LEGAL CONCERNS ARISING FROM THE USE OF CLOUD TECHNOLOGIES

by

Allan Paul Jackson

Submitted in partial fulfilment of the requirements for the degree

Doctor of Laws

in the

Department of Private Law

Faculty of Law

UNIVERSITY OF PRETORIA

Supervisor: Prof SJ Cornelius

October 2017

Declaration of Originality

I, the undersigned, do hereby declare that this thesis, which I submit for the degree of Doctor of Laws in the Faculty of Law at the University of Pretoria, is my own work and has not previously been submitted for a degree at any other university.

I have as best possible, correctly cited and acknowledged all my sources.

SIGNED: _____

ALLAN PAUL JACKSON

DATE:

SUPERVISOR: _____

PROFESSOR STEVE CORNELIUS

DATE:

Plagiarism Agreement

University of Pretoria

Plagiarism policy agreement

The University of Pretoria places great emphasis upon integrity and ethical conduct in the preparation of all written work submitted for academic evaluation.

While academic staff teaches you about referencing techniques and how to avoid plagiarism, you too have a responsibility in this regard. If you are at any stage uncertain as to what is required, you should speak to your lecturer before any written work is submitted.

You are guilty of plagiarism if you copy something from another author's work (e.g. a book, an article or a website) without acknowledging the source and pass it off as your own. In effect, you are stealing something that belongs to someone else. This is not only the case when you copy work word-for-word (verbatim), but also when you submit someone else's work in a slightly altered form (paraphrase) or use a line of argument without acknowledging it. You are not allowed to use work previously produced by another student. You are also not allowed to let anybody copy your work with the intention of passing if off as his/her work.

Students who commit plagiarism will not be given any credit for plagiarised work. The matter may also be referred to the Disciplinary Committee (Students) for a ruling. Plagiarism is regarded as a serious contravention of the University's rules and can lead to expulsion from the University.

The declaration which follows must accompany all written work submitted while you are a student of the University of Pretoria. No written work will be accepted unless the declaration has been completed and attached.

Full names of candidate: ALLAN PAUL JACKSON

Student number: U 15365990

Date: 14 NOVEMBER 2017

Declaration

1. I understand what plagiarism is and am aware of the University's policy in this regard.

Signature of candidate: _____

Signature of supervisor: _____

Summary

THE LEGAL CONCERNS APPLICABLE TO CLOUD TECHNOLOGIES

by

Allan Paul Jackson

Supervisor: Professor S.J. Cornelius

Department: Private Law

University: Pretoria

Degree: Doctorate of Law

The thesis is a study of the Legal concerns arising from the use of cloud technologies. During the research a multi-disciplinary and comparative research methodology was used.

The study examines the emerging legal questions about the issues and challenges of cloud-based technologies. It attempts to tackle the various issues experienced such as data security, personal data protection, intellectual property protection, as well as understanding where the cloud platforms, storage and database centres are located or hosted and the possible legal implications therof.

International sources from disciplines such as the computer sciences, regulators and legal practitioners, who have all presented critical responses to the growing challenges posed by the cloud and how the cloud is regulated, were used. By doing so the legal implications of jurisdiction, information ownership and issues of regulatory control, competition and cross-border data flow regulation were scrutinised.

The thesis is targeted to assist legal practitioners, academics and regulators by presenting a wider realistic view of the issues and challenges being faced. The results provide a first step

towards addressing the legal concerns arising from the use of cloud technologies and help drive the transformation of the legislation applicable for cloud technologies.

Acknowledgements

I am indebted to all the authors of the research material used in this thesis and would like to thank them. I gratefully acknowledge their research, work, comments and opinions, which have provided me with the basis for the preparation of this thesis.

I gratefully acknowledge the use of material from legal cases, products and companies. To present the best possible information, I felt it was relevant to the problem to use the cases, products, or businesses with which the reader would be most familiar.

If there is any similarity of the writing in this thesis to those of others, I do not attempt to take anything away from those works. However, I only wish to provide a broader perspective on the overall subject matter. I also do not intend to represent any of the facts of any case or situation used.

Finally, I wish to acknowledge the invaluable guidance, insights and support provided by my supervisor, Professor S.J. Cornelius.

Contents

Abbreviations

The list of abbreviations used

ADSL	Asymmetrical Digital Subscriber Line
AIPOPI	International Association for the Protection of Intellectual Property
ALRC	Australian Law Reform Commission
AMCHAM	American Chamber of Commerce (Belgium)
AOL	America Online
ASP	Application Service Provider
BCA	Binding Contractual Agreements
BCR	Binding Corporate Rules
BBC	British Broadcasting Corporation
CBDF	Cross-border Data Flows
CBI	Confederation of British Industry
CCIPS	Computer Crime and Intellectual Property Section
CJEU	Court of Justice of the European Union
CLIP	Conflict of Laws in Intellectual Property
CPIL	Code for Private International law
CSP	Cloud Service Provider
CTM	Community Trade Market
DMCA	Digital Millennium Copyright Act
DNA	Deoxyribonucleic Acid
DPR	Data Protection Regulation
DRM	Digital Rights Management
DTI	Department of Trade and Industry
DVD	Digital Video Disc
E-commerce	Electronic Commerce
ECHR	European Convention on Human Rights
ECJ	European Court of Justice
ECTA	Electronic Communications and Transaction Act 25 of 2002
EC	European Commission
EEA	European Economic Area
EFTA	European Free Trade Association
EICTA	European Information and Communications Technology Association
EU	European Union
FEDMA	Federation of European Direct Marketing Associations
FISA	Foreign Intelligence Surveillance Act

FTA	Free Trade Agreement (United States)
GDPR	General Data Protection Regulation
GfK	Global full-service Market
HBO	Home Box Office
IaaS	Infrastructure as a Service
IBM	International Business Systems
ICC	International Chamber of Commerce
ICRT	International Communication Roundtable
IDC	International Data Corporation
IP	Intellectual Property
IPR	Intellectual Property Right
IPs	Internet Protocols
ISP	Internet Service Provider
IT	Information Technology
ITV	International Television
JBCE	Japan Business Council in Europe
KPMG	Klynveld Peat Marwick Goerdeler (accounting firm)
LAN	Local Area Network
NCA	National Credit Act 34 of 2005
NIST	National Institute of Standards and Technology
NRA	National Regulatory Authorities
PaaS	Platform as a Service
PBS	Public Broadcasting Service
PDPR	Proposed Data Protection Regulation
PII	Personally Identifiable Information
PIL	Private International Law
POPI	Protection of Personal Information Act 4 of 2013
ROI	Return on Investment
RSA	Republic of South Africa
SaaS	Software as a Service
SLA	Service Level Agreement
TFEU	Treaty on the Functioning of the European Union
TRIPS	Trade-related Aspects of Intellectual Property Rights
UK	United Kingdom
USA	Unites States of America
USSFTA	United States–Singapore Free Trade Agreement
Web	Worldwide Web

WIPO	World Intellectual Property Organization
WTO	World Trade Organization
XaaS	X as a Service

1. Introduction

[A]s time goes on … the world will realise that at least for Intellectual Property the days of the nation-state are over.

Sir Robin Jacob, former Lord Justice of Appeal (2000).[1]

1.1. Problem Statement

Some of the most curious and at the same time the most challenging aspects of Intellectual Property (IP) is that it is constantly subject to change. While this is a product of various factors including shifts in fashion, cultural change, economic fluctuations, war and global expansion, one of the key reasons why IP law has continually been confronted by the challenge of 'the new' is because it is, and has always been, a creature of innovation and technology development. This has been the case since the development of the telegraph and camera through to wireless radio, tape players, personal computers and now the internet. Technology developments have always driven and shaped IP law and created new types of subject matter. Technology development has also provided new ways to reproduce, distribute and consume IP.[2]

In the traditional international sense, IP instruments such as the Berne Convention for the Protection of Literary and Artistic Works, Paris Act of July 24, 1971, as amended on September 28, 1979,[3] and Paris Convention for the Protection of Industrial Property of March 20, 1883, as amended on September 28, 1979,[4] offer IPRs protection to the interests of private producers of particular types of intellectual creations. The IP system comprises various types of IP protection in the form of patents, copyright and trademarks, each with their relevant requirements as to material content, constraints and rights limitations.[5] The IP system is not a

[1] JACOB, R. Hon. Mr. Justice, (2000) *International Intellectual Property litigation in the next millennium*. Case Western Reserve University. p. 516. http://scholarlycommons.law [Accessed 8 August 2015].
[2] WISEMAN, L. (2012) *Copyright and the challenge of the new*. Wolters Kluwer Information Law Series, 25, Netherlands, p. 1.
[3] *Berne Convention for the Protection of Literary and Artistic Works Paris 1971 (Act of July 24, 1971, as amended on September 28, 1979)* World Intellectual Property Organization. http://www.wipo.int/treaties/ [Access 12 January 2015].
[4] *Paris Convention for the Protection of Industrial Property 1883 (March 20, 1883, as amended on September 28, 1979)* World Intellectual Property Organization. http://www.wipo.int/treaties/. [Accessed 12 January 2015].
[5] *Ibid.*

single entity system; there are at least two aspects shared by each of the protected rights. Firstly, the rights of owners or holders are given 'the right to exclude others from reproducing the protected intellectual creation'. Secondly, the limited private rights granted must be balanced alongside the public's interest in the production and distribution of these intellectual creations.[6]

However, the fast increase in the development of new technologies in the last decade has introduced additional considerations to IP, challenging the legal systems of today. New technologies such as 'Boosted Cloud Computing and Databases' draw attention to the public and their rights within these new technologies.

Cloud computing and its associated systems are now a part of our daily lives, whether it is recognised or not. Mobile phones, personal computers, tablets and other smart devices to access and store data, in conjunction with ever changing software applications provided over the internet is used every day. It is used for creating online personal databases or accessing personal documents, photographs, emails and other information services from around the globe.[7] A vast majority of internet users would be clients of a cloud service provider such as Microsoft, Dropbox, Amazon, Facebook and Google[8] or other cloud service providers offering similar services. Such cloud services accommodate and host the users' innovative materials or work alongside the user's personal data and as such will have an impact on both IPRs and personal data protection rights within the cloud databases.[9]

While cloud service providers offer the conduit for cloud computing services to major commercial organisations and social innovators, it also raises undue concerns around a throng of IP and personal data protection uncertainties outside of the standard protection regimes. This is particularly so with respect to the IP areas of copyright and to a lesser extent on trademark and patent infringements within the cloud. These reservations also point more towards an individual's rights and to personal data protection, security and privacy as well as with increased concerns about cross-border data hosting and third party outsourcing

[6] KLOPPER, H.B. et al. (2011) *Law of Intellectual Property in South Africa*. Cape Town: LexisNexis. p. 433.
[7] GIBSON, K. (2015) *Keeping your secret recipe secret.* NU.IT. http://nu.it-online.co.za/ [Accessed 4 January 2016].
[8] HONG, K. (2014) *Dropbox reaches 300m users, adding on 100m users in just six months*. The next Web. http://thenextWeb.com/insider/ [Accessed 11January 2016].
[9] *European Commission Working Party. (2005) Working document on data protection issues related to Intellectual Property rights*. European Commission. Internal Market Directorate-General. Brussels. http://ec.europa.eu/justice/ [Accessed 14 September 2015].

jurisdictional issues.[10] In conjunction with existing rights, there is also the problem of 'digital rights management' of the rights holder's IP to prevent misuse of protected information such as tracking and tracing of users or monitoring users' preferences, in particular, unique identifiers which stay linked to personal information and processing of personal data.[11] New technologies such as cloud computing and database hosting continues to be one of the least understood legal sectors for cloud service providers, jurists and individual users alike.

Cordell discusses a statement made by Jones, Associate General Counsel for Intellectual Property Policy for Microsoft, who concluded at the 2012 International Association for the Protection of Intellectual Property (AIPOPI) Congress in Seoul, that how cloud IP issues could be resolved is much like "trying to read the tea leaves."[12]

Cloud computing is in itself not new and has been around for several decades. However, with the development of technologies, cloud services have become the 'state-of-the-art' computer user technology of today. Most cloud users have a limited understanding of the architecture, back office services and operations of a cloud system.

Providing a transformed knowledge of the legal aspects of IP and personal data protection in the cloud, the combined complexity of technology and law only intensifies existing legal challenges,[13] prompting legal practitioners to suggest that IP policy is failing to keep pace with Cloud technology developments.[14]

1.2. Legal Questions

Current understanding of legal concerns arising from the use of cloud technologies is 'what law is applicable for IP and personal data protection in the cloud'. The legal understanding remains based on the premise that it is always clear and known where the cloud platforms, storage and database centres are located or hosted. Similarly, 'who is administering and managing the cloud' and 'who is responsible for the security and data protection' seem to

[10] CHEUNG, A.S.Y. and WEBER, R.H. (2015) *Privacy and the legal issues in cloud computing*. Cheltenham: Edward Elgar Publishing.
[11] *European Commission Working Party. (2005) Working document on data protection issues related to Intellectual Property rights*. European Commission. Internal Market Directorate-General. Brussels. http://ec.europa.eu/justice/ [Accessed 14 September 2015].
[12] CORDELL, N. (2013) *Intellectual property in the cloud*. Allen and Overy. http://www.allenovery.com/ [Accessed 4 January 2016].
[13] *Ibid.*
[14] SMITH, B. (2010) *Cloud computing for business and society at the Brookings Institution*. Brookings Institution. Http://www.brookings.edu/ [Accessed 23 May 2015].

leave cloud service providers in conflict with this premise.[15] A basic illustration of this understanding would be an email service hosted in the cloud, for example a service such as Google's Gmail. Here Google, being a large everyday service provider, has host platforms and data storage facilities dispersed across several platform locations and depending on the user's access location, the email service may span across various country locations.

In addition, cloud service providers frequently utilise third-party services, which are invariably located in countries which do not have sufficient IP laws and in some cases may not have a competent jurisdictional capability. It should also be noted that data in the cloud is continually moving in a virtual world making it almost impossible to extricate the exact position of the data and its location or in which jurisdiction it may fall for ensuring the proper protection of the users' data.[16]

A number of legal questions arise as a consequence of the virtual method of the information placed in the cloud and on the data subject's information. For instance, questions related to the regional location of the cloud platform, the type of security for the data and how is the cloud users' IP and personal data protected? Furthermore, where there is the added complexity of cross-border transmissions, which territory becomes the host and who then has jurisdiction? Similarly, does the law of the host country involved offer protection for the data in the cloud? Question of this nature have a direct link to the legal challenges concerning IP and personal data protection in the cloud, as well as delictual[17] and criminal liability[18] for breaches of the cloud.

1.3. Assumptions

Based on topical readings it is reasonable to assume that there are numerous legal concerns regarding personal data protection and IP rights in cloud technologies, and that the applicable law for cloud technologies is not always clearly understood. Moreover, the rapid development of technologies makes it more challenging to know how the laws are to be applied. Likewise, given the compound archetype of cloud networks, it is reasonable to assume that multiple

[15] BULLER, D.J. and WITTOW, M.H. (2010) *Cloud computing: Emerging legal issues, data flows, the mobile user*. K and L Gates. http://www.klgates.com/ [Accessed 13 June 2015].
[16] NARAYANAN, V. (2012) *Harnessing the cloud: International law implications of cloud computing*. Journal of Internet Law, 14 (1). Research Gate. https://www.researchgate.net/ [Accessed 13 June 2015].
[17] MARCHINI, R. (2015) *Cloud computing. A practical introduction to the legal issues. 2nd ed*. London: BSI Standards Limited.
[18] WIDMER, U. (2009) *Telecommunications Media & Technology. Cloud computing – ICT as a service*. Who's Who Legal. http://whoswholegal.com/ [Accessed 4 May 2015].

territories would form part of the operations of a cloud network. Furthermore, it is also reasonable to assume that the equivalent or related personal data protection and IP laws for each territory involved with the cloud networks, may not always provide adequate legal protection for the cloud databases.[19]

1.4. Motivation

With an ever increasing amount of cybercrime and personal data infringement across the web, a greater number of concerns have been and still are expressed on the legal issues surrounding cloud technologies, in particular, cloud services and databases with specific emphasis on IP security and personal data protection.[20]

Earlier studies have highlighted a paucity in the appreciation of the legal concerns arising from the use of cloud technologies and the applicable law. Which has provided the motivation to explore the IP and personal data protection laws applicable in South Africa against the related applicable international rules and standards which apply to cloud technologies at a global level. Furthermore it is important to establish whether the current laws are sufficiently future proof to address the legal concerns as well as provide adequate protection for IP and personal data rights in cloud technologies.[21]

1.5. Methodology and Approach

A desktop study was conducted to examine the problem questions with the objective of identifying the applicable law for IP and personal data protection of cloud technologies. Furthermore, to provide a technical overview of the various types of commonly used services offered by cloud service providers and to offer a background understanding of the functionality and characteristics of cloud technologies and the related operational aspects of the networks. Moreover to present a quantifiable point to be used as a measure when considering the IP and personal data protection concerns and the related laws.

---

[19] SCOTT, R.J. (2012) *Understanding the legal risks of cloud computing. Navigating the network security and data privacy issues associated with cloud services*. Thomas Reuters Aspatore. https://www.scottandscottllp.com/ [Accessed 15 May 2015].

[20] HOOVER, J.N. (2013) *Compliance in the ether: Cloud computing, data security and business regulation*. Journal of Business & Technology Law, 8, No. 1, Article 18. Digital Commons. http://digitalcommons.law [Accessed 12 May 2015].

[21] ISRAELY, A. (2013) *Trends and applications. Big data poses legal issues and risks, database trends and applications*. dbta. http://www.dbta.com/Editorial/ [Accessed 4 May 2015].

The research focused on present-day IP mainly on copyright personal data protection laws of the European Union (EU), inclusive of the United Kingdom, the United States of America (USA), as these regions have large established global cloud service providers. In addition, these regions have developed laws more appropriate to the topical matter. These jurisdictions are considered, with a comparative aspect against the similar laws of the Republic of South Africa (RSA), taking into account the difference in the legal systems and technical development for each region. In addition, contributions of relevant laws, regulations and case support from countries such as Australia and Singapore and to the level of protection is afforded to cloud technologies.[22] Together with an overview of the jurisdictional issues of the related territorial laws and cross-border activities.

A broad approach to private international regulations and principles was used to provide support to the legal questions raised surrounding jurisdiction and cross-border complexities of cloud technologies. The study merely provides a high level overview of the typical of issues that may be experiencd when dealing with cloud technologies. A more complex study of these related private international laws would need to be undertaken in order to provide a more indepth clear undertanding of the complexities involved. Such study does not form part of this thesis.

A narrow approach to IP copyright and personal data protection in cloud technologies was taken. An effort was made to expose the gaps or differences and identify shortfalls in the law,[23] also taking into account international laws and regulation of personal data protection and IP rights.

[22] NARAYANAN, V. (2012) *Harnessing the cloud: International law implications of cloud computing*. Research Gate. https://www.researchgate.net/ [Accessed 13 June 2015].
[23] HOOVER, J.N. (2013) Compliance in the ether: Cloud computing, data security and business regulation. *Journal of Business & Technology Law*, 8 (1), Art. 18. Digital Commons. http://digitalcommons.law [Accessed 12 May 2015].

2. Cloud Technical Description

2.1. Introduction

Cloud Computing Services, Characteristics and Basic Terms

The cloud is a distinct term used in the information technologies arena (referred to as IT) and conceived as a metaphor, primarily designed for remote utilisation or virtual IT resources. These IT resources can be scalable and provisioned to suit the user's requirements. An important aspect about the cloud is that it should not be confused with the internet, which is an open access web-based platform. Most cloud services are privately owned and offer access to metered IT services. There is also a new increasing trend of providing cloud services to the public.[1] Cloud services are delivered by way of an IT platform for software and other supplementary applications are provided via remote file servers across the internet on a requirements basis.[2]

The service is offered to replace the storing and accessing of software and data on the user's desktop computer, mobile or another smart device, for example handphones or tablets. The user's software plus data will then reside on a remote server and will be accessible from wherever the user happens to be or can gain access to the network.[3] The resources accommodated in the cloud are commonly dedicated to the supply of so-called 'back-end' services and capability, predominantly user-based or specified. Unlike the internet, cloud services are not always web-based, even though they commonly use internet protocols (referred to as IPs within the technical description) and other technology protocol standards which allow the user remote access to the cloud resources. The cloud resources are usually deployed across businesses, organisations and other network service providers in various ways. These services are typically presented in the following two traditional methods:

1. Private cloud, deployed within a business or organisation using their infrastructure;

---

[1] THOMAS, E. PUTTINI, R. and ZAIGHAM, M. (2013) *Cloud computing: Concepts technology & architecture*. Cape Town: The Prentice Hall Services Technology Series.

[2] MARTIN, T.D. (2010) *Hey! You! Get off my cloud: Defining and protecting the metes and bounds of privacy, security and property in cloud computing*. Journal of the Patent & Trademark Office Society. Selected Works. https://works.bepress.com/ [Accessed 13 June 2015].

[3] SMITH, B. (2010) *Cloud computing for business and society at the Brookings Institution*. Brookings Institution. http://www.brookings.edu/ [Accessed 23 May 2015].

