach for Wiretapping*. (2007, August 6), at http://www.nytimes.com/2007/08/06/washington/06nsa.html?_r=1&ei=5065&en=4e05f95a4b60ac78&ex=1187064000&adxnnl=1&partner=MYWAY&pagewanted=print&adxnnlx=1186420061-viMuQY0XRHigIR/AOABJXA&oref=slogin (accessed 2 January 2011).

Franklin D. Roosevelt, *Message to Congress on the Concentration of Economic Power*. (1938, April 29), at http://informationclearinghouse.info/article12058.htm (accessed 27 July 2011).

Theodore Roosevelt, *Declaration of Principles of the Progressive Party*. (1906), at http://www.pbs.org/wgbh/amex/presidents/26_t_roosevelt/psources/ps_trprogress.html (accessed 4 July 2011).

Marc Rotenberg, *Privacy in the Commercial World: Subcommittee on Commerce, Trade, and Consumer Protection, House Committee on Energy and Commerce*. (2001, March 1), at http://energycommerce.house.gov/reparchives/107/hearings/03012001Hearing43/Rotenberg68.htm (accessed 21 August 2011).

Daniel Roth, *Fraud's Booming in Online Auctions, but Help Is Here bidding adieu*, Fortune. (2000), at http://money.cnn.com/magazines/fortune/fortune_archive/2000/05/29/280618/ (accessed 29 May 2011).

Mark A. Rothstein, *Tougher Laws Needed to Protect Your Genetic Privacy*,

Scientific American. (2008 September), at http://www.scientificamerican.com/article.cfm?id=tougher-laws-needed-to-protect (accessed 21 July 2011).

William Safire, *Goodbye to Privacy*, New York Times Book Review. (2005, April 10), at http://www.nytimes.com/2005/04/10/books/review/10COVERSAFIRE.html?pagewanted=1&ei=5070&en=49fbb1c2cb9f9459&ex=1179806400&adxnnl=0&adxnnlx=1179705411-9uaNPK6CUFqrfYMx736RaA (accessed 20 May 2011).

Pamela Samuelson, *Legally Speaking: Does Information Really Want To Be Licensed?* (1998), at http://sims.berkeley.edu/~pam/papers/acm_2B.html (accessed 20 November 2011).

Pamela Samuelson, *Privacy As Intellectual Property?* (2007), at http://people.ischool.berkeley.edu/~pam/papers/privasip_draft.pdf (accessed 20 July 2011).

B Sandburg, *UCC2B is dead -- Long live UCITA.* (1999), at http://www.lawnewsnet.com/stories/A1807-1999May26.html (accessed 1 October 2011).

Sans Institute, *The 7 Top Management Errors That Lead to Computer Security Vulnerabilities*. (2007), at http://www.sans.org/resources/errors.php (accessed 9 April 2011).

Sans Institute, *SANS Top-20 Internet Security AttackTtargets (2006 Annual Update)*. (2007), at http://www.sans.org/top20/?portal=29fe9b55eaffbdad4b0dc482a1e1e4a5 (accessed 7 April 2011).

Chris Schafer, *Judging the Judges: How Do Supreme Court Judges Rank?*, Canadian Constitution Foundation. (2007), at http://www.canadianconstitutionfoundation.ca/files/pdf/News-Release-PDF-Judging-the-Judges-10-April-2007.pdf (accessed 25 July 2011).

Uli Schmetzer, *Computer? Who Needs It? Japanese Teens Have I-mail*, SeattleTimes.com. (2000, May 29), at

http://seattletimes.nwsource.com/news/nation-world/html98/keit29_20000529.html (accessed 30 May 2011).

Sarah Schmidt, *Canadians Wary of Online Privacy Promises*, National Post. (2010), at http://www.nationalpost.com/news/story.html?id=2482724 (accessed 24 January 2011).

Bruce Schneier, *What Our Top Spy Doesn't Get: Security and Privacy Aren't Opposites*. (2008, January 24), at http://www.wired.com/politics/security/commentary/securitymatters/2008/01/securitymatters_0124?currentPage=all (accessed 24 January 2011).

Bruce Schneier, *The Tech Lab: Bruce Schneier* BBC News. (2009), at http://news.bbc.co.uk/2/hi/technology/7897892.stm (accessed 26 February 2011).