2. Public cloud offered through a platform for fee-based and advertiser supported services available over the internet.[4]

The cloud service providers mainly provide services in three sub-groups namely

a) 'Software-as-a-Service' (referred to as SaaS): business applications, client relations and support, Human Resources, finance, online payments and electronic marketplace for mini, small and medium-sized enterprises.
b) 'Platform-as-a-Service' (referred to as PaaS): platform for cloud computing service provision, client service management and billing.
c) 'Infrastructure-as-a-Service' (referred to as IaaS): virtual on-demand server, virtual data centre, flexible on-demand storage space and flexible local area networks (LAN), firewalls and security services.[5]

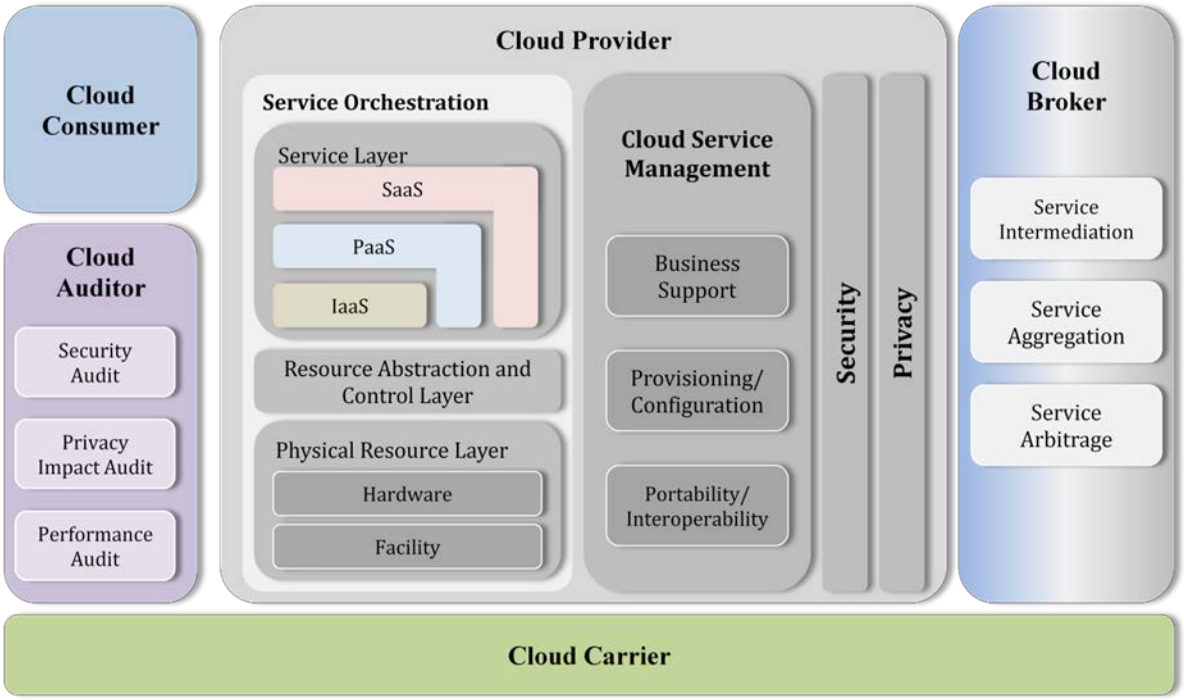

Figure 1: The National Institute of Standards and Technology (NIST) Reference Model.[6]

As per Figure 1, the reference model for cloud architecture defines five major players in the delivery process: the cloud consumer, cloud service provider, cloud carrier, cloud auditor and

[4] MAXEY, M. (2008) *Cloud computing public or private? How to choose cloud storage*. Sys-con Media. http://mikemaxey.sys-con.com/ [Accessed 25 May 2015].
[5] Cloud Security Alliance. (2011) *Security guidance for critical areas of focus in cloud computing V3.0*, Cloud Security Alliance CSA. https://cloudsecurityalliance.org/ [Accessed 15 December 2015].
[6] National Institute of Standards and Technology. (2011) *Cloud computing reference architecture*, NIST. http://www.nist.gov/customcf/ [Accessed 15 February 2016].

the cloud broker. Each of the players is an entity, person or an organisation that participates in a transaction or process and performs tasks within the cloud.[7]

The most important aspects about the cloud are the challenges and risks associated with the services offered. The private cloud services may have fewer risks and difficulties than the public cloud services. An indication of some of the primary risk and challenge areas inherent in the public cloud include personal data protection, digital operational management, increased security vulnerability and cross-border movement, together with data portability of IT resources.

All these difficulties and risks pertain to trust boundaries in shared resources and are more particularly related to the cloud services platforms. A more pressing challenge is to understand the operational activities associated with cloud, in particular data protection and security. These can include cloud platforms across multiple countries and various legal systems, especially when utilising third-party providers who operate platforms in non-allied countries. Cloud computing raises important questions concerning security, privacy and data protection management in conjunction with legal jurisdiction,[8] as well as understanding the governance policies of the country of the cloud service provider and its legislature. These concerns are echoed by policy makers and industry leaders,[9] furthering the 'legal debate' on the risks and challenges within cloud databases.[10]

2.2. How Cloud Computing Works

A cloud service is a computer-based platform capable of delivering application software services and supplemental applications over remote file servers. Instead of keeping data and large software programs on a computer, mobile device or tablet such data and software would be hosted on a remote server and be accessible wherever there are services provided.[11] The cloud may be deployed in either of the two ways mentioned above, privately within and

[7] *Ibid.*
[8] SMITH, B. (2010) *Cloud computing for business and society at the Brookings Institution*. Brookings Institution. http://www.brookings.edu/ [Accessed 23 May 2015].
[9] *Ibid.*
[10] MARTIN, T.D. (2010) *Hey! You! Get off my cloud: Defining and protecting the metes and bounds of privacy, security and property in cloud computing*. .Selected Works. https://works.bepress.com/ [Accessed 13 June 2015].
[11] SMITH, B. (2010) *Cloud computing for business and society at the Brookings Institution*. Brookings Institution. http://www.brookings.edu/ [Accessed 23 May 2015].

organisation or publicly. Private cloud is a closed platform and only accessible within the establishment in which it is has been set up.[12]

The public cloud is open and divided into three main segments: SaaS, PaaS and IaaS.[13]

2.2.1. The view of SaaS

The Software-as-a-Service (SaaS) cloud service is the most frequently used service that is seen in public networks and is the simplest of the cloud services to view. Commonly used in services such as Facebook, YouTube, Webmail and electronic commerce (e-commerce) sites such as Amazon and gaming sites. The SaaS services also appear in legal research sites such as LexisNexis and Westlaw.[14] The SaaS services in cases such as these are usually with the end-user, which is a development away from the software delivery application services seen in the early Dot-com years of the late 1990s. The service providers and vendors at that time, commonly referred to as Application Service Providers (referred to as ASPs)[15] used the internet as a medium to deliver their applications as broadband services were not yet available at the time.

The applications offered were simple transactions such as purchasing a book or music compact disc.[16] With the advent of broadband services and the development of cloud-based services, the ASP services have taken on a new approach to delivering software application and web-based services through the use of SaaS. The SaaS model allows the end-user to interact directly with the vendors through the online service providers[17] who provide the necessary software and remote data storage facilities. The remote data storage facility may have several ways of storing the end-user data. The primary method is the creation of various databases for vendors' use and databases for individual use. These databases may host a

[12] Information Systems Audit and Control Association. (2011) *IT control objectives for cloud computing: Controls and assurance in the cloud.* ISACA. http://www.isaca.org/ [Accessed 12 February 2016].
[13] *Ibid.*
[14] SMITH, B. (2010) *Cloud computing for business and society at the Brookings Institution*. Brookings Institution. http://www.brookings.edu/ [Accessed 23 May 2015].
[15] PETRO, N. (2007) *Software as a Service*. GP Solo Magazine. http://www.americanbar.org/ [Accessed 27 November 2015].
[16] *Ibid.*
[17] SMITH, B. (2010) *Cloud computing for business and society at the Brookings Institution.* Brookings Institution. http://www.brookings.edu/ [Accessed 23 May 2015].

variety of documents from sales records, personal online identity, financial information such as credit card data as well as accounting records and legal documents.[18]

The SaaS services have made it possible for a new business to grow as the service now unlocks valuable IT resources such as database management, email, accounting and sales applications, which were previously a financial burden to start up a business. New SaaS services can run through a simple peer-to-peer network with a broadband internet connection and a low-cost desktop computer.[19] Using the SaaS model allows the end-user the opportunity to pay for software and technical support on a monthly basis. This includes hassle free regular software and security upgrades and updates as well as immediate expansion capability on demand, making it considerably cheaper than investing in software and server hardware packages.

However, there are still risks and challenges to the use of cloud and SaaS. The main risk attached to some degree is the user not having direct control of his data as much of the data is stored in unknown locations within the cloud, especially if the data deals with confidential or other sensitive information. In addition, there is limited control over the security, particularly the operational safe keeping of the service provider or vendor. These risks remain even if there is a strong Service Level Agreement (referred to as SLA) in place. Other risks involve the operational downtime and the SaaS service provider's ability to keep the service running, even worse, if the service provider closes down or goes out of business. Any of these events would leave the business exposed and in some cases may even cause permanent damage from irretrievable data loss.

2.2.2. The view of PaaS

The next level in the cloud service offerings is Platform-as-a-Service (PaaS), which, goes a step beyond the SaaS services. PaaS services are for businesses, organisations and individuals who wish to provide their software applications to end-users across the internet. The PaaS cloud service is the platform that offers a model of business which requires more technical input from the end-user side. There is also a need to provide programmers and technical support as well as some network administration. As with the SaaS services, there is a need to provide desktop computers, an office network as well as a broadband connection to

[18] KENNEDY, D. (2009) *Working in the cloud*. ABA Journal. http://www.abajournal.com/ [Accessed 27 November 2015].
[19] Cloud Security Alliance. (2011) *Security guidance for critical areas of focus in cloud computing V3.0*, Cloud Security Alliance CSA, https://cloudsecurityalliance.org/ [Accessed 15 December 2015].

the internet. It has the same requirements as for setting up a small law practice or business. Setting up and maintaining your website and database to provide the new services and applications, which are timely and not cost effective, or by using the PaaS services in cloud is done in the same manner as Microsoft and Amazon.[20] With PaaS the business, organisation or individual can develop their applications and deploy the services on a service provider platform in the cloud. End-users would have no idea as to who is hosting the website service or applications and it would operate in the same manner as the SaaS application. The in-house developers and programmers will be able to develop and release applications through the service provider's PaaS development tools and cloud service. The PaaS services mainly provide web servers, data-storage capabilities, user authentication, backup facilities, accounting and other administration services. The PaaS service is there to assist businesses in developing and maintaining their applications as opposed to having resources performing secondary operational tasks. The use of PaaS also allows a company to scale resources to the firm's needs, taking into account growth by easily adding storage capacity, web capacity by just uploading new configuration files to the cloud service. The scaling up may also apply through changes made on the end-user control panel of the service provider, much in the same way as the SaaS applications. PaaS requires a 'pay-as-you-go' service. PaaS services may be payable in different ways, either by the amount of storage or by the amount of computing power utilised. In some instances, PaaS services may be charged according to client traffic.[21]

However, there are also risks and challenges to the use of PaaS. As with SaaS, there are the risks related to SLAs, security, data protection and data management. PaaS has additional service provider technical concerns[22] as well as extra-contractual items. On the technical aspect, there is more exposure related to your software applications as well as the service provider's software which could fail or cause security concerns and downtime as the business will be limited to the PaaS service provider's development tools. Depending on the contractual aspect, a business may also not be able to take advantage of third-party software or services to supplement the applications if there are complications and that the service provider provides the cloud environment for the software and operating system and services. This makes it

[20] BAUDIN, C. et al. (2015) *Practical guide to Platform as a Service PaaS*. Cloud Standards Customer Council. CSCC. http://www.Cloud-council.org/ [Accessed 15 February 2016].
[21] Information Systems Audit and Control Association. (2011) *IT control objectives for cloud computing: Controls and assurance in the cloud*. ISACA. http://www.isaca.org/ [Accessed 12 February 2016].
[22] Cloud Security Alliance. (2011) S*ecurity guidance for critical areas of focus in cloud computing V3.0*, Cloud Security Alliance CSA. https://cloudsecurityalliance.org/ [Accessed 15 December 2015].

difficult to change PaaS service providers quickly or easily creating a high dependency on the service provider which could be devastating to the business if the service provider changes development tools, the runtime environment or simply closes down.[23]

2.2.3. The view of IaaS

The third cloud service which is offered by service providers is known as Infrastructure-as-a-Service (IaaS). This service provides extended storage, development tooling and computing power, which allows the end-user to compete with larger online providers such as LexisNexis and Westlaw[24] without the financial outlay for infrastructure development. The development in IaaS requires more effort and is also more technically demanding. The technology for the creation of successful products is intricate and the architecture used has that much more computing power and data platforms.[25] If a business or organisation were to provide this type of service by itself, it would require large-scale data storage and industrial-scale computing power together with a dexterous internet interface to deliver efficient services to clients.

IT infrastructure is extremely complex and costly, which would also require a significant amount of technical and operational staff to keep the network running. Networks at this level have additional aspects to consider over those of the SaaS and PaaS systems. Examples are where the platforms are located and housed, cable and wiring of the compound IT architecture, power supplies, fool-proof services, backup power, industrial size air-conditioning, fire protection systems, constant software and security updates and license renewals, together with a network performance monitoring system. There is also the question of network bandwidth and what capacity would be required, which is an unforgiving moving target when the business is moving forward. All these aspects would be necessary to keep the system operational and the network safe.[26]

Service providers in the cloud offer IaaS as a complete service including data centres. Unlike the SaaS and PaaS services, the IaaS service does not limit the development tool or the run-time environment. The IaaS service allows for the creation of a virtual platform to a set of specifications defined for the business with a focus on the development and run-time environment. These services are established by the service provider in the same manner as

[23] *Ibid.*
[24] SMITH, B. (2010) *Cloud computing for business and society at the Brookings Institution*. Brookings Institution. http://www.brookings.edu/ [Accessed 23 May 2015].
[25] SEAGATE. (n.d.) *Data centre management: Trends and challenges*, SEAGATE. http://www.seagate.com/ [Accessed 16 January 2016].
[26] *Ibid.*

if the corporation had procured the hardware and software services for themselves.[27] Like the PaaS, IaaS allows for the scaling of resources according to the corporate needs. IaaS also provides for specific operating systems, database systems and web servers for corporate applications. The service provider will continue with all the other ancillary services, such as back-up, authentication, data centre management and administration, which the corporate will not be required to do. The IaaS services follow the same pay-as-you-go PaaS model, which is dependent on the amount of storage, bandwidth and computing power required.

The risks involved with SaaS and PaaS are also part of the risks within IaaS. However, there is a difference in the development tool and runtime environment. IaaS does not have the particular run-time lock-in problem as the other two services, which would allow the business to change cloud service providers if and when the need arose. The development tool is the responsibility of the corporate and not the cloud service provider making it simpler to move between cloud service providers. The IaaS cloud service provider is still accountable for the rest of the IaaS service requirements related to software, hardware and operational maintenance as well as ensuring the presence of the web applications. An added risk comes with the complexity and control gained when specifying the businesses' configuration requirements, thereby releasing the cloud service provider directly from this obligation. The risk associated with the corporate now has to provide their SLA to their clients or a performance guarantee. The performance assurance would include the same items such as uptime, quality of performance, incident management, escalation and penalties,[28] the same as a service provider would typically offer its clients in an SLA.

The benefits of using cloud computing are likely to outweigh the challenges and risks due to a view of a significant return on investment (referred to as ROI) coupled to a drastic reduction in hardware and software investment, maintenance and management.[29]

2.2.1. Cloud Computing, Definitions and Features

[27] Information Systems Audit and Control Association. (2011) *IT control objectives for cloud computing: Controls and assurance in the cloud*. ISACA. http://www.isaca.org/ [Accessed 12 February 2016].
[28] Cloud Security Alliance. (2011) *Security guidance for critical areas of focus in cloud computing V3.0*, Cloud Security Alliance CSA. https://cloudsecurityalliance.org/ [Accessed 15 December 2015].
[29] European Network and Information Security Agency. (2012) *Cloud computing benefits, risks and recommendations for information security rev b*. ENISA. http://www.bing.com/ [Accessed 16 January 2016].

The advancement of the internet and the widespread adoption of virtualised technology has brought cloud-based computing to the forefront. To understand and tackle the security concerns in the cloud it is best to set off by explaining the meaning of cloud computing definitions and features. The National Institute of Standards and Technology (NIST) of the USA, has gained considerable recognition for its translation and official guidelines on cloud computing.[30] Apart from the base definition of cloud provided by the NIST, there are five essential characteristics embedded in the definition, which requires some consideration. These are: a) on-demand self-service, b) broad network access, c) resource pooling and location independence, d) rapid elasticity and e) measured services.[31]

The *on-demand self-service* feature empowers the end user to control and manage the IT resource provisioning directly. The service provides access to different cloud services as and when the end-users require them. *Broad network access* allows the end-user to manage and control their cloud environment through a broad network access or a web browser, irrespective of their location; typically access can be gained through personal computers, laptops, smartphones or other such devices. Therefore, the service becomes *location independent* and enables the users to work 'over-the-cloud'. The third characteristic is *resource pooling and location independence,* which is an essential aspect of the cloud platform environment, as it caters for the efficient use of resource sharing among multiple users and customers from around the world in different data centres. It is more commonly referred to as multi-tenancy in larger cloud systems, where users can share costs and resources within a single system, making cloud systems more cost effective.[32] The fourth support aspect, *rapid elasticity,* works in areas where the hardware resources are expected to be shared and provisioned in real-time when required. The end-user can seamlessly utilise resources on demand and not have any part of the service affected. In fact, cloud systems have been designed to function with elasticity, scalability and customisation to meet such needs and demands, making resources appear to be virtually unlimited.

In the cloud environment, choices and options for users can be built into software platforms, whereas the cloud service providers can profit from the 'economies of scale.'[33] The last essential characteristic is *measured services*, which translated in simple terms, means that

[30] National Institute of Standards and Technology. (2011) *The NIST definition of cloud computing SP 800 – 145*. CSRC. http://csrc.nist.gov/ [Accessed 28 November 2015].
[31] *Ibid.*
[32] SLUIJS, J., LAROUCHE, P. and SAUTER, W. (2012b) *Cloud computing in the EU policy sphere interoperability, vertical integration and the internal market.* Tilburg Law and Economics Center (TILEC). https://www.jipitec.eu/ [Accessed 24 February 2016]. par.14.
[33] *Ibid.*

any cloud systems element, such as computation power, storage medium and IT device can be converted into a measurable charging plan or structure. Cloud service providers then have control over both the storage and infrastructure and depending on the delivery model and SLAs' set up with end-users, the end-users will have to pay for the services according to the service charge plan.

2.3. Advantages and Benefits of the Cloud

Cloud computing has significant benefits[34] based on the operational diversity. Through the cloud, users can access the applications and data from anywhere across the globe where there is network connectivity at any time they choose. The cloud also enhances the users' capability to collaborate and cooperate with others.[35] Cloud service providers also provide decentralised data providing better redundancy and thus less vulnerability to natural and human-made disasters.[36] Cloud service providers have skilled specialists to handle security, maintenance and system issues. The cloud offers rapid, intelligent and adjustable resources coupled with economies of scale as and when needed. However, cloud computing encounters hurdles that the industry and governments must still overcome before cloud computing reaches its real potential.[37]

2.4. Obstacles in the Confidence of Cloud

There are numerous advantages for small, medium and large businesses in using the cloud. However, the benefits are not without risks. The cloud creates a complex and intricate network of relationships which can compound contractual difficulties and compliances. At the centre of challenges are the main concerns, which remain the same as previously mentioned, such as security, confidentiality or privacy and additionally ownership of the e-data as well as systems liability for breakdowns and related downtime.[38]

---

[34] SMITH, B. (2010) *Building confidence in the cloud: A proposal for industry and government action for Europe to reap the benefits of cloud computing*. European Commission EC Justice News. http://ec.europa.eu/justice/ [Accessed 16 September 2015].

[35] European Network and Information Security Agency. (2012) Cloud computing benefits, risks and recommendations for information security rev b. ENISA. http://www.bing.com/ [Accessed 16 January 2016].

[36] *Ibid.*

[37] Cloud Security Alliance. (2011) *Security guidance for critical areas of focus in cloud computing V3.0,* Cloud Security Alliance CSA. https://cloudsecurityalliance.org/ [Accessed 15 December 2015].

[38] *Ibid.*

The cloud concerns around the security, privacy and reliability of information systems are not novel. The same apprehensions about the liability of delivering a simple letter or message remains. Cloud service providers are constantly looking at the daunting aspect of the official quagmire or persecution for merely being the channel/messenger of the information. The more pressing concerns are from the jurisdictions around the world who are grappling with the issues of security, privacy[39] and protection of personal data. In the USA, for instance, Courts have stated that hand-held phone Track and Trace location data are protected by the Fourth Amendment 'In re U.S. for an Order Directing a Provider of Electronic Communication Services to Disclose Records to the Government 534 F. Supp. 2d 585, 612 (W.D. Pa 2008)'[40] with which the current USA administration disagrees.[41.] In other instances, the British government is pushing forward with a National Deoxyribonucleic Acid (referred to as DNA) database, which will provide the state with a permanent source of personal character information of its citizens.[42] In Germany there is a difference of opinion, where the courts have repealed a law which allowed the authorities to 'retain data on telephone calls and emails, saying it "marked a grave intrusion" into the personal privacy rights and must be revised.' The personal privacy issue is not over as industry leaders and legislators are pushing governments to more reasonable limits to the access of electronic communications, (*In re Pen Register & Trap/Trace Device with Cell Site Location Authorisation, 396 F. Supp. 2d 747, 754 (S.D. Tex. 2005)*) ("While the cell phone, not originally conceived as a tracking device, law enforcement converts it to that purpose by monitoring cell site data.")[43], while the USA administration is pushing to expand to a warrantless surveillance of the internet. All of which affects cloud computing negatively. Four primary issues are in the way of cloud reaching its true potential and being openly accepted. The first problem relates to the main risks associated with the cloud, as before, security, privacy and loss of control or governance over the data. Also, there are further risks associated such as the mechanisms for separation, malicious damage to data and finally reliability.[44] The second issue relates to the ownership and control over online data,

[39] *Ibid*. 33.
[40] LEAGLE. (2008) *In Re U.S. for Order Dir. A Prov. Of Elec. Commune*. Leagle. http://www.leagle.com/ [Accessed 11 January 2016].
[41] Mc CULLAGH, D. (2010) *Feds push for tracking cell phones*. CNET news. http://www.cnet.com/news/ [Accessed 20 January 2016].
[42] BROWN, G. (2010) *Brown defends DNA database and CCTV roll-out.* Truth Alliance Network. http://truthalliance.net/ [Accessed 4 February 2016].
[43] HEALEY, A. (n.d.) *Tracking individuals via their cell phones: Answering the call*. Federal Law Enforcement Training Centres. https://www.fletc.gov/sites/ [Accessed 4 February 2016].
[44] European Network and Information Security Agency. (2012) *Cloud computing benefits, risks and recommendations for information security rev b*. ENISA. http://www.bing.com/ [Accessed 16 January 2016].

which can in some instances be uncertain or abused or misused.[45] The third issue relates to confidentiality and law enforcement having unfettered access to confidential data.[46] The fourth issue relates to the current laws which govern most of the online communications and their age in the Cloud technology era and if these laws are still adequate to provide the protection required or sought.[47]

2.5. Conclusion

Bridging the legal gap is still problematic although it is reasonably common knowledge that cloud computing technology has been around for several decades and new to laws and legal institutions which regulate and administer such technology are lacking. What is less commonly understood is the tremendous growth and expansion of the computer industry over the past ten years. Together technology development and the creation of mass storage devices, enhanced computer platforms and the arrival of the internet have shaken the foundation principles of industries, such as publishing, music, film and television.[48]

The use of technology is reshaping traditional business and introducing new commercial models using multimedia and social networking. Affiliated with these developments are significant advances in the development of network technologies, peer-to-peer architecture and broadband access for the internet, facilitating cloud computing for home users, both publicly and privately.[49] With traditional business models, IP safeguards had previously been able to maintain regulatory control with technology development.

The recent expansion of technology and networks, has introduced new challenges as to how IP safeguards remain interpreted and applied. Authorities are facing an ever increasing gap between the current regulations and technology development. Several leading authorities such as the EU and the USA have spent time investigating the knowledge gaps between law and technology, particularly in areas most commonly affected such as security, privacy and

[45] PICKER, R.C. (2008) *Competition and privacy in Web 2.0 and the cloud*. SSRN. Social Science Research Network. http://papers.ssrn.com/ [Accessed 4 February 2016].
[46] SMITH, B. (2010) *Building confidence in the cloud: A proposal for industry and government action for Europe to reap the benefits of cloud computing.* European Commission EC Justice News. http://ec.europa.eu/justice/ [Accessed 16 September 2015].
[47] DEMPSEY, J.X. (1997) *Communications privacy in the digital age: Revitalising the Federal wiretap laws to enhance privacy*. Albany publishers Law Journal of Science & Technology, 8 (1).
[48] MERGES, R.P., MENELL, P.S. and LEMLEY, M.A. (2012) *Intellectual Property in the new technological age. 6th ed*. New York: Aspen Casebook Series, Wolters Kluwer Law and Business. p. 684.
[49] Idem. p. 685.

the protection of personal data, all of which related to cloud databases. It is not always easy to define new regulations. As most complex regulatory questions are raised or qualified post infringements and as a consequence of this experience current regulations lag behind technology development creating the so-called ‘legal gap’.[50]

This has become part of the epic battle over the future of IP law and how to bridge the legal gap.

[50] *Ibid.*

3. General Legal Safeguards

3.1. Introduction

There is, at present, no all-embracing privacy or data (information) protection statute in South Africa which provides for full operative or mandated data protection obligations to be complied with by data controllers for the handling and processing of personal data. The treatment of personal data in South Africa remains controlled by common law and constitutional rights to privacy. There are several Acts concerning the requirements of personal data such as the Protection of Personal Information Act 4 of (2013)[1] (referred to a POPI), Electronic Communications and Transaction Act 25 of (2002)[2] (referred to as ECTA), and the National Credit Act 34 of 2005[3] (referred to as NCA). However, even though these Acts provide certain levels of protection, there remain gaps in the overall security system. The protections afforded regarding the common law and constitutional right to privacy are relatively weak and the risk of litigation has historically been small. The Department of Trade and Industry (referred to as DTI) has recently gazetted the new copyright amendment bill, the Copyright Amendment Bill b13 2017,[4] which appears to have a more comprehensive approach to dealing with the general protection of works and aspects of copyright in the digital environment.

While the other Acts address certain personal data protection requirements, the data protection requirements emanating from the POPI has viewed applications closer to personal data, which remains in the cloud databases. Such personal data is mostly about employees, clients and customers or potential customers. There are other types of personal data retained by businesses such as guest information on visits to premises or within the framework of the companies' exclusive activities. The POPI will have an effect on the following:

a) Businesses that collect, hold or utilise personal data as well as distribute or otherwise process personal data are required to do so under certain conditions.
b) Businesses may not gather or collect any more personal data than that which is necessary to complete the work for which the data was originally collected. For

[1] *The Protection of Personal Information Act No. 4 of 2013 of South Africa*, Policy, Law, Economics and Politics. http://www.polity.org.za/article/protection-of-personal-information-act-no-4-of-2013-gazette-37067-2013-11-26 [Accessed 6 December 2015].
[2] *Electronic Communications and Transactions Act 25 of 2002,* Government of South Africa. Southern African Legal Information Institute. http://www.gov.za/documents/ [Accessed 26 March 2016].
[3] *National Credit Act No. 34 of 2005*. Acts online. https://www.acts.co.za/ [Accessed 15 July 2016].
[4] *Copyright Amendment Bill b3, 2017*. DOTI. http://www.gov.za/ [Accessed 22 July 2017].

example, a business that gathers employee personal data for the purpose of making payments to such employees, cannot use the same data to sell the employees services or goods.

c) Companies must provide a particular 'opt-in' policy for direct marketing information or communications. Until recently companies had only been required to give an 'opt-out' system. There are some variations to the general rules, in that corporations may perform direct marketing on existing customers.
d) Businesses are required to take the necessary steps to secure the personal data, maintain data confidentiality and integrity of all personal data held or controlled by that business by ensuring the proper technical, operational and organisational measures are in place to prevent loss, damage or unauthorised destruction of the personal data.
e) Requirements addressing cross-border transfer of personal data.
f) The establishment of a new Information Regulator, currently in process, tasked with monitoring and administering the law, ensuring compliance, processing and handling of complaints about any noted violations. Furthermore, the Information Regulator will serve information notices, legal administration notices and infringement notices as well as obtain warrants for search and seizure as required.

While data protection is an integral part of a person's right to privacy, the legal protection must, therefore, provide cover in all instances of protection from personal data collection, storage, utilisation or communication by another person or institution. South Africa provides some degree of privacy protection through the Constitution[5] and Common Law. However, are the current laws sufficient and does the law focus on those aspects which are exploited?

To enable the law to provide adequate personal data protection, serious consideration should be given to opposing interests like the administration of national social programmes on how to maintain law and order while protecting the rights of other stakeholders. This raises questions around the cloud industry and their interest groups which require the use, handling and processing of personal data. Market clusters in the financial sector, healthcare, commercial and travel services are all impacted on by such laws. The essentials of balancing all the interest groups are extremely delicate.[6] To provide a more proper view of the balancing act of focus groups and the appropriate law for cloud requires a more holistic review of the law on an international level. How does South African law measure up?

[5] *The Constitution of the Republic of South Africa No. 108 of 1996, as amended*. Government of South Africa. http://www.gov.za/ [Accessed 21 February 2016].
[6] *Copyright Amendment Bill b3, 2017*. DOTI. http://www.gov.za/ [Accessed 22 July 2017].

3.2. National Information Security Directive

The EU is debating a proposal for a directive on information security which aims at raising the level of preparedness across all member states regarding information security issues affecting more than one member state. In doing so, the members shall set their legal framework and infrastructure allowing for cross-border information sharing and risk identification. In addition, the internal structures regarding a national authority and a computer emergency response team need to be established. The governmental authority is required to collect data and identify incidents which pose a risk to national information security. As these systems are interconnected across all member states, a consistent approach is necessary to detect and prevent the spread of an incident across the member states. The standardisation process of cloud services could potentially create systemic risks based on the uniform use of protocols and other technologies. Once these are breached or otherwise affected, all cloud service providers would be facing the same challenges. Thus, a European coordination framework seems warranted.

3.3. Cloud Access by Foreign and National Governments

Data access by the governments and their intelligence organs has become a prevalent topic in the media as it touches on and concerns every internet or cloud user. In particular, the USA's approach has been criticised as being not transparent and by far too intrusive into the liberties of its own as well as foreign nationals. In general, one can say that data access by an intelligence agency targeting foreign nationals is hardly regulated, and nearly any form of measures to obtain external information is allowed. However, when the agency wants to gain information about citizens of its own country, specific formal procedures must be followed. These differ profoundly, specifically between the USA and EU member states. Most noteworthy in the context of cloud is the fact that a transfer under the new EU-USA Privacy Shield Framework (previously under the Safe Harbour Framework) of the EU[7] is still thought of as compliant with EU law, regardless of the wide-ranging access rights of the USA intelligence agencies.[8]

[7] Communication from the Commission to the European Parliament and the Council. (2013) *On the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU*. EC Europa. http://ec.europa.eu/justice/ [Accessed 15 July 2016].

[8] ROBERT, S. (2013). *Privacy, technology and national security. An overview of intelligence collection*. Office of the Director on National Intelligence. Brookings Institution. https://www.dni.gov/index.php/ [Accessed 12 July 2016].

Often cloud services create a false sense of security as the users are not aware of where the data is processed and stored. Nevertheless, access is available where the data is accessible once it is uploaded into storage in a fixed location such as a USA cloud server. No contractual undertaking, be this the Safe Harbour Framework, EU-USA Privacy Shield Framework or any other commission project, or other business, will stop public law such as the Patriot Act of 2001[9] or the Foreign Intelligence Surveillance Act of 1978[10] from undermining any such an agreement. However, voluntary disclosure can be prevented through contractual undertakings. To succeed in a breach of contract suit based on prohibited voluntary disclosure, the claimant would have to find a way around the mentioned legal indemnity (in other words, filing the claim against a foreign subsidiary based on foreign law). Another often neglected fact is that the USA cloud companies and their international divisions (in particular EU divisions) are subject to the USA disclosure regulations and can be required to hand over data which is uploaded into storage anywhere in the world. If they do not follow such a request, they may face severe penalties.

Entrusting information to the cloud must only be done when the users are confident that the information contained is not confidential or critical in any form. Thus, journalists especially should consider using alternative technologies or encrypting all data sent to the cloud to ensure that no other party gains access to it. At this level, some situations might even raise human rights issues where the minority groups communicate through the cloud and could subsequently be harmed or slain if their information falls into the wrong hands.

3.4. Data Protection and Data Flows

Data protection laws are an integral part of the cloud computing framework.[11] In the EU there has been a recent change to the data protection regulations. The long-serving data protection

[9] T*he USA PATRIOT Act 2006: Preserving Life and Liberty (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism)*. Department of Justice. https://www.justice.gov/ [Accessed 9 July 2016].

[10] *The Foreign Intelligence Surveillance Act of 1978. Justice Information Sharing U.S. Department of Justice, Office of Justice Programs*. Bureau of Justice Assistance. https://it.ojp.gov/ [Accessed 9 July 2016].

[11] *General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC*. Eur-Lex. http://eur-lex.europa [Accessed 23 April 2016].

Directive 95/46/EC[12] has, after an actual judicial process, been repealed and the new General Data Protection Regulation (EU) 2016/679[13] (referred to as GDPR) adopted. The GDPR continues to ensure the protection of personal data, being data from which a person may be identified and data subject to extra protection and not be divulged to parties who do not require such data and are not entitled to receive this information.

Data protection law reform is gaining increased momentum worldwide, with more than one hundred countries now having new legislation in some form, either in draft format or implemented. The South African legislator enacted a new personal data protection law in the framework of the POPI Act[14], which was a significant step to providing more substantial personal data protection in South Africa. The initial outline of the POPI Act stands widely modelled on the previous EU Directive 95/46/EC. However, there are still areas in the POPI Act which can be improved following the EU adoption of the GDPR. [15].

It should be noted that with the promulgation of the POPI Act in 2013, other data protection laws, which deal with the same subject matter, will need to be reevaluated either by the Legislature or the Courts and may result in amendments. Potentially Acts such as the ECTA and NCA, which contain interim provisions on data protection, may be affected.

Furthermore, the EU in particular, is driving advanced reforms of data protection, which take into account a Unified Data Protection Regulatory Framework. The aim of such new framework is to streamline all the individual member states into one regulation so that the EU countries are united and aligned within a single law. Moreover, it should be noted that the new law continues to use the fundamental framework of the 1995 EU Directive, although with significant enhancements. Key features of the new law are set to improve on data protection

[12] *Directive 95/46/EC of the European Parliament and 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*. EC Europa. http://ec.europa.eu/justice/ [Accessed 22 April 2016].
[13] *General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC*. Eur-Lex. http://eur-lex.europa.eu/ [Accessed 23 April 2016].
[14] *The Protection of Personal Information Act No. 4 of 2013 of South Africa,* Policy, Law, Economics and Politics. http://www.polity.org.za/article/protection-of-personal-information-act-no-4-of-2013-gazette-37067-2013-11-26 [Accessed 6 December 2015].
[15] *General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC*. Eur-Lex. http://eur-lex.europa.eu/ [Accessed 23 April 2016].

and take into account some of the most important points, which were part of the EU Commissions overall desire to improve data protection. They include the following:

a) The introduction of the end-user's 'right to be forgotten' which means, data processors and data controllers are obligated to remove individual's details from a database if so requested.
b) Increased fines for non-compliance on a sliding scale or up to 2 percent of the company's revenues.
c) 'Data portability right' customers should be empowered to move personal data from one cloud service provider to another effortlessly, or without hindrance.
d) Data is acquired and handled justly.
e) Data stands retained only for quantified, clear and legitimate applications and only disclosed through compatible means and use, as per the above.
f) Data is held safe and secure, as well as accurate, up-to-date and complete.
g) Data retained is not disproportionate and only sufficient for the appropriate use.
h) Information is not reserved for longer than required.
i) Information is made available to the individual concerned upon demand.

Before engaging a cloud service provider, the data protection characteristics of the cloud service provider should be considered. Firstly, from a holistic point of view, regarding how the cloud-based services will be used towards the relevant business processes. There are various decision-making approaches which may be applied. However, some crucial cloud zones should be considered as part of this process. Issues relating to the following are important:

a) If the data are to be placed in the cloud, how sensitive is such data and what would the implications of a data breach be?
b) With respect to legislation, what international and national data protection laws are available and how do they fit in with the contractual provisions such as, RSA regulations, EU and USA laws, the EU-USA Privacy Shield Framework or sector-specific law, other laws relating to cross-border data flows that may impact on the decision or business process?
c) Cloud service provider and business stakeholder responsibility. Related to the controller and processors responsibilities, how are these assigned to the cloud-based transfers for the business process? Do particular participants have multiple roles or tasks, all of which need to relate back to the legal responsibilities of each stakeholder?
d) Crucially, data centre locations. Cloud service providers are notorious for not providing all data centre locations. Check on the jurisdictions, are these centres local or in other countries, and have cross-border data flow issues been considered?

e) Cloud service provider guarantees. Does the cloud service provider offer any guarantees or service provider certifications for the data centre locations for stored data? Are there any assurances that the client will be notified of any changes and that the changes will not breach any contractual conditions or relevant regulations?
f) Data flow notification. Do customers, data subjects or staff need to be notified if and when their data is moved to the cloud service provider's centres?
g) Data breach. What are the cloud service provider's data breach policies and procedures? Are such policies and procedures explicit in the agreement and what is the notification process for any such violation?

Following the minimum requirements checklist for data protection before selecting a cloud service provider, will ensure that the risks associated with data protection will at least be known. It may not always be possible to eliminate the risks. However, having a more realistic understanding will provide the knowledge necessary to plan the businesses' internal backup processes in case of data breaches.[16]

3.5. Intellectual Property and Related Issues

A complex number of questions on IPR arise in the context of cloud computing. These can be related to software supplied by the cloud service provider or software used on a cloud service provider's servers originating from the client. Other aspects such as data stored and accessed by cloud clients also raise IP issues.[17]

Before filing an action, the infringer needs to be identified as a first step. In most instances this will be hard to achieve due to the international nature of cloud services and the use of internet protocol addresses. Thus in most cases, an action is brought against the cloud service provider as the facilitator of the infringement. Such actions are a major concern for the users and suppliers of cloud computing services. Currently, no legal framework exists for IPRs applying and determining the national laws, which will govern an individual case, is complex.

As an initial point, clients entering into using the cloud must ensure that as the customer they are granted a contractual guarantee on any possible IP damages which may be caused by the cloud service provider's software. Furthermore, in the more common practice where the cloud service provider gives access to standard software applications, where clients regularly

[16] ESPION. (n.d.) *White Paper: Data protection in the cloud.* Espion Group. https://www.espiongroup.com/ [Accessed 15 April 2016].
[17] CORDELL, N. (2013) *Intellectual Property in the cloud.* Allen and Overy. http://www.allenovery.com/ [Accessed 4 January 2016].

utilise open source software for their particular requirements, the software is then adjusted either by the cloud service provider or the client to fit the customer's exact specifications. The cloud service provider may later utilise the newly modified software and distribute the software to additional customers while infringing on the innovative developing client's IP. In one respect, a customer must therefore thoroughly review the contract to be assured of the rights of use of the software as well as the right to further distribution of such software and whether any original grant is given to the cloud service provider. In another respect, the cloud service provider may only seek a short-term grant to access the particular adjusted open source cloud software to gain know-how.[18]

3.6. Governing Boundaries of Cloud Contracts

Cloud computing contracts are subject to the rules of general contracts of the jurisdiction where they are concluded. When dealing with private end users of the service, the primary regulatory provisions affecting such contracts are based on consumer protection law. To maintain the balance of the bargaining power between the rights of an innocent individual and a large cloud service provider, safeguards are put in place by various legislators. Often cloud service providers will limit or even exclude any duty to keep the service available as well as require an indemnification for any data loss, destruction, disclosure and so forth.[19] For example 'The Fairness criterion' as discussed by the South African Law Commission Report Project 47, Unreasonable Stipulations in Contracts, and the Rectification of Contracts, [20] as well as by the United Kingdom (UK), which implemented the Unfair Terms in Consumer Contracts Regulations 1999, wherein the report and terms of each provide that when a significant imbalance exists in the parties' rights and obligations to the disadvantage of the consumers, such a condition will be considered as unfair.

This form of safeguard will only apply to the user and not to the so-called 'critical subject matter', regarding the contract. In the long run, it rests with the Courts to show their willingness to expand the application of the law to cloud contracts and therefore bar distinct one-sided provisions of cloud contracts which are common today. If the recommendations of the published guidance memorandum are followed, one could expect that a consumer-sympathetic interpretation will be applied.

[18] See Intellectual Property related items discussed in Chapter 16.9.
[19] Google Inc. (n.d.) *Google cloud platform terms of service*. Google. https://cloud.google.com/ [Accessed 16 January 2016].
[20] The South African Law Commission. (1998) *Report Project 47. Unreasonable stipulations in contracts and the rectification of contra*cts. http://www.justice.gov.za/ [Accessed 3 February 2016].

Once a cloud contract is breached by a provider, the user will face the challenge of receiving back data transferred into the cloud. Potentially a cloud service provider could take its user's data 'hostage', requiring the payment of an additional fee or a disclaimer of any rights under the contract. These risks are one of the biggest challenges cloud computing technologies face as in essence the user loses control of the data sent to the cloud. The data then can be stored and processed anywhere in the world, making any enforcement action impossible.

3.7. Risk Assessment and Management

Risk assessment and risk management in the cloud should form part of any consideration when opting to use a cloud service. Based on a scale of economics, cloud service providers have the best position to offers a more resilient and secure cloud environment than a consumer who manages their own IT platforms. However there are always the risks associated when considering a new cloud service.

Firstly, there is the selection of the cloud service provider, then gaining and building the level of trust for a long term service relationship. Secondly, the sensitivity of the data which will be stored and used in the cloud against the security and privacy services offered. Typically these considerations would depend on the type of cloud services required (SaaS, PaaS and IaaS), the cloud model to be used, the data involved and any associated regulatory requirements. Thirdly cloud systems are always exposed to various threats that may have adverse effects on the users operations, assets and individuals or company.[21]

There are malicious bodies which may exploit vulnerabilities, both know or unknown, to compromise privacy, availability, information integrity and security, either processed, transmitted or stored in the cloud. The numerous types of risks which an organisation would need to take into consideration are primarily based around their requirements. Typically they would include but not be limited to some of the following, program management, administration, financial and accounting, safety, inventory, IP and products, supply chain and legal liability.

Risk management should be a holistic part of the company and should be viewed across all activities. Generally risk management may be fashioned into three categories and focused on the level at which they consider the risk-related issues or concerns. Category one, the company or organisation level, category two, the business operations level and category three,

[21] IORGA, M. and KARMEL, A. (2015) *Managing Risk in a Cloud Ecosystem*. NIST. http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=919954. [Accessed 17 August 2017].

the data systems level. Companies and individuals who use the cloud or are embarking on using the cloud services, should as a rule set up a risk management system and perform a risk assessment prior to entering into any agreement with a cloud service provider. A risk assessment may also be performed on existing cloud agreements. Once the analysis is performed and if any major risks are exposed, proactive mitigation plans can be established and executed through the risk management system.