Brigid Schulte, *Student Privacy Spotlighted in VA: Manassas School Board, City Pay in Discrimination Suit; Policies Tightened*. (2008, September 27), at http://www.washingtonpost.com/wp-dyn/content/article/2008/09/26/AR2008092603641.html?sid=ST2008092700733&s_pos= (accessed 27 September 2011).

John Schwartz, *FTC to Propose New Online Privacy Rules*, WashingtonPost.com. (2000, May 20), at http://www.washingtonpost.com/wp-dyn/articles/A39330-2000May20.html (accessed 2 May 2011).

John Schwartz, *Giving the Web a Memory Cost Its Users Privacy*, New York Times. (2001, September 4), at http://www.nytimes.com/2001/09/04/technology/04Cook.html (accessed 10 May 2011).

Treasury Board of Canada Secretariat, *Privacy Impact Assessment Guidelines: A Framework to Manage Privacy Risks*. (2002), at http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paipg-pefrld2-eng.asp (accessed 20 July 2011).

Maricela Segura, *Is Carnivore Devouring Your Privacy?*, 75 Southern California Law Review 231-270. (2001), at http://www-

rcf.usc.edu/~usclrev/pdf/075105.pdf (accessed 12 May 2011).

Jeffrey W. Seifert, *Unlocking the Key to Authority: The Contest Over Encryption Regulation*, 20 *Journal of Conflict Studies,* 1. (2000), at http://journals.hil.unb.ca/index.php/JCS/article/viewArticle/4338/4978#a83 (accessed 10 May 2011).

Kevin Shalvey, *Germany Privacy Agency OK With Google Facial Recognition* Click. (2011), at http://blogs.investors.com/click/index.php/home/60-tech/4045-germany-privacy-agency-ok-at-least-now-with-google-facial- (accessed 21 December 2011).

Kim Bartel Sheehan, *How Public Opinion Polls Define and Circumscribe Online Privacy*, 9 *First Monday*, 7. (2004), at http://www.firstmonday.org/issues/issue9_7/sheehan/ (accessed 24 June 2011).

Natasha Singer, *New Online Privacy Rules for Children*, New York Times. (2012), at http://www.nytimes.com/2012/12/20/technology/ftc-broadens-rules-for-online-privacy-of-children.html?_r=0&adxnnl=1&adxnnlx=1356472268-p+IWhdnIfSnfwJY3miX9tA (accessed 19 December 2012).

Siyabonga Africa, *Privacy Bill Promises Protection*. (2008, October 8), at http://www.itweb.co.za/sections/internet/2008/0810081040.asp?O=F&A=TELECOMS (accessed 9 October 2011).

Joyce Slaton, *Cybersex Visits the Ivory Tower*, Wired news. (2000, May 5), at http://www.wired.com/news/culture/0%2C1284%2C36105%2C00.html (accessed 15 May 2011).

Richard Smith, *Australia: ALRC Report On Australian Privacy Laws*. (2008), at http://www.mondaq.com/australia/article.asp?articleid=64940 (accessed 12 December 2011).

R. Jeffrey Smith, *Report Details Missteps in Data Collection*. (2007, March 10), at http://www.washingtonpost.com/wp-dyn/content/article/2007/03/09/AR2007030902353.html (accessed 2 January 2011).

International Standards for Business Government and Society, *Information Technology*. (2011), at http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_ics_browse.htm?ICS1=35 (accessed 26 December 2011).

Society of Professional Journalists, *Code of Ethics*. (2008), at http://www.spj.org/ethicscode.asp (accessed 26 April 2011).

Software Engineering Institute, *Report*. (1999), at http://www.sei.cmu.edu/ (accessed 14 November 2011).

Solera Networks, *Data Capture Appliances*. (2008), at http://www.soleranetworks.com/solutions/top-ten.php (accessed 1 September 2011).

Alisa Solomon, *The Big Chill*, The Nation. (2003, June 2), at http://www.thenation.com/doc/20030602/solomon (accessed 20 May 2011).

Amanda Sounart, *CMS Hires PricewaterhouseCoopers to Monitor HIPAA Violations*. (2008), at http://www.amnhealthcare.com/News.aspx?ID=17342 (accessed 5 June 2011).

Sources in Legal Disputes, *Published Case Citations to Principles of Corporate Governance, Model Penal Code, and Uniform Commercial Code as of March 15, 1999*. (1999, March 15), at http://207.103.196.3/ali/an99%5Fcit2.htm (accessed 14 November 2011).