3.8. Conclusion

The discussion has shown several aspects of general legal safe guards from the EU, USA and RSA. New regulations such as the POPI Act in the RSA together with the GDPR and Privacy Shield in the EU, as well as the far reaching rights of the USA intelligence agencies, provides a level of legal safeguard.

The EU and USA have established data protection laws and data flow protection by means of either the safe harbour principal or privacy shields. In addition the EU's GDPR, which provides a broad based data protection regulation mainly for the EU member states. From the information, it is clear that cloud service providers must have an establishment within the EU and that only cloud services within the EU are active. That would provide the user with recourse to EU laws and administration within the EU. It should be noted that in the past there was no call to have legislation aligned across the member states.

Therefore, the applicable laws in the other countries on contractual duties and rights may vary depending on in which state the action is raised. It is clear that enforcing a contract with a cloud service provider or raising a claim for damages across countries would always pose challenges. The EU has made great strides in this sector with the release of the new GDPR as well as by calling on the member states to align with the related legislation to have a single policy for dealing with such contractual issues. The move towards a single system will further encourage cloud development in the EU.[22] A lesson which could be followed by other countries to come together and form a single global cloud regulation for data protection. However, there is still the need to continually seek improvement in respect of cloud security and data protection risks.

[22] RICKY, M. and MAGALHAES, M.L. (2015) *Cloud data jurisdiction: The provider, the consumer and data sovereignty*. Cloud Computing. http://www.cloudcomputingadmin.com/articles-tutorials/compliance-regulations/cloud-data-jurisdiction-provider-consumer-and-data-sovereignty.html [Accessed 17 February 2016].

4. Cloud Safeguards and Legal Framework

4.1. Introduction

Cloud computing and cloud services, legal and protection structures have always raised questions and will always elicit further questions going forward, given the nature of technology innovation and development. However, cloud technology is subject to a varied number of legally prescribed and voluntary safeguards and boundaries. These include legislation through the POPI Act, the Competition Act 89 of 1998 (30 November 1998) as amended (referred to as the Competition Act)[1] and other IP regulations, which ensure certain safeguards, personal data protection, privacy and IPRs. The legal framework is attempting to maintain an open and accessible cloud market and the concept of 'net neutrality.' Although aimed at improving the rights of clients, such legislation is in practice not well harmonised to the essentials of cloud service providers and thus poses significant challenges in its daily application. A consideration highlighting the legal framework and appropriate safeguards for cloud as well as the potential measures, which cloud service providers can and should be implemented to ensure compliance, is required.

In practice the essential aspect of cloud services is to provide access, storage and portability of data and all are of central importance. Three likely scenarios are envisaged in respect of an individual's access to data stored in the cloud, as well as the available technical framework for the transfer of such data to other cloud systems. The first scenario is that of the cloud market, which is broken down into various players each with their particular individual systems based on self-developed proprietary technologies. In the second scenario a limited number of cloud service providers dominate the market. However, these cloud service providers will allow data transfers between their cloud and other cloud systems. Ideally, the third approach using a universal data standard, open interfaces and open source software should be sought as this methodology provides for the highest efficiency gains by making use of an international cloud.[2] This method would ensure open systems through enhanced data portability. It will also be one of the main future challenges facing regulators globally. It is, therefore, important that government procurement takes these subjects into account and require of their cloud suppliers

[1] *Competition Act No. 89 of 1998 as amended:* ACTS, http://www.acts.co.za/ [Accessed 11 January 2016].

[2] Organisation for Economic Cooperation and Development. (2009) *Briefing paper for the ICCP technology foresight forum*. OECD. https://www.oecd.org/ [Accessed 15 December 2015].

to fulfil a uniform data standard. Such action will put pressure on cloud service providers to ensure data portability and access within an appropriate legal framework and safeguards.[3]

Such legal safeguards can stem from various specific regulations or general competition law.[4] In the RSA legal safeguards stem from the POPI Act, the Competition Act as well as other IP regulatory instruments.

The two forms of regulatory systems namely 'specific regulation' and 'general competition law' need examination, in particular with respect to their relationship to the cloud. The structure of specific normative provisions such as interoperability and data portability, network neutrality, vertical integration control as well as e-commerce requirements are the main pillars for particular territorial regulation. The analysis shows that precise local law is only partially in a position to meet the demands of an appropriate legal framework for the cloud.[5]

As a consequence, general competition law must be invoked to overcome regulatory weaknesses. There are major items which need addressing, such as the likes of interoperability and data portability from one viewpoint and the limitations of vertical integration another point of view, which all impact in some way on the legal and safeguard framework.

4.2. Available Regulatory Instruments

To further understand the legal framework for cloud, it is important to understand how and what the available statutory tools are for cloud systems. Cloud should be included into economic regulation, to which sector-specific regulation and competition law belong and into comprehensive legal safeguards such as security, personal data protection, privacy and IPRs or business-related laws, which due to their scope, either touch on or are concerned with the cloud.

Economic regulation embraces two primary forms of state intervention as based on the two different regulatory regimes previously mentioned namely competition law and sector-specific regulation.

---

[3] DONOHUE, M. and YPSILANTI, D. (2009) *Briefing paper for the ICCP Technology Foresight Forum: Cloud computing and public policy*. OECD. https://www.oecd.org/ [Accessed 15 March 2016].
[4] Organisation for Economic Cooperation and Development. (2003) *OECD Peer Review. Competition Law and Policy in South Africa May 2003.* OECD. http://www.oecd.org/ [Accessed 12 January 2016].
[5] *Competition Act No. 89 of 1998 (Date of commencement of sections 1-3, 6, 11, 19-43, 78, 79 & 84 on 30 November 1998. The remaining sections of the Act commenced on 1 September 1999.)* Competition Commission. http://www.compcom.co.za/ [Accessed 15 March 2016].

a) Competition law, which is referred to as *ex post* regulation, is characterised by the fact that the Competition Authorities will intervene if market participants jeopardise free competition by way of restrictive agreements of abusive behaviour within the market. In exceptional cases of mergers, the Competitions Authority is allowed to pre-emptively block a structural change in the market.[6]

b) In contrast, sector-specific regulation is a form of *ex ante* regulation or at least partially so where it tries to prepare the ground for competition, which is only admissible in those markets in which the forces and players fail to ensure workable competition, for instance, natural monopolies.[7]

The competition law rules are considered to be applicable norms without regard to the particularities of a certain market; they are usually backwards looking as they rely on historical evidence. Sector-related regulations are correctly structured or designed to meet the requirements of a certain market. They are forward-looking, *ex ante*, sector-specific regulations and accepted in market segments in which competition pressure is weak or even non-existent and therefore the systematic abuse of market power is likely to be found.[8]

Both approaches have their strengths and weaknesses. Competition law is quite general and does not typically provide specific solutions, but is very flexible. The sector-specific regulation contains precise terms which provide certainty for regulatory bodies and concerned undertakings; it regularly provides faster and more efficient solutions.[9]

Competition law is applicable across all of the economies, notwithstanding the existence of any sector-specific regulation, which in contrast, is usually formulated against the backdrop of competition law. Consequently, while competition law rules try to protect open markets in general, sector-specific regulation often focuses on promoting entry into markets deemed to lack sufficient competition. As a principle, it may be stated that the existence of the law does not free an undertaking from the obligation to comply with general competition law rules.

---

[6] AGRELL, P. and BOGETOFT, P. (2002) *Ex-post regulation pre-project 2 – Final Report.* SUMICSID. http://www.sumicsid.com/ [Accessed 2 April 2016].

[7] Office of Gas and Electricity Markets. (2010). *RPI - X@20 Emerging thinking consultation document – Alternative ex ante and ex post regulatory frameworks.* Gas Department. Office of Gas and Electricity Markets. https://www.ofgem.gov.uk/ [Accessed 2 April 2016].

[8] ALEXIADIS, P. (2012) *Balancing the application of ex post and ex ante disciplines under community law in electronic communications markets: Square pegs in round holes*. Gibson Dunn. http://www.gibsondunn.com/ [Accessed 14 April 2016].

[9] WEBER, R.H. and GROSZ, M. (2008) *Legitimate governing of the internet.* Syracuse University., https://listserv.syr.edu/ [Accessed 14 April 2016].

Sector-specific regulation is designed to avoid undesirable developments and ensures market access for interested businesses.[10]

At the institutional level, sector-specific supervisory bodies and competition authorities are meant to coordinate their actions. From a procedural perspective, sector-specific regulation has the objective of establishing an adequate market structure. Therefore, the concrete norms are to be applied at first sequence, followed by the general competition law rules.

Since cloud computing has a close relationship to technical infrastructures such as fixed line and mobile infrastructures, an interaction between sector-specific regulation and competition law is unavoidable. Even if overarching rules for cloud, as an IT service, are not available on an international or regional basis, specific rules are in place for instance on network regulation as well as on content management which plays an integral part in the cloud markets.

4.3. Sector-specific Regulation

Several problems are dealt with by sector-specific regulation namely:

a) Interoperability and data portability
b) Network neutrality
c) Vertical integration
d) E-commerce

To understand e-commerce, communications and transactions, the South African e-commerce setting must be part of a more detailed discussion, alongside the EU electronic communications framework. The framework focuses on four main directives: the Framework Directive, the Access Directive, the Authorisation Directive and the Universal Services Directive, corresponding to the legal nature of these guidelines, the particular rules and their implementation at national level.

4.3.1. Interoperability and Data Portability

A portion of the South African regulatory framework, the POPI Act, defines an ‘electronic communication’ as information or data in the following way: ‘Any message being either, text, sound, image or voice, transmitted across an electronic communications network, which

[10] SLUIJS, J.P., LAROUCHE, P. and SAUTER, W. (2012a) *Cloud computing in the EU policy sphere interoperability, vertical integration and the internal market.* Tilburg Law and Economics Center. https://www.jipitec.eu/ [Accessed 12 January 2016].

stands stored in the user terminal or the network, pending such time that the receiver accesses such form of data'.

The EU regulatory framework defines an 'electronic communications' service as a service which consists mainly or wholly of the transmission of signals across an electronic network, which includes telecommunication services, but excludes services which provide or exercise publishing management control or material conveyed using 'electronic communications' systems and services.[11]

Theoretically, cloud computing could be summarised under the term of electronic services if the activity is concerned with services in the form of sending signals over electronic communications networks.[12] Such kind of business restriction on sending data signals does not apply in the daily practice of cloud computing.

Cloud service providers offer IT related services enabling the storing and processing of data. Usually, they are dependent on the internet service providers to facilitate the sending and receiving of signals on the networks; that is cloud service providers are not establishing the communications infrastructure nor are they associated with the respective services, meaning that regulations on electronic communications do not hit the core of cloud computing services.[13] Nevertheless, this technical assessment is not to say that a cloud service provider would exercise editorial control over any content transmitted.

The South African definition of 'processing', be it data or communications processing is laid out as follows, as it 'means in the least an activity or operation or any set of operations, either by automatic means or not, about personal information, including:

a) The collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;[14]
b) Transmission using broadcast, communications and dissemination or by production and availability in any other form; or

[11] SLUIJS, J.P. et al. (2012a) *Cloud computing in the EU policy sphere interoperability, vertical integration and the internal market.* Tilburg Law and Economics Center. https://www.jipitec.eu/ [Accessed 12 January 2016].
[12] *Ibid*.
[13] *Ibid.*
[14] 'Isibaya – Registration' (n.d.) *Public Investment Corporation*. https://isibayafund.pic.gov.za/ [Accessed 15 June 2016].

c) Unification, joining, as well as restriction, degradation, erasure or destruction of information.[15]

The South African regulation contains similar aspects to that of the Access Directive of the EU with some minor variations on their interconnection requirements with matching powers for the national regulatory agencies. Nonetheless, these requirements only concern electronic communications service providers. Therefore, the regulatory framework seems of little support for enhancing data portability and interoperability of cloud services.[16]

4.3.2. Network Neutrality

The relationship between cloud service providers and internet service providers (ISPs) is vulnerable to the network neutrality debate focusing on the question whether an ISP may intervene in the communications process. For instance, an ISP may introduce different network operational speeds of delivery or pricing structures for bandwidth.[17] From a substantive angle, the problem of the introduction of a model of differentiated quality of service for different services is at stake.[18] Obviously, network neutrality is significant for cloud computing since the delivery of services is typically time sensitive (not allowing for slow processes) and price structuring could jeopardise the price schemes of the cloud service providers.

Nevertheless, it should not be overlooked that priority services and differentiated pricing schemes could also enable cloud service providers to offer different kinds of services and make the reliability of these services dependent on the chosen service option.[19] A particular issue appears in the situation of scarce resources, for instance when the bandwidth is limited in mobile broadband. In this context, the questions on the network service provider's compliance with the neutrality standard must be examined.

The EU regulatory framework does not contain any specific network neutrality provisions, but does address the transparency element according to the policy that regulatory interventions

---

[15] *The Protection of Personal Information Act No. 4 of 2013 of South Africa,* Policy, Law, Economics and Politics. http://www.polity.org.za/ [Accessed 6 December 2015].
[16] SLUIJS, J.P. et al. (2012a) *Cloud computing in the EU policy sphere interoperability, vertical integration and the internal market.* Tilburg Law and Economics Center. https://www.jipitec.eu/ [Accessed 12 January 2016].
[17] HOGENDORN, C. (2007) *Broadband internet: Net neutrality versus open access*. Chogendorn. http://chogendorn.web [Accessed 15 January 2016].
[18] MIALON, S.H. and BANERJEE, S. (2012) *Platform competition and access regulation on the internet*. Research Gate. https://www.researchgate.net/ [Accessed 11 January 2016].
[19] *Ibid*.

in the market would legitimise providing the network clients are sufficiently informed of the network operator practices and network management standards. Transparency policy should overcome the potentially adverse effects of non-compliance with the network neutrality standard.[20] Nevertheless, national legislators are entitled to introduce specific rules which could have an impact on bandwidth management.

Ultimately, a certain fragmentation of national markets cannot be avoided. From the EU perspective, this consequence is acceptable since it would be in the national interest to introduce a competitive environment in support of their countrywide market participants.

Looking from this angle, the chief problem for cloud service providers consists of the fact that different regulations would require deliberation for various national markets, notwithstanding the transnational character of cloud services. The fragmentation could cause additional transaction costs even if the rules are transparent and the network management forecast.[21] Apart from costs, it might also become harder to guarantee a positive processing quality and speed to clients of cloud services. Clouds are especially vulnerable to this situation as their prime service delivery comprises outsourced computer intensive bandwidth demanding processes, often for corporate customers with high demand for reliability as they depend on cloud to operate their businesses.[22]

A possible countermeasure could consist of improved standardisation of the procedural and service related rendering of cloud. As a negative impact of normalisation, a particular weakening of competition between the cloud services providers can hardly be avoided.

4.3.3. Vertical Integration

As mentioned, with interoperability and data portability, a cloud service provider does not offer ‘electronic communications’, services over ‘electronic communications networks’. Therefore, such a service provider does not usually fall under the EU regulatory framework on electronic communications. Likewise in South Africa, the service provider does not come under regulatory frameworks. Nevertheless, both the EU and South African service providers are

[20] *Ibid.*
[21] BEREC. (2012) *Guidelines for quality of service in the scope of net neutrality. Body of European Regulators of Electronic Communications*. BEREC. http://berec.europa.eu/ [Accessed 10 February 2016].
[22] SLUIJS, J.P. et al. (2012a) *Cloud computing in the EU policy sphere interoperability, vertical integration and the internal market*. Tilburg Law and Economics Center. https://www.jipitec.eu/ [Accessed 12 January 2016].

subject to competition law in respect of vertical integration.[23] Consequently, the electronic communications structures do not play a direct role in this context.

Cloud services are likely to fall within the term of 'information society services'. Whether this assessment leads to certain access requirements, either under EU and RSA regulatory frameworks, has not yet been clarified. At first glance, the fact that certain services have a particular purpose does not qualify them for access to infrastructure even if content providers face similar access problems. In principle the matching challenges are not significantly different from those of 'electronic communications' services and networks, meaning that an application by analogy should not be excluded, particularly since the recent amendments to the EU Access Directive have included information society services and broadcast content services.[24]

4.3.4. Electronic Commerce

E-commerce is a central part of people's daily functioning and plays an essential part in the economic lives of individuals. It in itself also presents a series of complex issues. It involves the integration of many elements of technology, infrastructure, business operations as well as public policy. All these factors need to function together effortlessly to yield the most beneficial results to the public. The regulation of e-commerce would, therefore, need to take all this into account and still allow for innovation and new technology development.[25]

E-commerce regulations often rely on other notions than those of electronic communications laws, namely regarding 'information society services'. For instance, EU Directive 1998/34 uses the definition of a service usually provided for payment, remotely, via 'electronic means and at the distinct request of a receiver of services'.[26]

---

[23] *Competition Act No. 89 of 1998 (Date of commencement of sections 1-3, 6, 11, 19-43, 78, 79 & 84 on 30 November 1998. The remaining sections of the Act commenced on 1 September 1999.)* Competition Commission. http://www.compcom.co.za/ [Accessed 15 March 2016]. Chapter 3 S 12A. 2 (f).

[24] SLUIJS, J.P. et al. (2012a) *Cloud computing in the EU policy sphere interoperability, vertical integration and the internal market.* Tilburg Law and Economics Center. https://www.jipitec.eu/ [Accessed 12 January 2016].

[25] Department of Communications. (2000) *A Green Paper on Electronic Commerce for South Africa* Department of Communications. http://www.gov.za/sites/ [Accessed 11 April 2016].

[26] *European Parliament and of the Council of 22, 1998. Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations*. Official Journal L 204, 21/07/1998 P. 0037 – 0048. Eur-Lex. http://eur-lex.europa.eu/ [Accessed 12 April 2016].

Cloud services appear as a type of information society service. Therefore, in the EU countries the e-commerce Directive 2000/31 is applicable,[27] mainly containing rules being relevant in the cloud context in respect of jurisdictional issues and secondary liability for cloud services. The specific functions of the different ISPs are to be taken into account.

The primary purpose of an access provider entails the delivery of internet access availability. Therefore an access provider could be held liable for failing to provide internet access, based on contractual performance obligations. The most common problem is whether the failure to provide access can be attributed to the access provider, which depends on the type of malfunction experienced, given that the access provider is merely acting as a 'transporter' since characteristically the data is communicated across an electronic network. As the access provider makes it technically possible for a user to gain access to illegal material, it does not necessarily make the access provider a non-diligent performer regarding Article 12 of the EU E-commerce Directive.[28]

The notion of secondary liability as regulated in the E-commerce Directive encompasses the question whether service providers could become liable for actions of their users. According to the E-commerce Directive, a distinction must be drawn between a mere access provider, a caching service provider and a hosting provider.[29] Since a cloud service provider is designing and rendering individual services, the provision on the secondary liability of access providers would not be applicable.

Cloud service providers offering only content and services can be qualified as hosting providers. Therefore, when a cloud service provider has knowledge of illegal activities or illegal materials, the specific data must be removed. If the cloud service provider does not have any control over the recipient of the service, the secondary liability is limited to injunction relief.[30] Nevertheless, it should not be overlooked that the secondary liability provisions of the EU E-commerce Directive remains deliberated in the European Courts[31] and that the introduction of

[27] *European Parliament and of the Council of 22, 1998. Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations*. Official Journal L 204, 21/07/1998 P. 0037 – 0048. Eur-Lex. http://eur-lex.europa.eu/ [Accessed 12 April 2016].
[28] Idem. Article 12
[29] Idem. Articles 12-14.
[30] *Electronic Communications and Transactions Act 25 of 2002, Government of South Africa*. Southern African Legal Information Institute. http://www.gov.za/ [Accessed 26 March 2016].
[31] EU Courts Debate. (2007) *Legal analysis of a single market for the information society (SMART 2007/0037)*. EC Europa. http://ec.europa.eu/ [Accessed 26 March 2016]. See also *E-commerce directive, liability of intermediaries*. EC Europa. https://ec.europa.eu/ [Accessed 26 March 2016].

the appropriate EU-USA Privacy Shield Framework or otherwise the safe harbour provisions still are under deliberation.

It appears that a fresh, redefined approach to the hosting requirements stated in Article 14 of the EU E-commerce Directive[32] is essential, given the development of technology and in particular cloud technology. Nonetheless, there appears to be a justified view to enforcing a liability on a cloud service provider to control a client's data if a hosting provider is not required to do so. The chief technology difference lies in the dispersed server delivery of a broad scale up-down service, making administration of the data that much harder to attain than if the data remained hosted on a single server. As technology develops, so do various forms of clouds develop. Meanwhile, cloud service providers, together with hosting services, have joined to form a new service product called cloud hosting.

Distinction from the previous style of devoted or dedicated hosting services, where data hosted on the web was handled and stored on a single server in a particular location, cloud hosting allows storage and processing to take place in various localities. The data are relocated to a server centre where the costs are lowest and which is available to perform the required operations. The relocation of data yet again highlights the inconsistency of cloud technology and the existing law produced through uncompromising definitions in legislation such as the E-commerce Directive.

The E-commerce Directive is not very clear as far as jurisdictional rules are concerned since, according to its purpose, the new framework does not intend to establish additional rules for private international law. The preface does provide for the reservation that the traditional rules should not restrict the freedom to provide information society services.[33] As a principle, EU countries are not allowed to interfere with the cross-border provision of information society services. The applicable legal framework should remain based on the rules of the nation of domicile of the service provider.[34] Therefore, if a cloud service provider complies with the regulations of its country of domicilium, services could be delivered to clients in other territories.[35]

---

[32] *European Parliament and of the Council of 8 June 2000. Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce')*. Official Journal L 178, 17/07/2000 P. 0001 – 0016. Eur-Lex. http://eur-lex.europa.eu/ [Accessed 12 April 2016].