Pablo T. Spiller & Svein Ulset, *Why Local Loop Unbundling Fails?*, Nordic Workshop on Transaction Cost Economics in Business Administration. Bergen, Norway June 20 - 21 2003. (2003), at http://mora.rente.nhh.no/conferences/TCEWorkshop2003/papers/Ulset_Spiller.pdf (accessed 2 January 2011).

Kannan Srinivasan, *Technologies competing to offer superfast Internet service*, Associated Press. (2000, May 8), at http://www.startext.net/news/doc/1047/1:HOMEPAGE7/1:HOMEPAGE70508100.html (accessed 8 May 2011).

Staff Reporter, *FTC Issues Guidelines for E-Commerce Ads*, Wall Street Journal. (2000, May 4), at http://interactive.wsj.com/articles/SB957402460160455109.htm (accessed 14 May 2011).

Ronald B. Standler, *Privacy Law in the USA*. (1997), at http://www.rbs2.com/privacy.htm#anchor111111 (accessed 28 November 2011).

Stanford Institute for the Quantitative Study of Society, *InterSurey*. (2000), at http://www.stanford.edu/group/siqss/Press_Release/press_release.html (accessed 11 May 2011).

The Starphoenix, *Citizens Deserve Adequate Funding for Privacy Office*. (2010), at http://www.thestarphoenix.com/citizensdeserveadequatefundingprivacyoffice/2710730/story.html (accessed 22 March 2011).

C Stern, *Justice Department Approves AT&T Buyout of MediaOne*, Washington Post Online. (2000, May 26), at http://www.washingtonpost.com/wp-dyn/articles/A7885-2000May25.html (accessed 2 May 2011).

Gina Marie Stevens, *Privacy: Total Information Awareness Programs and Related Information Access, Collection, and Protection Laws (RL31730)*, U.S. Congressional Research Service. (2003), at http://www.cdt.org/security/usapatriot/030214crs.pdf (accessed 20 July 2011).

Elizabeth Stewart, *MoD Loses Hard Drive Holding Military Personnel Data: Portable Drive Holding Private Details of 100,000 Army, Navy and RAF Personnel Belonged to MoD IT Contractor, EDS*. (2008, October 10), at http://www.guardian.co.uk/uk/2008/oct/10/military-defence (accessed 11 October 2011).

Jennifer Stoddart, *Annual Report to Parliament 2007-2008: Report on the Privacy Act* (2008), at http://www.privcom.gc.ca/information/ar/200708/200708_pa_e.asp (accessed 6 December 2011).

Jennifer Stoddart, *Canada Celebrates Privacy Awareness Week by Helping Businesses Improve Privacy Practices* CNW Telbec. (2009), at http://www.newswire.ca/en/releases/archive/August2008/27/c7355.html (accessed 31 December 2011).

Jennifer Stoddart, *Privacy Guardians Warn Multinationals to Respect Laws*, Office of the Privacy Commissioner of Canada. (2010), at http://priv.gc.ca/media/nr-c/2010/nr-c_100420_e.cfm (accessed 20 April 2011).

Brad Stone, *Student Files are Exposed on Web Site*, New York Times. C1 (2008, August 19), at http://www.nytimes.com/2008/08/19/technology/19review.html (accessed 15 May 2011).

Brad Stone, *Online Age Verification for Children Brings Privacy Worries*. (2008, November 15), at http://www.nytimes.com/2008/11/16/business/16ping.html?_r=1&partner=rss&emc=rss (accessed 17 November 2011).

Martin Stone, *Study Shows 300 Mil Worldwide Web Users*, Newsbytes. (2000, March 22), at http://www.newsbytes.com/pubNews/00/146087.html (accessed 3 March 2011).

Martin Stone, *Clinton, FCC Oppose FTC Privacy Plan* E-Commerce Time (2000, May 24), at http://www.ecommercetimes.com/news/articles2000/000524-nb1.shtml (accessed 3 May 2011).

Jason Straziuso, *Net Registration Sparks Uproar in France*, *SV.com*. (2000, May 23), at http://www.mercurycenter.com/svtech/news/breaking/merc/docs/083274.htm (accessed 29 May 2011).

Subscription-Service.Com, *Internet Business*. (2000), at http://www.subscription-service.com/internet_business.html (accessed 8 May 2011).

Sv.Com, *Real Estate Web Site Shares Drop Sharply After Antitrust Probe Disclosure*. (2000, April 26), at http://www.mercurycenter.com/svtech/news/breaking/merc/docs/064460.h

tm (accessed 29 May 2011).

Sv.Com, *Regulators Take Steps to Halt Profit Claims by 14 Online Firms or Individuals*. (2000, May 1), at http://www.mercurycenter.com/svtech/news/breaking/merc/docs/068652.htm (accessed 29 May 2011).

Sv.Com, *Investigators Hit Snag in Building Case Against `Love Bug' Suspects*. (2000, May 17), at http://www.mercurycenter.com/svtech/news/breaking/merc/docs/015693.htm (accessed 29 May 2011).

Nikki Swartz, *U.S., Canadian Firms Have Different Views of Privacy*. (2004, September 1), at http://www.allbusiness.com/legal/221693-1.html (accessed 17 March 2011).

Mike Swift, *Stanford Study Shows Opting Out of Web Tracking Not So Easy*, Mercury News. (2011), at http://www.mercurynews.com/rss/ci_18524333?source=rss (accessed 25 July 2011).

William F. Swiggart, *Internet Law: A New Arena for Legal Conflict*, The LawyerPages.com. (2000), at http://www.thelawyerpages.com/attorney/article7_frm.htm (accessed 21 June 2011).

Rebecca Sykes & Elizabeth De Bony, *E.U.-U.S. Privacy Deal Rotten, Observers Say*, InfoWorld. (2000, March, 14), at http://www.infoworld.com/articles/en/xml/00/03/14/000314enharbor.xml. (accessed 1 August 2011).

Tampa Bay Business Journal, *Californian Sues Certegy Over Data Theft*. (2007, August 16), at http://tampabay.bizjournals.com/tampabay/stories/2007/08/13/daily45.html (accessed 2 January 2011).

Kazumi Tanaka, *Web Links Can Be Considered Illegal, Osaka Court Judgment Says*, Asia BizTech. (2000, April 7), at http://www.nikkeibp.asiabiztech.com/wcs/leaf?CID=onair/asabt/news/9900

1 (accessed 29 May 2011).

Liz Tay, *Privacy Must Be Addressed, For Innovation's Sake*, IT News For Australian Business. (2009), at http://www.itnews.com.au/News/163197,privacy-must-be-addressed-for-innovations-sake.aspx (accessed 18 December 2011).

Josh Taylor, *Healthcare Identifier Legislation Passes*, ZDNet.com.au. (2010), at http://www.zdnet.com.au/healthcare-identifier-legislation-passes-339304038.htm (accessed 25 June 2011).

John A. Taylor, *Should Public Policy Support Open-Source Software?* (2000), at http://www.prospect.org/controversy/open_source/taylor-j-3.html (accessed 21 May 2011).

Techweb.Com, *Internet2: Up, Running, and Real* (2000, May 5), at http://www.techweb.com/wire/story/TWB20000510S0026 (accessed 10 May 2011).

Carrie Teegardin, *Guess Who Knows How Much You Earn Each Week?*, The Atlanta Journal-Constitution. (2008), at http://www.ajc.com/search/content/business/stories/2008/01/20/worknumber_0120.html (accessed 23 May 2011).

The History Place, *Presidential Impeachment Proceedings*. (2003), at http://www.historyplace.com/unitedstates/impeachments/nixon.htm (accessed 13 December 2011).

M. Theoharis, *E-ethics: Being a Professionally Responsible Attorney in the Age of Iinformation*, Cyber Space Law Journal. December. (1999), at http://www.legalengine.com/ (accessed 3 June 2011).

Patrick Thibodeau, *Mass. Could be Fifth State to Adopt Anti-UCITA law.* (2003, June 4), at http:///www.computerworld.com/softwaretopics/software/story/0,10801,81812,00.html (accessed 24 November 2011).

Iain Thomson, *Bank of New York Loses 12.5 Million Customer Details*, SC Magazine for IT Security Professionals. (2008, September 1), at http://www.securecomputing.net.au/News/121357,bank-of-new-york-

loses-125-million-customer-details.aspx (accessed 1 September 2011).

Iain Thomson, *Google Boss Dismisses Privacy Concerns*. (2009), at http://www.securecomputing.net.au/News/162419,google-boss-dismisses-privacy-concerns.aspx (accessed 10 December 2011).

Suzanne Tindal, *COAG Commits to Health IDs in 2010*. (2009), at http://www.zdnet.com.au/coag-commits-to-health-ids-in-2010-339299911.htm (accessed 8 December 2011).