[33] Idem. Preamble.

[34] Idem. Article 3.

[35] HELLER, M. (2004) *The country of origin principle in E-commerce Directive: A conflict with conflict laws?* 12 Eur Rev Priv L RQSL. http://www.rgsl.edu.lv/ [Accessed 12 April 2016].

Nevertheless, a particular problem exsists in the fact that the E-Commerce Directive addresses EU states not in private enterprises such as network operators and the internet service providers. Since the Directive does not enjoy horizontal effects, the regulatory tools to streamline cloud operations appear weak.

4.4. Conclusion

Sector-specific regulations catering for the need of cloud service providers, especially regarding rights associated with the data flow to and from an internet service provider, which seem to be a solution in addressing the seemingly growing restriction on the side of the ISP, would likely be compensated by the cloud service providers as these are interested in innovative technologies facilitating a faster rate of data flow. Without such measures, cloud service providers will increasingly be faced with the challenge of actually being able to deliver their services to customers. Moreover, it is not only inconvenient for the customers, but will add enormous costs to the economy because of the lost competitive advantage which is generally to be gained by using more efficient technology such as cloud computing services. The risks associated with a vertical integration that is an ISP and a cloud service provider merging could also be reduced through regulations enforcing the supply of the ISPs service. The ISP must then ensure that it treats its cloud service provider in the same manner as other service providers.

Moreover, new methods for the protection of IPRs need to be explored and developed. The corresponding responsibilities of cloud service providers need to be precisely defined to ensure effectiveness, with a particular focus on E-commerce Directive Article 14 to provide additional clarification on the liability protection requirements, with a clear, reliable framework for cloud service providers.

Furthermore, public cloud service providers who do not have platforms and co-locate with other cloud service vendors and utilise competitor infrastructures, such as Apple's iCloud, which runs their service off servers provided from the likes of Microsoft or Amazon cloud servers[36] should be pressured to provide transparency on how their services are offered and performed. This can be achieved through guidance of the professional industry standards and educating the cloud users of the risks involved with these methods of cloud services.

[36] CLARKE, G. (2011) *'Apple's iCloud runs on Microsoft and Amazon services: Who says Azure isn't cool and trendy now'.* The Register. http://www.theregister.co.uk/ [Accessed 2 August 2016].

5. Competition Law

5.1. Introduction

Competition law provisions are not sector related, but apply across all markets. In most markets the Competition Act is used as a legal control for restrictive and abusive practices and conduct, as well as price discrimination by dominant firms and mergers. Furthermore, on various occasions, it has been seen that competition law play an increasingly important role in the IT markets and now also cloud services.

5.2. Market Definitions

Given the broad spectrum of competition law and market diversity, it is necessary to firstly view the definition of the term 'market' as seen by the EU and South African competition law practices.

Defining a market is the primary process when performing competition investigations in South Africa and many other jurisdictions. In more recent considerations the EU has involved the so-called 'economics-based' aspects of a market and developments in economics tooling, and industry organisation theories have led more economists to query the out-dated practice of delineation of specific market boundaries.[1]

The EU Commission released a notice on the definition of the so-called relevant market, which now reflects the Commissions new practice and policy. Taking into account Articles 101 and 102 as well as the EU Mergers regulation, in practice, an incredibly influential guide.[2]

The purpose of having these market definitions is to provide the guidance to identify and define the boundaries with competing companies. The guidelines serve to create the framework which the Commission will apply to the competition policy. The key aspect of the market definition is

[1] BOSHOFF, W.H. (2014) *Antitrust market definition: rationale, challenges and opportunities in South African competition policy.* Competition Commission. http://www.compcom.co.za/ [Accessed 15 January 2016].

[2] Directorate for Financial and Enterprise Affairs, Competition Committee. (2012) *Roundtable on Market Definition.* OECD. http://ec.europa.eu/competition/international/multilateral/2012_jun_market_definition_en.pdf [Accessed 15 April 2016].

to identify in an organised way the constraints involved in competing companies and what issues will be faced.[3]

5.3. International Interpretation of Market Definition

The application of competition law in respect of restrictive agreements or abusive behaviour of a market dominant firm requires the definition of the relevant product or service as well as temporal, geographic markets. Usually, the definition of the relevant market is based on the concept of demand-side substitutability, to be accessed and determined by a qualitative analysis of product or service characteristics and intended product or service use.[4]

In the case of cloud, an upstream market of cloud service providers and a downstream market of ISPs must take the following into account:

a) On the upstream level, the notion of the relevant market could be limited to individual types of cloud services such as SaaS, IaaS and PaaS. The justification for such a narrow differentiation lies in the fact that the three types of services differ in characteristics and use.[5] This approach does not accurately take into account the supply-side substitutability since cloud computing services rely on mass customization. Only if the cloud service providers can exploit economies of scope by ensuring a vast amount of services at a limited cost, the significant investments into the facilities would be justified.[6]

b) As far as the downstream level is concerned, a distinction between broadband access and narrowband access is possible, as well as to differenciate between fixed and mobile access to communications networks. Given the most recent technological developments, such kind of differentiation of sub-markets is becoming less convincing over time.[7]

---

[3] OSTERUD. E. (2013) *EU Competition Law - abuse of dominance (Article 102 TFEU)*. University of Oslo. http://www.uio.no/studier/ [Accessed 23 April 2016].
[4] KAGAN. J. (2013) *Bricks, mortar, and google: defining the relevant antitrust market for internet-based companies.* NYLS Law Review. http://www.nylslawreview.com/ [Accessed 17 January 2016].
[5] SLUIJS, J.P. et al. (2012a) *Cloud computing in the EU policy sphere interoperability, vertical integration and the internal market*. Tilburg Law and Economics Center, https://www.jipitec.eu/ [Accessed 12 January 2016].
[6] *Ibid.*
[7] *Ibid*.

A particular problem concerns the market definition of wholesale call termination: according to conventional practice, each respective network is establishing its relevant market as no choice to deal with another operator exists other than the operator to which the calling party subscribes, in this case, the terminating operator.[8] A similar reasoning could apply to the cloud services since a client can usually communicate with the cloud service provider only through a particular ISP.[9]

The geographic market definition has to take into account the fact that clouds are built on the premise of universality, mobility and omnipresence, making purely national markets too narrow; moreover, the geographic market scope must encompass the specific cross-border business.[10] Therefore, in principle, the cloud market is global, but subject to linguistic and cultural market delimitations for specific services.[11] On the downstream level, a cloud service provider can be subject to national regulation, for instance, on interconnection and roaming practices. Consequently, territorial markets are more fragmented and nation-wide issues can play a bigger role.[12]

5.4. Interoperability and Data Portability

Interoperability and data portability are one of the primary operational aspects for cloud data users, as once they have entered into a cloud services agreement or otherwise, existing contractual relations should remain unchanged, excluding the choice of an alternate service provider which would not be economically viable. The data user becomes entirely dependent on the services of the selected cloud service provider.

---

[8] *Official Journal of the European Union. Recommendation 2003/311 of 11 February 2003 on relevant product and service markets within the electronic communications sector susceptible to ex ante regulation in accordance with Directive 2002/21 [2003] OJ L 114/45*, ICT. https://www.ictregulationtoolkit.org/ [Accessed 6 January 2016].

[9] SLUIJS, J.P. et al. (2012a) *Cloud computing in the EU policy sphere interoperability, vertical integration and the internal market.* Tilburg Law and Economics Center, https://www.jipitec.eu/ [Accessed 12 January 2016].

[10] KLOPPER, H.B. et al. (2011) *Law of Intellectual Property in South Africa.* Cape Town: LexisNexis. See also WEBER, R.H. (2010) *Internet of things – New security and privacy challenges*. Semantic Scholar. https://pdfs.semanticscholar.org/ [Accessed 18 January 2016].

[11] KAGAN, J. (2013) *Bricks, mortar, and google: defining the relevant antitrust market for internet-based companies*. NYLS Law Review. http://www.nylslawreview.com/ [Accessed 17 January 2016].

[12] SLUIJS, J.P. et al. (2012a) *Cloud computing in the EU Policy Sphere Interoperability, Vertical Integration and the Internal Market.* Tilburg Law and Economics Center. https://www.jipitec.eu/ [Accessed 12 January 2016].

Competition law refers to the supposed client 'lock-in situation', which is considered the abusive conduct of a market dominant firm.[13] Such a kind of customer lock-in agreement leads to provoked dependence on a particular cloud service provider.[14] The first problem in the analysis of hypothetically illegal behaviour relates to the question of whether the cloud service provider has a dominant market position. The assessment of whether the cloud service provider has a dominant position depends on the market definition as discussed above. In practice, the Courts would apply the competition law approach that facilitates the assumption of market dominance and the assessment of market entry barriers.[15]

At first glance, fierce competition seems to exist between various firms active in the cloud services and network markets.[16] In the second example, the changing of a cloud service provider in practice is often hard-hitting and causes tremendous costs, as such the client's ability to quickly disengage from their existing cloud agreement or service provider.[17]

The behaviour of a dominant market firm could lead to anti-competition foreclosure, predominantly in cases with companies who have a high market share. In situations such as those the client would experience difficulties to port data from one cloud service provider to another or even having to take up working together with two or more cloud service providers simultaneously, even if these scenarios, do not easily fit into the broad manoeuvre of abusive behaviour, as recognised in the Competitions Act. Alternatively, in cases found in the EU as defined in the Guidance Paper of the EU Commission,[18] the client is stuck in certain investments about customization of services and the relocation of private or proprietary information on the cloud service provider's facilities.[19]

---

[13] *Competition Act No. 89 of 1998 (Date of commencement of sections 1-3, 6, 11, 19-43, 78, 79 & 84 on 30 November 1998. The remaining sections of the Act commenced on 1 September 1999.)* Competition Commission. http://www.compcom.co.za/. [Accessed 15 March 2016].
[14] *Ibid*.
[15] BRASSEY, M. et al. (2002) *Competition Law*. Cape Town: Juta Publishing. p. 181.
[16] Competition Tribunal of South Africa. (2015) *Large Merger – Vodacom (Proprietary) Limited/Neotel (Proprietary) Limited*. Competition Tribunal. http://www.comptrib.co.za/publications/ [Accessed 18 April 2016].
[17] SLUIJS, J.P. et al. (2012a) *Cloud computing in the EU policy sphere interoperability, vertical integration and the internal market*. Tilburg Law and Economics Center. https://www.jipitec.eu/ [Accessed 12 January 2016].
[18] KLOPPER, H.B. et al. (201) *Law of Intellectual Property in South Africa*. Cape Town: LexisNexis.
[19] SLUIJS, J.P. et al. (2012a) *Cloud computing in the EU policy sphere interoperability, vertical integration and the internal market*. Tilburg Law and Economics Center. https://www.jipitec.eu/ [Accessed 12 January 2016].

In cases such as these, the competition laws would need to encourage non-proprietary cloud systems by carefully monitoring the actions of dominant cloud service providers such as Google, Facebook, Microsoft and Amazon. If these market-dominant service providers decide to shield their service offerings against other cloud service providers, such action may violate completion law given their market strength and position.

5.5. Vertical Integration

Regarding the Competition Act, Chapter 2, Part A, sec 5(1) restrictive vertical practices are prohibited. It states the following:

> An *agreement* between parties in a *vertical relationship* is forbidden if it has the effect of substantially preventing or lessening competition in a market unless a party to the *agreement* can prove that any technological, efficiency or other pro-competitive, gain resulting from that *agreement* outweighs that effect.[20]

For instance, where a cloud service provider and an ISP propose to merge, apart from the vertical integration of two firms by way of a merger, vertical restraints can also be based on restrictive agreements or abusive behaviour.[21] Furthermore, the Competition Act prohibits minimum resale price maintenance outright.[22] It also prohibits agreements which have the effect of substantially preventing or reducing competition between a firm, its suppliers and clients.[23]

[20] *Competition Act No. 89 of 1998 (Date of commencement of sections 1-3, 6, 11, 19-43, 78, 79 & 84 on 30 November 1998. The remaining sections of the Act commenced on 1 September 1999.)* Competition Commission. http://www.compcom.co.za/ [Accessed 15 March 2016]. Chapter 2, part A section 5.

[21] KLOPPER, H.B. et al. (2011) *Law of Intellectual Property in South Africa*. Cape Town: LexisNexis. p. 399.

[22] *Competition Commission v BMW South Africa (Pty) Ltd t/a BMW Motorrad (97/CR/Sep08) [2010] ZACT 21 (17 March 2010)*. South African Legal Information Institute. http://www.saflii.org/za/ [Accessed 7 March 2016].

[23] *Competition Act No. 89 of 1998 (Date of commencement of sections 1-3, 6, 11, 19-43, 78, 79 & 84 on 30 November 1998. The remaining sections of the Act commenced on 1 September 1999.)* Competition Commission. http://www.compcom.co.za/ [Accessed 15 March 2016]. Ch. 2 part A section 5.

5.6. Restrictive Agreements

EU competition law is concretising the general provision of Article 101 of the Treaty on the Functioning of the European Union (TFEU) on restrictive vertical agreements through regulation 330/2010 on Vertical Restraints[24], the supposed block exemption regulation.

Together with the Guidelines on Vertical Restraints released by the Commission,[25] the key factor in the assessment of vertical agreements is the existence of market power. Regulation 330/2010 exempts contractual arrangements if both parties hold less than thirty percent market share in their respective markets. Again, the market definition plays a significant role; the more the market is fragmented, for instance, in SaaS, PaaS and IaaS, the more likely the mentioned market ratio will be exceeded.[26]

a) *Threshold exceeded.* If either party exceeded the thirty percent threshold, the block exemption, Regulation 330/2010, would not be applicable and the vertical agreement must be assessed under Article 101 of the TFEU. Therefore, the crucial fact involves the question whether suitable alternatives in the form of other cloud service providers are available. Since cloud services are offered on a global scale, the substitutability condition should be fulfilled; however, an alternative to the given ISP is usually not present.

b) *Below threshold.* If the market share is below the threshold of thirty percent, then the vertical agreement can be justified if it does not contain a supposed blacklist restriction which defeats the application of Regulation 330/2010.[27] Such types of blacklist issues are resale price, maintenance and long-lasting non-compete obligations.[28]

Comparable to the EU Competition regulation, the South African Competition Act[29] prohibits agreements and concerted practices irrespective of whether they constitute a deal by

[24] *Commission Regulation (EU) No. 330/2010 of 20 April 2010 on the application of Article 101(3) of the Treaty on the Functioning of the European Union to categories of vertical agreements and concerted practices*. Eur-Lex. http://eur-lex.europa.eu/ [Accessed 20 April 2016].
[25] Information from European Union Intuition's, Bodies, Offices and Agencies European Commission. (2010) *Guidelines on vertical restraints (2010/C 130/01)*. Eur-Lex. http://eur-lex.europa.eu/ [Accessed 12 January 2016].
[26] SLUIJS, J.P. et al. (2012a) *Cloud computing in the EU policy sphere interoperability, vertical integration and the internal market.* Tilburg Law and Economics Center. https://www.jipitec.eu/ [Accessed 12 January 2016].
[27] Idem. p. 52
[28] Idem. p. 52 (article 5)
[29] *Competition Act No. 89 of 1998 (Date of commencement of sections 1-3, 6, 11, 19-43, 78, 79 & 84 on 30 November 1998. The remaining sections of the Act commenced on 1 September 1999.)* Competition Commission. http://www.compcom.co.za/ [Accessed 15 March 2016].

companies or groups of companies which compete against each other and whose contracts either prevent, restrict or reduce competition and may also exclude competition. Practices or agreements of this nature frequently include the direct or indirect setting of procurement and selling prices as well as setting trade conditions and market segmentation, by the allotment of suppliers and clients. They also may include the pricing structures and areas, as well as specific products or services and finally collusion on tendering.

5.7. Abusive Market Behaviour

a) *Market dominance.* Another competition law restriction is abusive behaviour in the event of market dominance according to Article 102 of the TFEU. Market dominance is assessed along the lines of the described market definitions;[30] the narrower the market is designed, the more likely market dominance exists. Vertical integration of a cloud service provider by an ISP, which does not satisfy the requirements of a dominant market position, is not governed by competition law.[31]

In practice, abusive behaviour often consists of pricing margins depletion or predatory pricing.[32] Currently, the cloud market is dominated by only a handful of big providers; these are Microsoft, Google, Amazon and Dropbox. Smaller service providers are emerging. However, their focus is mostly on a limited market segment targeting mainly the more lucrative commercial utilisation in the private cloud, while users are accustomed to receiving elementary cloud services free of charge, in other words, cloud email and limited cloud data storage.

Since the larger service providers mentioned above have already set up the required infrastructure, they might be inclined to deter further competition. Service providers such as Amazon could consider a predatory pricing strategy as its servers are used for their primary business, which is the online sale of goods. Offering its unused capacity is only an additional add-on and does not necessarily need to be sustainably priced. Over the last few years, a sharp fall in cloud service prices has occurred. Amazon was the first to reduce its pricing, followed by Microsoft and then other market service providers.[33] At first glance the

[30] OSTERUD, E. (2013) *EU Competition Law - abuse of dominance (Article 102 TFEU)*, University of Oslo., http://www.uio.no/studier/ [Accessed 23 April 2016].
[31] SLUIJS, J.P. (2012) *Network neutrality and internet market fragmentation*. TILEC Discussion Paper No. 2012-015, Common Market Law Review, 49 (5). 2012. https://papers.ssrn.com/ [Accessed 24 April 2016].
[32] HAY, G.A. (1982) *The economics of predatory pricing*. Cornell Law School. http://scholarship.law.cornell.edu/ [Accessed 26 April 2016].
[33] BORT, J. (2015) *Google just took the lead in the dangerous game called 'race to zero'*. Business Insider. http://www.businessinsider.com/ [Accessed 30 April 2016]. See also WATROUS, L. (2016)

development appears to be an advantage for the cloud user, but on closer inspection, the dominant market position of the large service providers remains concrete. Furthermore, the market entry barrier is increased for new competitors due to the lower profit margins which result in an extended period to recoup the initial setup costs for the new hardware and software. Thus, large service providers with established infrastructure systems as well as the financial resources, which are already active in the market, are advantaged.

Additionally, classifying any action as predatory pricing is complicated as generally competitive pricing is allowed. An accurate assessment of the circumstances and timing of the operations is, therefore, essential in determining whether a service provider is selling under its costs to drive competition out of the market.

The most critical issue in the context of abusive market behaviour is access to the market. For example the refusal of an ISP to deal with non-affiliated cloud service providers, given the fact that the web service provider is tied into a vertically integrated scheme with another cloud service provider.[34]

The detailed competition law assessment of such a situation depends on the interpretation of the Commission's guide paper on Article 102 of the TFEU providing its opinion on the interpretation of the relevant term 'discrimination'.[35] Furthermore, the European Courts often deal with the abusive behaviour of IT and Telecommunications provider enterprises,[36] for example in the France Telecom case.[37]

Wanadoo,[38] a France Telecom subsidiary engaged in the sale of internet service access, which was provided with Asymmetrical Digital Subscriber Line (referred to as ADSL) services by its parent company while competing on the market with other such service providers. The other market participants were required to buy the ADSL service from France Telecom, which

---

The cloud and the race to zero: Amazon and Google go at I.T. Huffington Post. http://www.huffingtonpost.com/ [Accessed 14 December 2016].

[34] SLUIJS, J.P. et al. (2012a) *Cloud computing in the EU policy sphere interoperability, vertical integration and the internal market.* Tilburg Law and Economics Center. https://www.jipitec.eu/ [Accessed 12 January 2016].

[35] *Information from the European Union Institutions and Bodies Commission. (2009) Communication from the Commission, Guidance on the Commission's enforcement priorities in Applying Article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings (2009/C 45/02)*. Eur-Lex. http://eur-lex.europa.eu/ [Accessed 19 February 2016].

[36] DOLMANS, M. and LEYDEN, A. (n.d.) *Internet & antitrust: An overview of EU and national case law*. Competition Laws Bulletin. https://www.clearygottlieb.com/ [Accessed 4 May 2016].

[37] *France Telecom SA v. Commission of the European Communities. Case C-202/07 P*. Curia Europa. http://curia.europa.eu/juris/ [Accessed 6 May 2106].

[38] *Ibid.*

had a monopoly on the service. However, Wanadoo sold its services to customers below actual 'production' costs and thus utilised a well-conceived scheme of malevolent pricing aimed at pre-empting the calculated market for high-speed internet access at the expense of its competitors.[39] While the customers were better off in the short term because of this malevolent pricing, they would have ultimately had to bear higher costs once the competitors disappeared from the market. Therefore, the European Court of Justice (referred to as ECJ) sanctioned France Telecom for its anti-competitive behaviour.[40]

This case credibly shows that the potential for market abuse and anti-competitive conduct is real. Recently, Telekom Drossel announced that it would cap all its customers' broadband connections to a maximum gigabyte amount.[41] This cap, would, however, not apply to data received from services provided by its partner for film and music streaming portal.