United States Department Of Transportation, *63 Federal Register 116*. (1998), at http://www.epic.org/privacy/id_cards/dot-idcard-698.html (accessed 17 June 2011).

Treasury Board of Canada, *Regulatory Reform through Regulatory Impact Analysis: The Canadian Experience*. (2008), at http://www.tbs-sct.gc.ca/pubs_pol/dcgpubs/manbetseries/VOL14-1_e.asp (accessed 12 April 2011).

Trips, *Agreement on Trade-Related Aspects of Intellectual Property Rights*. (2003), at http://www.wto.org/english/tratop_e/trips_e/trips_e.htm (accessed 27 November 2011).

Anton Troianovski & Danny Yadron, *U.S. Expands Child Online Privacy Law to Cover Apps, Social Networks* Wall Street Journal. (2012), at http://online.wsj.com/article/SB10001424127887323777204578189430101877770.html (accessed 19 December 2012).

Truste, *TRUSTe*. (2003), at http://www.truste.org/ (accessed 2 June 2011).

Uk Financial Services Authority, *Decision Procedure and Penalties Manual Release 070 Section 6.2* (2007), at http://www.fsa.gov.uk/pubs/hb-releases/rel70/rel70depp.pdf (accessed 7 September 2011).

Information Commissioner Office of The UK, *Privacy Impact Assessment, Version 2*, Author. (2009), at http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/files/PIAhandbookV2.pdf (accessed 3 March 2011).

Uniform Commercial Code, *Uniform Commercial Code*. (2001), at http://www.law.cornell.edu/ucc/ucc.table.html (accessed 22 September

2011).

Uniform Commercial Code, *Articles 1-9.* . (2003), at http://www.law.cornell.edu/ucc/ucc.table.html; Individual state statutes can be linked through see http://www.law.cornell.edu:80/uniform/ucc.html#a2 (accessed 25 November 2011).

Uniform Electronic Transactions Act, *Uniform Electronic Transactions Act.* (1999), at http://www.law.upenn.edu/library/ulc/uecicta/etaam99.htm (accessed 24 November 2011).

University of Strathclyde School of Law, *A Short History of Cyberspace*. (1999), at http://itlaw.law.strath.ac.uk/LLM/dist/telqxq/telsem4.html (accessed 30 May 2011).

David Utter, *Study: Data Breaches Break Consumer Trust*. (2007, April 11), at http://www.securitypronews.com/news/securitynews/spn-45-20070411StudyDataBreachesBreakConsumerTrust.html (accessed 7 December 2011).

Robert Vamosi, *Security Watch: Congress Loves Identity Thieves*. (2005, November 11), at http://reviews.cnet.com/4520-3513-6381707-1.html (accessed 14 August 2011).

J.W.G.D Van Belle, *Data Privacy and Consumer Protection in South African E Commerce*. (2004, October), at http://www.commerce.uct.ac.za/InformationSystems/Research%26Publications/2004.asp (accessed 23 January 2011).

Stephan Van Drake, *Buyers of Tiffany Lamp Claim They're Click-and-Switch Victims*. (2000, May 11), at http://164.109.144.131/cgi-bin/gx.cgi/AppLogic+FTContentServer?pagename=law/View&c=Article&cid=ZZZMF0GI38C&live=true&cst=1&pc=5&pa=0&s=News&ExpIgnore=true&showsummary=0 (accessed 14 May 2011).

Vancouver Sun, *Data Security Breaches Costly, Study Finds*. (2008, July 28), at http://www.canada.com/vancouversun/news/business/story.html?id=f817f849-6dd5-4a6e-8404-f4f6009ff224 (accessed 1 July 2011).

Lisa Vanderwal, *Australia: Proposed Changes to the Privacy Act, and the Privacy*

Act in Action: the Privacy Commissioner's decisions in 2009

Privacy: Who cares? (2010, March 15), at http://mondaq.com/australia/article.asp?articleid=95892 (accessed 17 March 2011).

Hal R. Varian, *The Information Economy: How Much Will Two Bits Be Worth in the Digital Marketplace?* (1996), at http://www.sims.berkeley.edu/~hal/pages/sciam.html (accessed 4 July 2011).

G Venditto, *Lessons from the Starr Report: Democracy Is messy*. (1998), at http://www.internetworld.com/print/1998/09/21/opinion/19980921-target.html?InternetWorld+4308+starr&report (accessed 21 September 2011).

Verizon, *2012 Data Breach Investigations Report*. (2012), at http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf (accessed 29 March 2012).

D. A Vice, *U.S. Launches New Site to Curb Web Fraud* (2000, May 9), at http://www.washingtonpost.com/wp-dyn/articles/A29693-2000May8.html (accessed 9 May 2011).

Jaikumar Vijayan., *Oops! Calif. State Pension Fund Admits Breach of Retiree Data*. (2007, August 22), at http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9032159&intsrc=hm_list (accessed 2 January 2011).

Jaikumar Vijayan., *Forget Hackers; Companies Responsible for Most Data Breaches, Study Says*. (2007, March 10), at http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9013142&intsrc=news_list (accessed 2 January 2011).

Vormetric Inc., *White Paper: California SB 1386 & AB 1950: Implementing Effective Encryption Protection for Personal Information Privacy*. (2005), at http://www.vormetric.com/downloads/SB_1386_AB_1950.pdf (accessed 14 August 2011).

Tas Voutourides, *Privacy Protected by Interception Legalities. Law Society*

Gazette. (2000, November 13), at http://www.lawgazette.co.uk/news/privacy-protected-interception-legalities (accessed 15 May 2011).

A Walrus, *SOAP, or Just a Load of Subs?* (2000, May 12), at http://www.it-director.com/00-05-12-1.html?itde1205 (accessed 12 May 2011).

A Walrus, *Why Not Stop Viruses at Your Company Boundary?* (2000, May 19), at http://www.it-director.com/00-05-19-3.html?itde1905 (accessed 28 May 2011).

Roy Want, *RFID--A Key to Automating Everything*, ScientificAmerican. (2008 August), at http://www.scientificamerican.com/article.cfm?id=rfid-key-automats-everything (accessed 21 July 2011).

Webcom.Com, *Process of Development*. (2003), at http://www.webcom.com/legaled/bkgd.html#_Toc353089109 (accessed 22 July 2011).

Webster Dictionary, *Govern.* (2003), at http://www.m-w.com/cgi-bin/mweb (accessed 12 April 2011).

Mary Hayes Weier, *Wal-Mart Unveils New Customer Privacy Policy*, InformationWeek (2009, July 20), at http://www.informationweek.com/news/security/privacy/showArticle.jhtml?articleID=218501013 (accessed 21 July 2011).

David Weisbrot, *Technology-Neutral Privacy Principles Should Govern Rapidly Developing ICT*. (2008, August 11), at http://www.alrc.gov.au/media/2008/mbn2.pdf (accessed 11 August 2011).

Ellen Whinnett, *All Your Details at Click of a Mouse: Your Personal Details are Being Spied on by Hundreds of Government and Private Agencies as New Technology Sees Data-sharing Reach Record Levels* Sunday Herald Sun. (2009), at http://www.heraldsun.com.au/news/victoria/all-your-details-at-click-of-a-mouse/story-e6frf7kx-1225759387740 (accessed 9 August 2011).

Aoife White, *EU Poll Shows Three Out of Four Europeans Worried about Personal Data Online*. (2008, January 22), at

http://news.theage.com.au/technology/eu-poll-shows-three-out-of-four-europeans-worried-about-personal-data-online-20080122-1nba.html (accessed 22 April 2011).

White House, *Framework for Global Electronic Commerce*. (1997), at http://www.technology.gov/digeconomy/framewrk.htm (accessed 5 August 2011).

The Whitehouse, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*. (2009, May 29), at http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf (accessed 29 May 2011).

The Whitehouse, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*. (2012), at http://www.whitehouse.gov/sites/default/files/privacy-final.pdf (accessed 23 February 2012).

Why-Not.Org, *World Wide Web User Statistics*. (2002), at http://www.why-not.com/company/stats3.htm#GVU6 (accessed 23 January 2011).

John R. Wilke, *Misuse of Routing Technology Becomes a Concern in AOL-Time Investigation*. (2000, May 11), at http://interactive.wsj.com/articles/SB958013973530817636.htm (accessed 22 May 2011).

Chris Williams, *Data Watchdog Jacks Up Charges: Privacy Costs After All*, The Register. (2009), at http://www.theregister.co.uk/2009/10/01/ico_charges/ (accessed 5 October 2011).

Ralph F. Wilson, *How Widespread Is Credit Card Fraud Against Merchants?* (2000), at http://www.wilsonweb.com/wct3/fraud-problem.htm (accessed 12 July 2011).