It remains to be seen whether other ISPs will follow this same behaviour. If so, the portal usage of cloud services would be severely impaired as it relies heavily on bandwidth due to its decentralised nature.

b) *Refusal to supply.* Another critical behaviour could consist of the refusal to provide a service, either actual or constructive. An illegal vertical integration is to be assumed in the case of cloud service providers and ISPs' integration with the subsequent foreclosure of rival cloud service providers upstream or competing ISPs downstream.[42] However, duties to supply a service are considered to have the potential of exerting an adverse effect on innovation. Ensuring constant market access by forcing a particular stream from ISPs will likely outweigh the potentially detrimental effect a decision not to stream services to a party would have. Competition would break down as it can only take place in a market in which the ISPs currently regulate access. A mandatory rule relating to the relevant Directives and Regulations could mitigate the potential limitations ISPs try to put on cloud service providers' broadband communication. The European Courts have analysed the particular problems mainly in the following case, *Oscar Bronner GmbH & Co. KG v. Mediaprint Zeitungs- und Zeitschriftenverlag*

[39] BAVASSO, A. (2009) *Recoupment in predatory pricing: France Telecom v. Commission*. Allan and Overy. http://www.allenovery.com/ [Accessed 8 May 2016].
[40] France Telecom SA v. Commission of the European Communities. Case C-202/07 P. Curia Europa. http://curia.europa.eu/juris/ [Accessed 6 May 2106].
[41] DOBSCHAT, C. (2013) *Surprise: Telekom-Drossel for all customers and traffic exceptions for "Partner" confirmed.* Mobile Geeks. https://translate.google.com/ [Accessed 8 May 2016].
[42] SLUIJS, J.P. et al. (2012a) *Cloud computing in the EU policy sphere interoperability, vertical integration and the internal market*. Tilburg Law and Economics Center. https://www.jipitec.eu/ [Accessed 12 January 2016].

GmbH & Co. KG Case C-7/97;[43] Article 86 of the EC Treaty - Abuse of a dominant position - Refusal of a media undertaking holding a dominant position in the territory of a member state to include a rival daily newspaper of another business in the same member state in its newspaper home-delivery scheme;[44] as well as *Microsoft Corp. v. Commission of the European Communities, Case T-201/04.* ('Microsoft').[45]

In the *'Bronner'* case, a three-pronged test was introduced. It looked at the questions of whether the essential facility or infrastructure of an ISP is indispensable as a facility for a cloud service provider to deliver access to its customers, irrespective of the option of alternative modes of transport inside the same market.[46] The test addressed the question of whether the dominant party's refusal was 'likely to eradicate all other competition on behalf of the party pursuing access.'[47]

In the *'Microsoft'* case, it was considered that it had to be proven that access to the interoperability information controlled by 'Microsoft' was indispensable to compete in the workgroup server market.[48] Applying this reasoning to a potential market abuse situation in which an ISP refuses access to a competing cloud service provider, the determinative factor would be whether such action is likely to eliminate all competition by other cloud service providers. As an ISP fulfils a central function in the free flow of data, such a decision not to service a cloud service provider or user will seriously impair the functioning of the internet. Thus the ISP must give the cloud service provider access; otherwise competition on the market would not be possible or only operate in a negligible fashion.

The case surrounding Article 9a of the German Telecommunications Law of 2004 highlighted that actions with respect to the implementation of regulatory measures aimed at ensuring competition in the market have to be taken by the National Regulatory Authorities and not by

---

[43] *Oscar Bronner GmbH & Co. KG v. Mediaprint Zeitungs- und Zeitschriftenverlag GmbH & Co. KG, Mediaprint Zeitungsvertriebsgesellschaft mbH & Co. KG and Mediaprint Anzeigengesellschaft mbH & Co. KG, Case C-7/97 (1998)*. Curia Europa. http://curia.europa.eu/ [Accessed 15 May 2016].
[44] *Ibid.*
[45] *Microsoft Corp. v. Commission of the European Communities Case T-201/04. (2007)*. Curia Europa http://curia.europa.eu/ [Accessed 15 May 2016].
[46] *Oscar Bronner GmbH & Co. KG v. Mediaprint Zeitungs- und Zeitschriftenverlag GmbH & Co. KG, Mediaprint Zeitungsvertriebsgesellschaft mbH & Co. KG and Mediaprint Anzeigengesellschaft mbH & Co. KG, Case C-7/97 (1998*). Curia Europa. http://curia.europa.eu/ [Accessed 15 May 2016].
[47] *Ibid.*
[48] *Microsoft Corp. v. Commission of the European Communities Case T-201/04., (2007)*. Curia Europa. http://curia.europa.eu/ [Accessed 15 May 2016].

the national legislator.[49] In this case, the German parliament fundamentally passed a blanket exemption applicable to parts of the German Telekom network, thus limiting the abilities of the National Regulatory Authorities to regulate these systems. In principle, the independence required from a market regulator was undermined by allowing the legislator to interfere in its decision-making process. The ECJ correctly concluded that Germany had violated EU Law.[50] The National Regulatory Authorities are better equipped to assess a market situation on a case by case basis and act by imposing measures before the event occurs (*ex-ante* measures).[51]

Article 114 of the TFEU allows EU institutions to synchronise laws across the EU when they diverge to such an extent that it jeopardises the internal market. The boundaries of the EU's competence in taking measures to achieve its goal are not entirely clear. From one perspective, the ECJ has expressed its view that mere disparities between regulatory approaches are insufficient to justify synchronisation action and that an actual and real obstacle is required.[52] Likewise, from another perspective, subsequent cases have indicated that the court has understood the rapid technological development will invariably lead to a differing approach across the member states and thus a degree of flexibility is necessary to allow the EU institutions to achieve their objective of synchronising diverging national legislations.[53] Nevertheless, any synchronisation regulation must be firmly linked to the purpose of the regulatory framework.[54] It has been argued that consumer protection under Article 95(3) of the European Commission (EC) would justify an increase in synchronisation of the telecommunications market even if negative consequences of such action was

[49] E*uropean Commission v. Federal Republic of Germany. Failure of a Member State to fulfil obligations – Electronic communications – Directive 2002/19/EC – Directive 2002/21/EC – Directive 2002/22/EC – Networks and services – National rules – New markets. Case C-424/07. (2009*). Curia Europa. http://curia.europa.eu/ [Accessed 15 May 2016].

[50] *Directive 2002/19/EC of the European Parliament and the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive)*. Eur-Lex. http://eur-lex.europa.eu/ [All accessed 18 May 2016].

[51] *European Commission v. Federal Republic of Germany. (Advocate General Opinion) Case C-424/07. (2009)* Curia Europa. http://curia.europa.eu/ [Accessed 15 May 2016].

[52] *Federal Republic of Germany v. European Parliament and Council of the European Union. Directive 98/43/EC – Advertising and sponsorship of tobacco products – Legal basis – Article 100a of the EC Treaty (now, after amendment, Article 95 EC). Case C-376/98.* Curia Europa. http://curia.europa.eu/ [Accessed 15 May 2016].

[53] *United Kingdom of Great Britain and Northern Ireland v. European Parliament and Council of the European Union. Regulation (EC) No 460/2004 – European Network and Information Security Agency – Choice of legal basis. Case C-217/04*. Curia Europa. http://curia.europa.eu/ [Accessed 17 May 2016].

[54] Idem. par. 47.

envisaged for market operators.[55] Thus, it seems that the ECJ would not overturn efforts by the Commission to regulate network management.[56]

To achieve the efficiency gains brought about by the use of cloud services, vertical integrations must be closely scrutinised as they could potentially have a significant effect on the growth of cloud technology in the future.[57] Cloud service providers have the ability to utilise a variety of ISPs which in turn also makes an ISP seem more attractive to a customer because of the cloud systems that can potentially be used through its network.[58] In the USA, a cloud service provider agreement with all ISPs is very easy to achieve as there are only a few large service providers. However, in Europe every country has a few service providers, thus reaching an agreement with all of them is nearly impossible.[59] Furthermore, the network management policies in most EU countries differ, which creates issues as to the uniformity of transfer between EU members.

Europe has recently seen an increase in cases relating to broadband access. The *Telecom Italia* case in 2013 highlights how network infrastructure owners abuse their dominant position and try to deter competition by treating orders from their internal divisions favourably to those of other service providers.[60] Having imposed a heavy fine on Telecom Italia in the order of 103MEU seems warranted due to the tremendous impact which service access has on every single internet user and service provider.[61]

---

[55] *The Queen, on the application of Vodafone Ltd and Others v. Secretary of State for Business, Enterprise and Division (Administrative Court) – United Kingdom. Regulation (EC) No 717/2007 – Roaming on public mobile telephone networks within the Community – Validity – Legal basis – Article 95 EC – Principles of proportionality and subsidiarity Regulatory Reform. Reference for a preliminary ruling: High Court of Justice (England & Wales), Queen's Bench. Case C-58/08*. Curia Europa. http://curia.europa.eu/ [Accessed 17 May 2016].

[56] SLUIJS, J.P. (2012) *Network neutrality and internet market fragmentation*. TILEC Discussion Paper No. 2012-015, Common Market Law Review, 49 (5). 2012. https://papers.ssrn.com/ [Accessed 24 April 2016].

[57] ODLYZKO, A. (2009) *Network neutrality, search neutrality, and the never-ending conflict between efficiency and fairness in markets*. University of Minnesota. http://www.dtc.umn.edu/ [Accessed 14 May 2016].

[58] ROCET, J.C. and TIROLE, J. (2003) *platform competition in two-sided markets*. Research Center for Humanities and Social Sciences. http://www.rchss.sinica.edu.tw/ [Accessed 22 May 2106].

[59] SLUIJS, J.P. et al. (2012a) *Cloud computing in the EU policy sphere interoperability, vertical integration and the internal market.* Tilburg Law and Economics Center. https://www.jipitec.eu/ [Accessed 12 January 2016].

[60] Anonymous. (2013) *A428 - TLC: Antitrust, Telecom Italia abused its dominant position in the network infrastructure*. Autorità Garante Della Concorrenza e Del Mercato. http://www.agcm.it/en/ [Accessed 17 May 2016].

[61] *Ibid.*

The EU has left the market open by allowing the ISPs to manage traffic within the boundaries of competition law as long as they communicate their actions clearly to customers. As a counterweight to any imbalance created, the national regulators can set minimum standards that have to be maintained with regard to all network transmissions.[62] Ultimately a differing level of service provided in various member states will affect the customers through different pricing and access. The outcome of Telecom Italia case was not the result expected and did not align with the goal of one internal European market without boundaries.

Nevertheless, suggestions have been made to distinguish the necessary harmonisation process by focusing on areas where the benefits will be the maximised, specifically, against the prospects of economies of scale. They will be delivered through technology or by external cross-country measures where lower costs are achieved, more specifically based on the quality of being diverse and not comparable with general preferences or selections, or the need to compensate for regulatory experiments.[63]

5.8. A South African Perspective of Abusive Market Behaviour

The South African perspective of abusive market behaviour changed in 1994 with the transition to democracy. The transition brought about significant changes to key industries which dominated the marketplace. In some instances these large companies continue to enjoy market dominance, supported by the State. However, in the late 1990s the South African Competition Act[64] was drafted, promoting the entry of small and medium businesses into markets which were previously impenetrable due to the dominant positions of larger companies.

The establishment of the South African competitions enforcement agencies would indicate to some degree that abusive behaviour by dominant companies was very

[62] HOU, L. et al. (2008) *Network neutrality in Europe*, Eurocpr. http://www.eurocpr.org/ [Accessed 21 May 2016].
[63] STREEL, A. (2012*) Where should the European Union intervene to foster the internal market for eComms?* SSRN. https://papers.ssrn.com/ [Accessed 7 April 2016].
[64] *Competition Act No. 89 of 1998 (Date of commencement of sections 1-3, 6, 11, 19-43, 78, 79 & 84 on 30 November 1998. The remaining sections of the Act commenced on 1 September 1999.)* Competition Commission. http://www.compcom.co.za/ [Accessed 15 March 2016].

prevalent and that the provisions of the Competitions Act were 'under-enforced.'[65] Lewis (2008) said

> Under-enforcement is the likely upshot even in an economy whose history and structure suggests the substantial likelihood of anticompetitive unilateral conduct and whose enforcement agencies are firmly committed to enforcing the rules prescribing this type of behaviour.[66]

The South African Competition Act has one potential area of concern, which relates to the most unusual aspect of 'rules-based' interpretation of exclusionary abuse of dominance. A view of Section 8 of the Competitions Act shows a list of distinct exclusions, which includes items such as refusal to supply and buy and below-cost pricing. These aspects are prohibited if involved with a dominant company. Where such companies also have anti-competitive impacts, which are not outweighed through technology, pro-competitive gains or efficiencies, these aspects may be contrasted with leading competition law practitioners in particular in cases where abuse of dominance was widely stated as unlawful by current legislation.

The duty of setting specific acts that would trigger the application of the statues is in the hands of the authorities and the Courts, guidelines and case precedents. The primary question to be addressed is which of South Africa's 'rules-based' interpretations of exclusionary abuse of dominance provisions are 'fit-for-purpose', or would a single, open-source effects-based interpretation be more applicable and if it is comparable to the EU and the USA standards?[67]

There is an increasing accord in the international arena regarding the development of the rules of law which prohibit specific anti-competitive behaviour. A fundamental question about this is whether these provisions should be included in South African legislation? Providing an answer would necessitate analysing both the advantages and disadvantages of sections 8(c) and 8(d) of the Competitions Act. On the one hand, if the outcome of the analysis had a few limited benefits within the present structure and if the disadvantages are numerous and vigorous, it would create a desirable position to amend the Competitions Act. A situation of this nature

---

[65] ROBERTS, S. (2011) *'Administrability and business certainty in abuse of dominance enforcement: An economist's review of the South African record'*. Compcom. http://www.compcom.co.za/ [Accessed 8 August 2016].

[66] LEWIS, D. (2008) *'Chilling competition'. Hawk ed. International Antitrust Law and Policy: Fordham Competition Law*. New York: Juris Legal Information. p. 428.

[67] MACKENZIE, N. (2014) *Rethinking exclusionary abuse in South Africa*. Competition Commission. http://www.compcom.co.za/ [Accessed 22 April 2016]. See also MACKENZIE, N. (2012) *Working paper, replacing Section 8(D) of the Competitions Act with an Effects-Based Exclusionary Abuse of Dominance Provision.* Centre for Competition Economics. http://static1.squarespace.com/ [Accessed 25 April 2016].

would only be possible if the cost of amending the Act would be warranted. On the other hand, if the advantages were to outweigh the disadvantages, there would be no requirement to modify the Act.[68]

The primary benefit of the Competitions Act in South Africa is the uncharacteristic approach which was proposed that the Act tolerates a disgraceful abusive form of practice which must be treated more severely. In turn, it improves on administration capability, ensures legal certainty, encourages effective deterrence and affords comfort that rules founded on international best practice are entrenched in the South African competition law. Legal practitioners argue that such expected advantages have not yet been recognised in practice.

Following the Competitions Act inauguration, some of the limited and standing descriptions of exclusionary behaviour continue to exasperate actual enforcement, which adds to the low-performance results or stated as under-inclusive as observed by Lewis (2008).[69] The argument about the provisions of the Competitions Act which prohibit exclusionary abuse of dominance appears to no longer be 'fit-for-purpose'. Moreover, the legislature ought to consider exchanging the applicable sections with a single, open-source effects-based interpretation prohibition, which would be disciplined through administration penalties for first-time violators.[70]

Given the risks of under-inclusion, the outcome of proving abuse of dominance in South Africa with such hurdles as mentioned would be difficult at best. Moreover, this is evident from the small number of cases which involved exclusion and with the extensive evidence required since the inauguration of the Competition Acts in 1999. There have been four companies decisively convicted of an exclusionary abuse of dominance, although only two have been ordered to pay penalties.

> The Supreme Court of Appeal's decision in the Senwes case was overturned by the Constitutional Court on 12 April 2012 (thereby upholding the Tribunal's decision finding Senwes to have contravened section 8(c) by committing a margin squeeze).[71]

---

[68] *Ibid.*

[69] LEWIS, D. (2008) *'Chilling competition'. Hawk ed. International Antitrust Law and Policy: Fordham Competition Law*. New York: Juris Legal Information.

[70] MACKENZIE, N. (2014) *Rethinking exclusionary abuse in South Africa*. Competition Commission. http://www.compcom.co.za/ [Accessed 22 April 2016].

[71] ADAM and ADAMS (2012). *Senwes: A victory for the Competition Commission but a potential Pandora's Box*, Polity. http://www.polity.org.za/ [Accessed 29 April 2016].

Commission v. Senwes Case CCT 61/11 [2012] ZACC 6 and the Tribunal has found Telkom guilty of contravening sections 8(b) and 8(d)(i) on 7 August 2012 in Commission v. Telkom SA Ltd case 11/CR/Feb04.[72]

5.9. Conclusion

From the above discussion, it is clear that there is a need to harmonise competition legislation on a global level. Ensuring a uniform approach to regulation has many benefits. Mainly it will enable the ISPs to offer the same service across all countries with economies of scale and supply cloud users with a reliable and uniform service throughout the globe.[73] Cloud service providers remain specifically interested in a consistent framework as they otherwise would have to deal with situations in which data transmitted by way of a country with weak regulatory standards, and thus low base service levels, affects their customers in other markets or states where the service level is high. Interestingly, it appears as if the EU members are creating incentives to implement stricter legislation than that of the current EU level. Such action should be an inspiration for other countries to follow suit and enhance their laws to similar or the same levels as that of the EU member states.

[72] *Commission v. Senwes Case CCT 61/11 [2012] ZACC 6 and the Tribunal has found Telkom guilty of contravening sections 8(b) and 8(d)(i) on 7 August 2012 in Commission v Telkom SA Ltd case 11/CR/Feb04*. Competition Tribunal. http://www.comptrib.co.za/ [Accessed 29 April 2016].

[73] SLUIJS, J.P. (2012) *Network neutrality and internet market fragmentation*. TILEC Discussion Paper No. 2012-015, Common Market Law Review, 49 (5). 2012. https://papers.ssrn.com/ [Accessed 24 April 2016].

6. Cloud Data Protection Regulation

6.1. Introduction

The advantages of cloud services make it attractive to an extensive range of business, public and governmental customers, from all sizes of enterprises, which lack the resources or expertise capable of administrating a complex and expensive internal IT platform, to larger international corporates attracted to each other for potential financial benefits.

Nonetheless, in spite of the complex administration and economic benefits of using the cloud, there are numerous information security and privacy protection issues, especially when the cloud is used for processing or handling personal information. The problems result from the various business, public and governmental customers' ostensible lack of control over and oversight of the way in which personal information is protected and managed within each customer's domain.

The discussion covers problem areas that cloud customers should consider when making decisions to engage the services of a cloud service provider. A view of the fundamental data protection principles behind the obligations of data users and data controllers[1] and then provides the more common data protection issues which enterprises experience when pursuing the services of a cloud service provider. The discussion provides an outline of some business model characteristics which cloud service providers have adopted and how these characteristics impact on the protection of personal data and data privacy. The inputs provided below should be deliberated when enterprising customers consider or address engaging the services of a cloud service provider.

6.2. Cloud Service and Deployment Models

There are numerous categories and characteristics of cloud. For the purpose of this segment the focus will be on the following service models and deployment models, with due consideration to the applicable privacy and personal data protection: private and public cloud

[1] A number of data protection laws define the data user and data controller as the bodies that gather, use and store such personal data belonging to the data subject or individuals.

service models, incorporating SaaS, PaaS and IaaS, deployment models, as discussed in the Technical Description.[2]

The relevant service models, private and public clouds

The private cloud is intended for the exclusive use of private organisations and organisational customers should be in a position to mandate all the necessary controls to safeguard personal data that the agency has entrusted to the selected cloud service provider. In contrast, public cloud models are meant to be shared by multiple customers with a variety of different customer needs. Hence the public cloud service providers tend to make the cloud platforms as generic as designs will allow engaging and drawing as many customers as possible. As such, the level of provision and controls exercised by organisational clients of public clouds is inevitably much lower when compared to that of private cloud service providers.

As far as personal data protection is concerned, the primary distinction between the various deployment models is that in using the SaaS model, the cloud service provider also supplies and frequently operates the related software for the data users. In the SaaS model the software that the cloud service provider offers may not be completely customisable to the data customers' or users' compliance and security requirements. This is because the public cloud service providers need to serve a large number of clients with the same software. It should also be noted that some SaaS cloud service providers cooperate directly with data users' customers, which renders the roles and responsibilities of each party in respect of 'who is collecting what personal data' and for 'what purpose', even hazier. The PaaS and IaaS models, in contrast, allow data users to install their software, which can safely be assumed to be more readily compliant with specific business, security and regulatory requirements of the data users

6.3. Cloud Concerns for Data Protection Authorities

Cloud computing is undoubtedly a very attractive business enabler, offering such benefits as a short lead time, minimal investment and ease of use for any business initiative or operation that requires IT support. Gartner, a market leading IT research and advisory firm, estimated that the cloud would grow from 11 billion dollars in 2012 to 244 billion in 2017.[3] However, given the attractiveness of cloud it should not be forgotten that there are still the inherent risks, such

[2] Information Systems Audit and Control Association. (2011) *IT control objectives for cloud computing: Controls and assurance in the cloud*. ISACA. http://www.isaca.org/ [Accessed 12 February 2016].
[3] GARTNER Inc. (2013) *Forecast: Public cloud services, worldwide, 2011-2017, 4Q13 Update*. Gartner. https://www.gartner.com/ [Accessed 7 December 2015].

as those risks related to the lack of control, security, privacy and personal data protection when entrusting confidential data to a third party or cloud service provider for either data handling or data storage.

The EU had set up a Working Party by Article 29 of the Data Protection Directive 95/46/EC (1995) which consists of agents from each of the Member States Data Protection Authorities as well as the EU Commission and Data Protection Supervisor. Among its aims are to advise the EC and make recommendations to the EU concerning all matters about the protection of personal data. It considers the lack of control over and the deficiency of information about the cloud operations to be the two key risks associated with the use of cloud.[4]

The South African interpretation provides protection through the POPI Act.[5] Many of the provisions of the POPI Act are similar to those found in the now repealed EU Data Protection Directive 95/46/EC (1995),[6] and one can see where the inspiration originates. The Scope of Application of the POPI Act applies to processing data, which is captured on record by a responsible party that is (1) domiciled in South Africa or (2) making use of means located in South Africa. The scope is similar to that of the EU Directive's applicable rules, as the POPI Act applies to data processing; firstly by or on behalf of a South African based 'organisers', for instance: by data processors for South African companies or secondly when an organiser uses services and infrastructure means for data processing located in South Africa.

EU Regulation 2016/679 Article 50 (Conflict), is in contrast with the regulation's antecedent, the EU Directive 95/46 (1995). Nevertheless, there is a particular provision in circumstances of conflict with supplementary laws. The POPI Act relates to the exclusion of any other data protection rules or laws that are applicable, unless such rule or law, 'provides for circumstances for the lawful handling of personal data' that are more common than those set out in the POPI Act conditions for the authorised processing, the wide-ranging conditions prevail.

[4] European Commission. (2012) *Article 29 Data Protection Working Party*. EC Europa. http://ec.europa.eu/justice/ [Accessed 9 January 2016].
[5] *The Protection of Personal Information Act No. 4 of 2013 of South Africa, Policy, Law, Economics and Politics*. http://www.polity.org.za/ [Accessed 6 December 2015].
[6] *Directive 95/46/EC of the European Parliament and 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.* EC Europa. http://ec.europa.eu/justice/ [Accessed 22 April 2016].

Many other countries provide data protection laws.[7] However, data users take the ultimate responsibility for and are accountable for the safekeeping and use of personal data under their control, even when they outsource the processing thereof to other parties.

The data users should take the appropriate measures to ensure that personal data should not remain utilised for anything other than the purpose for which it was originally specified. Moreover, to keep it no longer than necessary and protect it against unauthorised or accidental access, processing erasure, loss or use no matter whether they are processing the data themselves or have entrusted it to a third party to do so. They should accordingly fulfil their obligations under the law; data users must safeguard that adequate controls stay specified in both their requirements and any agreements they negotiate with the outsourced data processors.

As previously illustrated, cloud services are considered as a unique method of outsourced service; data users will find the various business models somewhat different from the usual outsourced business models, with the exception of private cloud where cloud services are dedicated to a single client and their requirements.[8] Data users may be unable to exert the level of control they typically can in the one-on-one relationship with the traditional outsourcer. Data users may also be unaware of some of the cloud characteristics that have a potential negative impact on personal data privacy.

6.4. General Data Protection Standards

Currently, more than 100 countries and jurisdictions have introduced data protection laws since the early 1970s.[9] The majority of these countries subscribe to the core standards of the Organisation for Economic Co-operation and Development (referred to as OECD 2013) Privacy Guidelines on the Protection of Privacy and Cross-border Flows of Personal Data, which were initially published in 1980.[10] The guidelines have since been an updated with an

[7] GREENLEAF, G. (2015) *Global data privacy laws 2015: 109 countries, with European laws now a minority.* Privacy Laws & Business International Report. SSRN. http://papers.ssrn.com/ [Accessed 8 December 2015].
[8] National Institute of Standards and Technology. (2011) *The NIST definition of cloud computing SP 800 – 145.* CSRC. http://csrc.nist.gov/ [Accessed 28 November 2015].
[9] GREENLEAF, G. (2015) *Global data privacy laws 2015: 109 countries, with European laws now a minority.* Privacy Laws & Business International Report. SSRN. http://papers.ssrn.com/ [Accessed 8 December 2015].
[10] Organisation for Economic Cooperation and Development. (2013) *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data [C (80)58/FINAL, as amended on 11 July 2013 by C (2013)79] extract of Part Two.* OECD. https://www.oecd.org/ [Accessed 8 December 2015].

amendment in July of 2013. There is particular interest in addressing the core standards and specifically about personal data and the Cloud. The POPI Act provides the following personal data protection in Chapter 2 section 5, Rights of data subjects,[11]

> A data subject has the right to have his, her or its personal information processed by the conditions for the lawful processing of personal information as referred to in Chapter 3 conditions of data processing.

The guidelines are appropriate to personal data, irrespective of the personal data being in the private or public domains, which, either because of the method of processing or the nature and context of utilisation, poses a risk to the individual's privacy rights. The data processing conditions are corresponding and are read together. The conditions should not be interpreted as,

a) preventing the application of different protective measures to various categories of personal data, depending on their nature and the context in which they are collected, stored, processed or disseminated; or
b) in a manner which unduly limits the freedom of expression.[12]

There are some exceptions to the conditions which include aspects relating to national security, national sovereignty and public policy (*Ordre public*), and should be,

a) as few as possible, and
b) made known to the public.

The data processing conditions remain as the minimum level of data handling and can be complemented by additional data protection means for the individual's privacy rights. The added regulations may impact on cross-border data flows of personal data.

The underlying data processing conditions extracted from the POPI Act, 'Chapter 3 Conditions for Lawful processing of Personal Information' *Part A, Processing of personal information in general,*[13] as well as part two of the (OECD 2013) Guidelines Governing the Protection of Privacy and Cross-border Flows of Personal Data[14] are addressed.

---

[11] *The Protection of Personal Information Act No. 4 of 2013 of South Africa, Policy, Law, Economics and Politics.* http://www.polity.org.za/ [Accessed 6 December 2015].
[12] Organisation for Economic Cooperation and Development. (2013) *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data [C (80)58/FINAL, as amended on 11 July 2013 by C (2013)79] extract of Part Two*. OECD. https://www.oecd.org/ [Accessed 8 December 2015].
[13] *Ibid.*
[14] *Ibid.*

A. Accountability - Condition 1

The responsible party is to ensure conditions for lawful processing. The responsible party must ensure that the conditions set out in this chapter, and all the measures that give effect to such conditions are complied with at the time of the determination of the purpose and resources of the processing and during the processing itself (POPI Act).

Data users should be accountable for compliance with measures that give effect to the above conditions, as well as with measures to address incident response and breach handling. If data users are to engage cloud services that involve personal information, they should formally assess all privacy impacts through a privacy impact assessment. Furthermore, data users should ensure that the cloud service providers they choose have appropriate incident response and breach handling procedures in place (OECD 2013).

B. Process Limitation and Collection Limitation - Condition 2

The legitimacy of processing, minimality, consent, justification and objection and collection directly from data subject (POPI Act).

There should be limits to the gathering 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 subject (OECD 2013).

C. Purpose Specification - Condition 3

The data collection for a particular purpose, retention and restriction of records (POPI Act).

The objectives 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 fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose (OECD 2013).

D. Further Processing or Use Limitation - Condition 4

Further processing to be compatible with the purpose of collection (POPI Act).

Personal data should not be disclosed, made available or otherwise used for purposes other than those specified by Paragraph 9 except: with the consent of the data subject; or by the authority of law (OECD 2013).

E. Data or Information Quality - Condition 5

The quality of the information collected (POPI Act).

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 (OECD 2013).

F. Openness - Condition 6

Documentation, notification to data subject when collecting personal information (POPI Act).

There should be a general policy of openness about developments, practices and policies on personal data. Means should be readily available for establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller (OECD 2013).

G. Security Safeguards - Condition 7

Security measures on integrity and confidentiality of personal information. Information processed by operator or person acting under authority; security measures regarding information dealt with by an operator; notification of safety compromises (POPI Act).

Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data (OECD 2013).

H. Data Subject or Individual Participation - Condition 8

Access to personal information, correction of personal information, manner of access (POPI Act).

An individual should have the right to confirm whether a data user has held his or her personal data. He or she should also be entitled to obtain a copy of such data within a reasonable period and in a reasonable manner, and to have the data erased, rectified, completed or amended as appropriate.

When engaging cloud services, data users must ensure that cloud service providers can support data users' obligations concerning the fulfilment of data access and data correction requests (OECD 2013).[15]

[15] POPI and OECD for all conditions quoted: *The Protection of Personal Information Act No. 4 of 2013 of South Africa, Policy, Law, Economics and Politics*. http://www.polity.org.za/ [Accessed 6 December 2015]. See also Organisation for Economic Cooperation and Development. (2013) *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data [C (80)58/FINAL, as amended on 11 July 2013 by C (2013)79] extract of Part Two*. OECD. https://www.oecd.org/ [Accessed 8 December 2015].

This condition may be especially difficult when a data user is using SaaS services, as the entire software system is designed and operated by the cloud service provider. If the requirements provided above were not taken into account at the design stage or the cloud service providers are unaware of the data users' obligations, it is the data users that would eventually shoulder the legal responsibility for any failure to honour data access and correction requests.

I. Personal Data Free Flow Standard and Legal Restrictions

A jurisdiction may restrict the transfer of personal data to another jurisdiction that does not substantially observe the former's data protection standards.

The final condition requires data users to establish the legal basis for entrusting personal data to cloud service providers that may then transfer the data to other jurisdictions.[16]

6.5. Cloud Business Model Challenges

Data users engaging cloud services should observe all the data protection conditions and standards as listed in the POPI Act and OECD 2013 Directive. Given the nature of cloud services, users should pay particular attention to the conditions, purpose specification, use limitation and security safeguard standards to elaborate on how these conditions and rules relate to data protection and with particular reference to the three primary cloud business models of SaaS, IaaS and PaaS, as previously discussed.

6.5.1. Outsourcing

As previously mentioned the use of the cloud establishes a particular form of outsourcing, and as such all of the challenges related to outsourcing involving the security, privacy and processing of personal data apply. These problems typically include the areas discussed below.

a. Authentication and Identity Management Technical Safeguards

One of the appealing features of cloud services, particularly the public cloud, is its ability to be accessed over the internet from anywhere where a connection is available. While this characteristic meets the mobility needs of the data users, it also allows easier access for hacking and exploitation. The security safeguards standard stipulates that a secure identity

[16] *Ibid* (OECD).

management system of authentication and authorising legitimate users must be in place to protect the personal data stored in the cloud.

b. Data Portability, Data Erasure and Exit Plan

The handling of data after a cloud contract has ended, or after fulfilment of the original purpose of their collection should be well considered. A formal exit plan defining how personal data should be handled and protected in the event of contract completion or mid-term termination is recommended. Furthermore, the agreement should contain a provision ensuring that when personal data is no longer needed or erased, it is indeed permanently deleted and no longer in the cloud service provider's possession. These steps will ensure that the purpose specifications and use limitation standards will be adhered too.

c. Limitation on Data Uses in the Cloud

Cloud service providers are often in a position to receive, handle and access personal data provided by multiple clients. In line with the use limitation standard, cloud service providers should be formally reminded that they cannot retain or use the personal data entrusted to them beyond the terms outlined by individual clients. They also are reminded that they must not aggregate the personal data of multiple clients for new or previously undisclosed purposes.

In other cases, data users may be engaging a SaaS that their customers directly use and access (such as cloud-based payment gateways). When customers interact directly with the SaaS application (payment gateway) the SaaS cloud service provider may be in a position to collect additional information about these clients such as their patterns and locations of access and the types of devices used. Data users must think carefully about who owns such information and what limitations should be obligatory for its use through the purpose specifications standard.

d. Obligations under Individual Participation Standard

Again, if data users are using a SaaS with which their clients interact directly, they need to ensure that the provider of that SaaS is capable of helping the former to meet their obligations by respecting an individual's right to personal data access and correction. In other words, the SaaS provider may need to provide an end-to-end mechanism for fulfilling the access and correction requests from data subjects, or at least support data users in doing so, within a reasonable time frame.

e. Formal Data Breach Management and Notification Arrangements

The accountability standard stipulates that data users should be prepared for all eventualities and among other things pre-develop a data breach handling and notification plan. When a data user engages outside parties such as cloud service providers in handling personal data on its behalf, the plan should involve the active participation of the cloud service providers, provided that it is useful and meaningful.[17]

6.5.2. Cloud Cross-border Data Flows

Many jurisdictional territories with data protection legislation have cross-border data flow restrictions in place that prohibit the transfer of personal data outside their jurisdictions by data users unless specific conditions are satisfied. The RSA is no exception to this rule. The POPI Act[18] in Chapter 1 section 2 (a) (ii), provides for protecting the interests of free flow information and personal data across international borders. The facilitation of incidence regarding the powers of the Act are found at section 40 (a), the EU Regulation 2016/679 (170), and in the Directive in Article 25.[19] Typically, such conditions include the consent of the data subject as well as assurance that the regulator and jurisdictions to which the personal data shall be moved to have implemented a similar standard of protection for the personal data.

Even in instances where it has been recognised that jurisdictions do not have specific cross-border data flow restrictions in their data protection laws, such, as the Canadian Personal Information Protection and Electronic Documents Act,[20] data users cannot merely move collected personal data across borders without considering regulatory limitations and hold points. This is because data users are always responsible for the protection and use of the personal data in their safekeeping. In cases where a data user chooses to transfer the data which they have collected outside of their jurisdictions and any misuse of, or breach of the data occurs as a result of the data transfer, they will be held responsible for the data protection 'Acts' of the jurisdiction in which they operate. The RSA is no exception to these same

[17] Office of the Privacy Commission of Canada. (n.d.) *Cloud computing for small and medium sized enterprises*. OIPC. https://www.oipc.bc.ca/ [Accessed 11 December 2015].
[18] *The Protection of Personal Information Act No. 4 of 2013 of South Africa, Policy, Law, Economics and Politics*. http://www.polity.org.za/ [Accessed 6 December 2015]. Chapter 1 section 2 (a) (ii).
[19] *General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC*. Eur-Lex. http://eur-lex.europa.eu/. [Accessed 23 April 2016]. See also *Directive 95/46/EC of the European Parliament and 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*. EC Europa. http://ec.europa.eu/justice/ [Accessed 22 April 2016].
[20] *Personal Information Protection and Electronic Documents Act Codification. S.C. 2000, c. 5 Current to May 12, 2016 (Last amended on June 23, 2015)*, Minister of Justice. http://laws-lois.justice.gc.ca/ [Accessed 11 March 2016].

conditions. They may also have to find a way of assuring the clients that the customer's personal data, which were relocated to another jurisdiction, will have the same protection that is provided in the RSA.

To allow computing resource exploitation in a time proficient manner, cloud service providers often locate their data centres in multiple territories covering various jurisdictions. To allow the same resource to be shared by clients operating in different time zones as well as different peak hour requirements with high demand, all such activities are occurring at various periods of the day. A useful feature of the cloud and the cloud service providers is the ability to dynamically allocate cloud platform resources to clients in a flexible and optimised method to ensure proficient utilisation of any available resources. The result of this optimised usage is that customers' data may be relocated or moved to any of the cloud service providers' data centres which may be located in more than one jurisdictional territory rather rapidly. From the cloud service providers' viewpoint, the set-up of having distributed data centres in more than one location often stresses the cloud service provider's superior ability to ensure data and capacity availability. If one centre suffers an outage, due to infrastructure failure or natural disaster, the client's data can be shifted seamlessly to one of the alternative data centres that remain unaffected. However, there is always the danger of the cloud service providers not being able to readily identify the location of the clients' data in a prompt manner.[21] Therefore, when engaging a cloud service provider, data users must seriously consider the following implications of cross-border data flows. South African cloud service providers are aware of the risks attached to the cross-border activities and should make clients aware of the same.

a. Risks of Storing Data in Jurisdictions without Adequate Data Protection Laws

The risks for data users of storing personal data in jurisdictions without data protection laws are evident. Firstly, such locations do not enforce any minimum legal standard on the cloud service providers or their staff. Accordingly, staff may be unaware of any data protection rules requiring them to respect the original purpose of the personal data entrusted to them and to protect the personal data territorially and electronically by the data sensitivity. Secondly, there is no incentive or reason, apart from possible contractual obligations, for the staff in such jurisdictions to follow any such data protection standards. The absence of any legal sanctions

[21] *European Commission. (2012) Article 29 Data Protection Working Party. This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC (as revised by 2009/136/EC) where relevant*. EC Europa. http://ec.europa.eu/justice/ [Accessed 9 January 2016].

if anything goes wrong discourages them from spending any additional time or energy on data protection compliance. South Africa requires cloud service providers to operate within their jurisdictional boundaries. However, this may not always be the case, given the diversity of the network operators, the reliance on external infrastructure and available broadband to provide the required service level commitments.

b. Risks of Storing Data in other jurisdictions

Outside the RSA borders and regardless of whether other jurisdictions have data protection laws in place, the personal data stored in those jurisdictions become automatically subject to the legislation of those jurisdictions. Therefore, cloud service providers need to familiarise themselves with the rules of other jurisdictions to understand the repercussions they may face from their data users or clients if any data breach were to happen. For instance, data stored in other jurisdictions may be subject to monitoring or access by law enforcement agencies without court warrants/orders. In such circumstances the transferral of client's personal data to other jurisdictions exposes such data to unforeseen disclosure and regulation by foreign authorities. Cloud service providers may have a duty to inform their customers that their stored personal data will be located in a foreign jurisdiction, as well as inform them of any implications attached to the stored data.

c. Efforts to Facilitate International Cross-border Data Flows

International or cross-border transfer issues of data are not new and are familiar problems. Numerous international struggles have been embarked on to facilitate easier cross-border data flows and the efforts have progressed with varying degrees of success, maturity and relevance. Chapter 1 section 2 (b) of the POPI Act[22] describes how the administration of personal data may be handled and also the establishment of conditions in harmony with adopted international principles, regarding the lowest threshold requirement for the lawful processing of personal data. The South African Law Commission's goal is to safeguard and ensure that legislation provides sufficient levels of data protection.

Regarding the EU Regulation, a condition has been included that prohibits the transfer of personal data to other countries that do not have sufficient data protection laws themselves by way of Chapter 10: Cross-border flows clause 94.[23] Similarly, these requirements are found

[22] *The Protection of Personal Information Act No. 4 of 2013 of South Africa, Policy, Law, Economics and Politics*. http://www.polity.org.za/ [Accessed 6 December 2015]. Chapter 1 section 2 (b).
[23] The South African Law Reform Commission. (2005) *Privacy and Data Protection Discussion Paper 109 Project.* Justice Department. http://www.justice.gov.za/ [Accessed 6 January 2016].

in the EU Regulation 2016/679 and were previously aligned with the EU Directive 95/46 (1995).[24]

Binding Corporate Rules (BCRs),[25] or Binding Contractual Agreements (BCAs) that provide 'an adequate level of protection' are other means of transference according to which cross-border data flows may be legitimate within corporations operating across multiple jurisdictions. The BCRs or BCAs allow the company to be approved by the RSA regulator by undertaking to comply with the POPI Act when processing personal data outside of the RSA. South Africa is also in agreement with the EU on such data transfers.[26] The potential clients of approved cloud service providers must, therefore, determine what services or contracts they are offered. The BCRs or BCAs should follow the principles required in the POPI Act and EU Regulation for processing personal data. There are also further means to assist with the cross-border data flow, such as the individual concerned has provided consent for the performance or closure of agreements with the person involved, including third party aspects where the contract is in the individuals' interest.

d. Compensation Controls

Compensation controls in South Africa are not usually looked at when checking the cloud service provider features. One compensating control that data users may consider when engaging the services of cloud service providers is to determine the exact locations in which the client's personal data will reside especially when the data centre sites are not within the RSA. Moreover, they should then ascertain as to whether those sites offered by the cloud service provider have data protection laws analogous to those in South Africa, or the jurisdictions of the client's choice and if necessary specify the locations in which the cloud service providers are allowed to store such personal data.[27] Similarly, it would be useful to ensure that the cloud service provider's staffs, who have access to that data, are equally aware of the relevant data protection laws of the jurisdiction[28] of the locations offered. Data users correspondingly need to consider whether a cloud service provider's claim to be compliant with international efforts to facilitate cross-border data flows is relevant to their decision to use

[24] South African Legal Information Institute. (2014) *POPI – Is South Africa keeping up with international trends?* SAFLLI. http://www.saflii.org/za/ [Accessed 11 March 2016].
[25] European Commission. (2016) *Overview on binding corporate rules.* EC Europa. http://ec.europa.eu/justice/ [Accessed 12 December 2016].
[26] *Ibid.*
[27] European Union (2012). *Article 29 Data Protection Working Party Opinion 05/2012 on Cloud Computing Adopted July 1 2012*. EC Europa. http://ec.europa.eu/justice/ [Accessed 6 January 2016].
[28] Office of the Privacy Commissioner for Personal Data, Hong Kong. (n.d.) *Information leaflet on cloud computing.* PCDP. https://www.pcpd.org.hk/ [Accessed 29 September 2015].

that particular cloud service provider. These seemingly obvious and straightforward compensating controls are not without their challenges or not all cloud service providers are willing to disclose the locations of their storage facilities, let alone allowing clients to specify a 'wish list' of places in which their data can be stored. However, potential customers should continue to make such demands to force cloud service providers to realise the importance of transparency over storage locations and eventually provide clients with location choices.

6.5.3. Third-party Contractor Agreements

Amongst the many attractive features of cloud computing are the scalability and flexibility of the cloud resources. Scalability means that the cloud resources can be either scaled up or scaled down as needed by the data users. Flexibility implies that such expansion and contraction of resources can be met very quickly and often at the touch of a button.[29] The implication is that cloud service providers have sufficiently large resources to cater for unpredictable demands. A pragmatic view is the higher likelihood that they will share the economic risk with other infrastructure service providers by establishing a series of outsourcing arrangements.[30] In such arrangements the cloud service providers build and own a core capacity themselves. At a point when the developed capacity is utilised to a defined level, the cloud service provider will enter into an outsourcing agreement to obtain extra capacity be it hardware and workforce, to temporarily meet demand. As demand from data users can go down as well as up, the additional resources are obtained temporarily until the cloud service provider is satisfied they will be necessary on a permanent basis.