Brett Winterford, *Two in three Australian companies leak data*, SC Magazine For IT Security Professionals. (2009), at http://www.securecomputing.net.au/News/152610,two-in-three-australian-companies-leak-data.aspx (accessed 11 August 2011).

Wired News, *Yahoo Nazi Sales Protested*. (2000, April 11), at

http://www.wired.com/news/politics/0%2C1283%2C35592%2C00.html\ (accessed 23 April 2011).

Troy Wolverton, *Despite New Policies, Illegal Goods Still on Big Auction Sites*. (2000, April 26), at http://news.cnet.com/news/0-1007-200-1765027.html (accessed 29 May 2011).

Troy Wolverton, *Yahoo Accused of Illegal Video Game*. (2000, March 29), at http://news.cnet.com/news/0-1007-200-1596474.html? (accessed 29 March 2011).

Cara Wood, *Web Users Have False Sense of Security: Truste, TNS*. (2006, December 7), at http://www.dmnews.com/Web-users-have-false-sense-of-security-Truste-TNS/article/93762/ (accessed 26 December 2011).

Wordsmyth, *Govern.* (2003), at http://www.wordsmyth.net/cgi-bin/simplesearch.cgi?matchid=17696&senses=1&retall=1&template=wordsmyth (accessed 1 June 2011).

Working Party, *Working Document on Biometrics. Article 29 - Data Protection Working Party, 12168/02/EN WP 80*. (2003, August 1), at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp80_en.pdf (accessed 1 September 2011).

Working Party, *Opinion 2/2004 on the Adequate Protection of Personal Data Contained in the PNR of Air Passengers to Be Transferred to the United States' Bureau of Customs and Border Protection (US CBP). Article 29 - Data Protection Working Party, 10019/04/EN WP 87*. (2004, January 29), at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp87_en.pdf (accessed 10 September 2011).

World Health Organization, *Risk Assessment - The Programme*. (2008), at www.who.int (accessed 2 March 2011).

Dan Worth, *ICO Wants Power to Bang Up Data Protection Offenders: Privacy Watchdog Also Wants Greater Authority to Investigate Company Procedures*, V3.co.uk. (2010), at http://www.v3.co.uk/v3/news/2271081/ico-outlines-desire-increased

(accessed 6 October 2011).

Ben Worthen, *Why All The Data Breaches? Businesses Just Don't Care*. (2008, September 9), at http://blogs.wsj.com/biztech/2008/09/09/why-all-the-data-breaches-businesses-just-dont-care/ (accessed 9 September 2011).

WSJ.Com, *Two Intel Products Aim to Speed B-to-B Language*. (2000, May 8), at http://interactive.wsj.com/articles/SB957754899342036512.htm (accessed 29 May 2011).

WSJ.Com, *Wine Retailers on the Internet Untangle Web of Vintage Laws*. (2000, May 22), at http://interactive.wsj.com/articles/SB958954682837772353.htm (accessed 29 May 2011).

Tom Young, *Lose Data and You Go To Jail*. (2008, May 8), at http://www.computing.co.uk/computing/news/2216073/lose-jail-3989942 (accessed 10 May 2011).

Tom Zeller, *An Ominous Milestone: 100 Million Data Leaks*. (2006, December 18), at http://www.nytimes.com/2006/12/18/technology/18link.html?_r=1&oref=slogin (accessed 26 December 2011).

Kim Zette, *Voter Privacy Is Gone -- Get Over It*. (2008, January 31), at http://blog.wired.com/27bstroke6/2008/01/voter-privacy-i.html (accessed 3 February 2011).

Jonathan Zittrain, *Lost in the Cloud*, The New York Times. (2009, July 20), at http://www.nytimes.com/2009/07/20/opinion/20zittrain.html?_r=2&partner=rss&emc=rss (accessed 21 July 2011).

Conference Papers

J. N Moore, *The Rule of Law: An Overview*. Paper presented at the Meeting of the U.S./Soviet Conference on the Rule of Law, Moscow & Leningrad (1990 March 19-23).

C Murray & D Mamorek, *Adaptive Management: A Science-Based Approach to*

Managing Ecosystems in the Face of Uncertainty. Paper presented at the meeting of the Fifth International Conference on Science and Management of Protected Areas: Making Ecosystem Based Management Work, Victoria, BC (N. Munro ed., 2003, May 11-16).