The potential concern with such outsourcing arrangements is that the cloud service provider may or may not require all the spare capacity in practice. An effect of having the extra capacity on an *ad hoc* basis could mean that the cloud service provider will not make too much effort or exert themselves to build in or negotiate the necessary personal data controls in their contracts with third party outsourcers, an area which remains uncertain. The main risk of third party outsourcing lies in the potential loss of control. In the case of the cloud, the contractual relationships are between the cloud service providers and the third-party contractors. Nevertheless, the latter may also serve all the cloud service provider's clients. Therefore, the contract between the cloud service provider and the third-party contractor is unlikely to be tailored to meet the regulatory requirements of each and every data user. Further complicating the matter is that very few cloud service providers are transparent about their third-party

[29] National Institute of Standards and Technology. (2011) *The NIST definition of cloud computing SP 800 – 145.* CSRC. http://csrc.nist.gov/publications/ [Accessed 28 November 2015].
[30] Office of the Privacy Commissioner for Personal Data, Hong Kong. (n.d.) *Information leaflet on cloud computing.* PCDP. https://www.pcpd.org.hk/ [Accessed 29 September 2015].

contractor arrangements. Hence, potential clients are not in a position to gauge the severity of the risks involved. If cloud service providers engage in third-party contractor arrangements, data users need to take the following issues into consideration.

a. Lack of Formal Contractual Relationship

When the cloud service provider engages in third-party contracts the cloud service provider's operations are potentially supported by a range of outside parties. In addition data users are unable to specify the necessary controls to the third-party contractors. This means that third-party contractors enjoy no direct contractual relationship with the data users. In the event of any breach or misuse of personal data caused by the third-party contractors, data users will be unable to hold them contractually liable. The lack of a direct contractual relationship with data users substantially weakens the sense of responsibility and loyalty that third-party contractors feel. Accordingly, third-party contractors may not feel obliged to alert all users with whom they do not have a strong contractual relationship, about any data breaches they may suffer. In extreme cases, third-party contractors can walk away from catastrophic data breaches, leaving the data users to face the full legal consequences. In any event, data users need to remember that the resulting legal and reputational damage to themselves cannot be convincingly refunded by suing either the cloud service provider or its third-party contractors for breach of contract.

b. Lack of Privacy Awareness and Legal sanction

Another critical area which comes into play, as previously noted, if third-party contractors entrusted with the processing of personal data are found in jurisdictions without data protection laws, they could suffer from lack of knowledge and respect for personal data protection. Such a situation poses more risks to data users. As with contractual relationships, the third-party contractor may be able to walk away from a catastrophic data breach or incident of misuse without being subject to any law or legal sanction.

c. Cloud Services Engagement Decision (Judgement Call)

Based on the items discussed above, it is of great importance that data users determine the outsourcing policy and practice of any cloud service provider whose services they intend to engage. They must thereafter exercise judgement concerning whether adequate controls over outsourcing arrangements and third-party contractors are in place before entering into any formal agreement or contract with the cloud service provider.

6.5.4. Standard Offering

Most cloud service providers, particularly those offering public cloud services, offer only a limited number of predefined cloud service solutions or set packages to their clients. Data users looking to work with such providers should prudently view all the details of such offerings to ensure that all of their requirements under the usual standard of purpose specification, use limitation and security safeguards remain established.

a. Security and Compliance Gap

Data users who discover that the standard offerings of potential cloud service providers do not meet their safety or compliance requirements should not consider those cloud service providers. However, should the data users choose to ignore the gap in security or compliance necessities and accept to use the contemptible cloud solutions or set packages, they will be placing both the personal data in their care as well as their business reputation at risk. A more prudent way of dealing with contemptible cloud services offerings would be to discuss the relevant issues with the cloud service providers concerned. Providing them with an opportunity to tailor or otherwise improve the non-compliant offerings to meet the data users' standard requirements or to such a state where the data user is comfortable with the improved offering and is confident that they are in compliance with the usual standards of 'purpose specifications', use limitations and security safeguards.

b. Verification

Even if cloud service providers are willing to customise or otherwise improve their cloud services solutions or set package offerings to ensure they meet all the data users imposed requirements, the next challenge for data users is 'how to make sure that additional controls are definitely in place and executed properly'. In traditional outsourcing arrangements auditing rights are typically included in the contract. However, the situation is more challenging on cloud service providers whose operations and boundaries are rather fluid and as such make it virtually impossible to audit the compliance in the traditional manner. To overcome the complex challenges of audit reviews of the cloud service providers' compliance, it is imperative that new and innovative resources or other means of auditing be developed by which cloud service providers would be able to demonstrate their level of compliance with requirements or expectations of data users.

Certification involving independent assessments may be one way for cloud service providers to validate conformity with predetermined standards. However, data users who are unfamiliar with the workings of these standards and the certification process could be misled by the creative use of a certification reference in cloud service providers' marketing materials. To improve their protection, data users should thus familiarise themselves with the scope of the

security and auditing standards commonly used or claimed by the cloud service providers and assess their relevance and adequacy on a case-by-case basis.

6.6. Conclusion

Data users are all the time challenged. Data users are ultimately held responsible for the appropriate handling of all personal data in their possession. Such responsibility is not a transferable legal obligation and thus the outsourcing of personal data processing to a cloud service provider does not shift the liability to that cloud service provider. The primary challenge for data users utilising cloud platforms is, therefore, to figure out a way to maintain control and oversight comparable to managing the personal data themselves.

When the users have understood the main data protection principles as discussed above, particularly the principles of determinative specifications, use limitation and security safeguards, data users looking to engage the services of cloud service providers should carry out proper risk assessments of all potential offerings. In doing so they must identify any gaps that may exist between those offerings and the cloud service provider's own requirements. Any gaps identified, must be addressed by implementing appropriate controls to avoid or at least limit the risk avoidance and reduction measures. These are mostly designed to prevent risks from materialising. Data users may also consider more sophisticated measures of encryption which should enable users to maintain a high level of data confidentiality as they will be the only party capable of deciphering the data. Concerns over access and misuse by unauthorised parties will thus be significantly reduced.

7. International Law and the Cloud

This section discusses public and private international law in relation to cloud technologies, providing an overview of some of the legal issues related to the cloud. The information provided merely introduces international law and the interactions with the cloud, highlighting the extent of the complexities of international law. Both public and private international law topics can in themselves form the basis for further dedicated studies so as to analyse the full comprehension of jurisdiction, choice of laws as well as the rules for common law, statutory or codified laws, all of which will influence the international regulation surrounding the operational characteristics and overall cloud environment. However, such comprehensive studies fall beyond the scope of this thesis.

7.1. Introduction

The principle of territoriality has dominated the development of IP governance for years, dating back to the initial setting of standards.[1] International IP protection was initially of little importance as cross-border data flow activity was limited. The consequence of the lower importance was that works, which qualified for IP protection, were almost always limited to their country of origin. In the nineteenth century, the international markets saw a tremendous growth in cultural, social and economic development in Europe and an increased demand for various works, of which printed was the most prevalent.[2] With the heightened demand for printed works across Europe and other countries, it became evident that the requirement for international copyright protection of works was as compelling as that at a national level. This situation led the British authorities to decree that copyright protection was extended to all works, regardless of origin and replacing the *International Copyright Act 1838* with the new amended *International Copyright Act, 1844, 7 & 8 Victoria, c.12.* The new Act provided that 'the British monarch could, by Order in Council, grant to foreign authors copyright protection for works as well as performance rights.'

[1] DRAHOS, P. (2002) *Developing countries and international Intellectual Property standard setting. The Journal of World Intellectual Property, 5 (5*), pp. 765–789, Wiley. http://onlinelibrary.wiley.com/ [Accessed 2 April 2016].
[2] KLOPPER, H.B. et al. (2011) *Law of Intellectual Property in South Africa*. Cape Town: LexisNexis. p. 150.

Furthermore, the new Act also provided for a reciprocal copyright arrangement with a foreign state.[3] Subsequently, what has trailed over the years has been the development of IP protection and the creation of a succession of conventions and treaties with which the international community works today.

The importance of the international IP protection development is crucial, specifically with respect to cross-border data flows and jurisdictional issues as well as mutual legal protection by way of the relevant applicable laws between territories. The cross-border data flow activity issues are further challenged since the introduction of the internet and more recently the development of various cloud service models. The legal risks and challenges associated with the cross-border data flow are still some of the major hurdles which the legal community faces. Complex problems with regard to data portability, location, security and privacy are at the top of the list. Both public and private international law are drawn closer together to assist in resolving these issues, be it through the development of new law or expanding the current legislation to bridge the gaps between new technology development and legislation.

Before engaging a cloud service provider or entering into any agreement with a cloud service provider, a customer should, as a minimum consider the risks that would be involved as well as the challenges with cloud services at an international level. Having a more informed understanding will assist in the decision-making process and enable the customer to choose a cloud service provider that offers less risk and fewer challenges. Furthermore, the client may negotiate improved safeguards for their IP, confidentiality and privacy concerns.

7.2. Cloud Jurisdiction - Cloud Border-crossing

The cloud environment raises various jurisdictional concerns based on the 'virtual-world' nature of operations in a similar way to that of the internet. The internet enables the cloud systems to be international and it is this global platform which creates the particular need to review the jurisdictional concerns and cross-border issues. These problems already exist in the mainstream of the internet. However, they are intensified in the cloud. It has been shown that the cloud operates beyond the boundaries of the 'so-called' local domain, with operations going beyond the jurisdictional authorities of local areas into other regions and even beyond those authorities themselves. Some authors consider the cloud as a natural evolution of the

[3] DEAZLEY, R. (n.d.) *School of law commentaries, (Primary sources on Copyright 1450-1900)*. University of Birmingham. http://www.copyrighthistory.org/ [Accessed 4 April 2016].

internet.[4] The notion of jurisdictional authority underlines the ability of these various powers that be, to assert jurisdiction effortlessly over the cloud.

7.3. Jurisdiction

The courts and territory deal with the command of the state under international public and private law to regulate or otherwise impact upon people, property and circumstances.[5] Authority in public international law should not be confused with the competence of a court to try a case or the power of law to regulate a situation in private international law,[6] but to some extent, such competencies are interrelated.

Formally, on the one hand perspective jurisdiction is the power to for example enact rules of general Acts, governmental decrees and/or individual court decisions, decisions of administrative bodies on the application thereof. On the other hand enforcement jurisdiction is the power to take concrete actions, such as measures of constraint, to ensure the efficient use of the rules by their subjects. These authorities are treated differently in public international law.

Public international law forms the basis of an administration's jurisdiction – conferring upon it grounds for international jurisdiction,[7] mainly regarding territory and nationality. The purpose, therefore, is to set the limits of a government's competence. Since the cloud crosses many boundaries, many establishments may claim jurisdiction over the same international situation, relying on one or another legal rule, which affects the people abroad. It is essential to determine how jurisdictional authority remains territorially controlled through public international law.

Any research on the appropriate regulation of international law will not be complete without at least considering the 'SS Lotus' case (France v. Turkey) 1927 PCIJ Rep Series A No. 10

[4] CRAIG, R. et al. (2009) *Cloud computing in the Public Sector: Public manager's guide to evaluating and adopting cloud computing*. CISCO. http://www.cisco.com/ [Accessed 17 March 2016].
[5] GEOFFREY, C.C.I. (2012) *Rethinking Jurisdiction under International Law*. Works Bepress. https://works.bepress.com/ [Accessed 15 March 2016].
[6] DUGARD, J. (2013) *International Law, A South African Perspective. 4th ed*. Cape Town: Juta & Co. pp. 146–147.
[7] DUGARD, J. (2013) *International Law, A South African Perspective. 4th ed*. Cape Town: Juta & Co.

(referred to as Lotus),[8] where the Court established three principles regarding the basis of jurisdiction in international law.

> A state may not exercise its authority in the territory of another state: unless there is a rule sanctioning it to do so. A state may use its authority in its area over acts occurring elsewhere – unless there is an international law preventing this (extraterritorial jurisdiction). In international law, the territoriality of criminal cases is not absolute.[9]

Even with the rules established by the Court in the Lotus case, it remains debatable as to whether or not an authority may enforce within the limits of its territory any rule with an extraterritorial reach. The Lotus philosophy concerning the law authorises a limitless exercise of prescriptive jurisdiction. However, this may not be the correct deduction. States are considered to be sanctioned to exercise jurisdiction if they can advance a legitimate interest based on personal or territorial connections of the matter to be regulated.[10] As a consequence, authorities have broad discretion freely to define the geographical reach of their jurisdictions alone at national or local law or jointly with other jurisdictions and international conventions, treaties and regulations. This behaviour of states and authorities becomes crucial.

Moreover, the cloud is territorially anchored, which makes it relatively easy to link to authorities' territories, but contributes to the risk potential of concurrent jurisdictional assertion. On the one hand, the cloud concerns service providers and users having a nationality, domicile and residence somewhere. On the other hand, 'the cloud itself is a complex network of database centres,[11] that are situated in built infrastructure linked to the internet using backbone infrastructure which are both territorially embedded.

Authorities may legally and legitimately claim jurisdiction to ensure compliance with their public policy over the internet and the cloud. The ECJ put it in the following manner: at Paragraphs 86 and 87 of the Joint cases C-316/07, C-358/07 to C-360/07, C-409/07 and C-410/07:[12]

> Par. 86. First, while it is factual that illegal transactions on the Internet may, particularly when they are of a transnational character, prove harder to control and sanction than other types of criminal behaviour, such circumstances are not restricted to the gambling and betting sector. A

[8] The Permanent Court of International Justice. (1927) *Collection of judgments "The Case of the SS Lotus": Series A. No. 10 September 7th 1927*. ICJ. http://www.icj-cij.org/ [Accessed 16 March 2016].
[9] *Ibid.*
[10] DUGARD, J. (2013) *International Law, A South African Perspective. 4th ed.* Cape Town: Juta & Co.
[11] SCOTT, R.J. (2012) *Understanding the legal risks of cloud computing navigating the network security and data privacy issues associated with cloud services*. Thomas Reuters Aspatore. https://www.scottandscottllp.com/ [Accessed 15 May 2015].
[12] Judgement of the Court (Grand Chamber) (2010) *In Joined Cases C-316/07, C-358/07 to C-360/07, C-409/07 and C-410/07,* Curia Europa. http://curia.europa.eu/juris/ [Accessed 20 March 2016].

> participating Member State cannot be, deprived of the right to involve the internet, the application of the autonomous restraining rules which it accepts for appropriate purposes in the public interest simply because that technological middle has a character that is, in essence, transnational.
>
> Par. 87. Secondly, it is undisputed that the participating Member States are not dispossessed of legal means enabling them to ensure, as efficiently as possible, compliance with the rules which they lay down about performers operating on the Internet and falling, for one reason or another, within their jurisdiction.

The technology available helps authorities to enable website blocking to enforce the national or local law online and to create online borders for each state. The ECJ has recognised the importance of having such enforcement measures.[13]

> Para 43. A standard, which, implements the national legislation at issue in the central proceedings, such as the sanction, which the judge who heard the application for interim relief, imposed on the Ladbrokes companies. To bar access, to their internet site, for individuals living in the Netherlands and to make it impossible for such people to take part in telephone betting, which is a critical component of the security in respect of games of chance, that is planned to be delivered by the Netherlands within its region and cannot, consequently be, considered as an additional constraint over and above that which arises directly from the provisions of the Work.
>
> Para 44. That applying measures merely safeguards the effectiveness of Netherlands legislation concerning games of chance. Without such a rule, the prohibition laid down by the Work would be unsuccessful since commercial service providers who are not licensed by the national authorities, would be able to provide games of chance on the Netherlands market.

7.4. Private International Law

Public international law, which revolves more around the state and primarily criminal law, has shown that international principles and national rules are the primary concerns. However, the focus of Code for Private International Law (referred to as CPIL) routinely deals with civil and commercial law matters, in particular with the laws which involve the cloud and IP, privacy, contract and delict (or tort). CPIL provides the business community and individuals with legal protection. Two fundamental questions arise from private international law situations once jurisdictional authority has been fixed, namely which judge is competent and which law

[13] Judgement of the Court (Second Chamber) (2010) *Case C-258/08, Ladbrokes Betting & Gaming Ltd, Ladbrokes International Ltd v, Stichting de Nationale Sporttotalisator*. Curia Europa. http://curia.europa.eu/juris/ [Accessed 16 March 2016].

applies? In cases involving South Africans, an assumption is made that the data user is always domiciled in the RSA.

7.5. Court of Jurisdiction

In the EU, the law for the court of jurisdiction historically stayed controlled by the '*Brussels Regime'.* This was a standard set of rules regulating which courts would have jurisdictional authority in legal disputes of a civil or commercial involvement between individuals residing in the different EU member states and the European Free Trade Association (referred to as EFTA). The Council Regulation (EC) No. 44/2001 of 22 December 2000, on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (referred to as Regulation (EC) 44/2001),[14] and the newer Regulation (EU) No. 1215/2012 of the European Parliament and the Council of 12 December 2012, on jurisdiction and the recognition and enforcement of judgements in civil and commercial matters (recast) (referred to as Regulation (EU) 1215/2012),[15] have complete rules for the assignment of jurisdiction over where disputes will be heard. It also governs the recognition and enforcement of foreign conflicts or judgements. Both the update regulations have substantially replaced the much older Brussels Convention of 1968.

The Regulation (EC) 44/2001 or sometimes referred to as the 'Brussels 1 Regulation', was updated in the form of Regulation (EU) 1215/2012 in 2012 and came into force in 2015. The court of jurisdictional authority is now regulated by Regulation (EU) 1215/2012. The new updated rules define which courts are competent to decide cases in civil and commercial matters in the EU, for example cases which deal with privacy, IP, contract and delictual law (or tort) as a standard. If Regulation (EC) 44/2001 does not apply, for instance; if the defendant stands domiciled outside of the EU, then the national law of the respondent's country of residence applies for identifying the court of jurisdiction.

7.6. Forum Selection

The complicated question of the validity of a choice of court agreement can only be briefly addressed. The new changes made to the old Regulation (EC) 44/2001 Article 23 versus the

[14] *Council Regulation (EC) No. 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters*. Eur-Lex. http://eur-lex.europa.eu/ [Accessed 10 March 2016].
[15] *Regulation (EU) No. 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast)*. Eur-Lex. http://eur-lex.europa.eu/ [Accessed 18 January 2016].

Regulation (EU) 1215/2012 Article 25, offers the possibility of choosing a court of a member state.

> Article 25
> If the parties, regardless of their domicile, have agreed that a court or the courts of a Member State are to have jurisdiction to settle any disputes, which have arisen or which may arise in connection with a particular legal relationship, that court or those courts shall have jurisdiction unless the agreement is null and void as to its substantive validity under the law of that Member State. Such jurisdiction shall be exclusive unless the parties have agreed otherwise.[16]

Possibly, the most significant change here is that the domicile requirement for parties to a jurisdictional agreement has fallen away. So a jurisdictional clause will fall within the scope of Regulation (EU) 1215/2012 Article 25 even if none of the parties remain domiciled in a member state (provided the courts of a member state have been chosen in the clause).[17]

Article 25 also sets the formal conditions of making such a choice. However, in consumer contracts the user is notably protected if the cloud service provider, being domiciled or established in another member state, 'directs' its activities to the member state in which the consumer is domiciled;[18] the individual may submit their claim to the courts of the member state in which they are domiciled.[19] As agreed, a choice of forum depriving the consumer of their individual right may only be concluded 'after the dispute has arisen'.[20] The effect of a forum selection within general terms and conditions is, therefore, limited. Regulation (EU) 1215/2012 will protect the consumer even if the other party has no establishment within the EU.[21]

If the courts of a *third state,* for instance when a USA court is selected, in principle, Regulation (EC) 44/2001 will not apply. The involved court of the member state, such as Germany, would implement the *Lex fori* (the law of the country in which an action is brought), including CPIL, in particular conflict of law rules.[22] However, the position of *Lex fori* and use of conflict of law

---

[16] Idem. Article 25.
[17] CORDELL, N. (2013) *Intellectual Property in the cloud*. Allen and Overy. http://www.allenovery.com/ [Accessed 4 January 2016].
[18] *Regulation (EU) No. 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast)*. Eur-Lex. http://eur-lex.europa.eu/ [Accessed 18 January 2016].
[19] *Ibid.*
[20] Idem. Article 23.
[21] Idem. Articles 17-19.
[22] *Coreck Maritime GmbH v. Handelsveem BV and Others. Reference for a preliminary ruling: Hoge Raad der Nederlanden - Netherlands. Brussels Convention - Article 17 - Clause conferring jurisdiction*

rules still is debated, and Regulation (EU) 1215/2012 does not lead to the end of the discussion.[23] Under CPIL rules, a court selection is only operative against a consumer if the forum has been agreed to after the dispute has arisen.[24] If another member state's law applies, then German courts will not be involved, which does contain such prohibition, the forum selection in a consumer contract could nevertheless be unfair according to Directive 93/13.[25] According to the CPIL, a professional user will be bound by the jurisdiction clause unless it is foreseeable that the overseas decision will not be recognised or enforced in Germany.[26]

7.7. Default Rules and Applicable Law Determination

There are two possibilities when the proper law of a contract must be determined, namely:

a) Express or tacit selection of law by the parties on the strength of the principle of freedom of contract. When the proper legislation of an international contract has to be determined, one has to enquire whether the parties made an express choice of an applicable legal system. In the absence of such express choice of law, the next step is to determine whether the parties have made a tacit choice.

b) No choice of law by the parties. If it is evident that the parties refrained from making an express or an implied choice of law, the court itself will have to ascertain the proper legislation of the contract. The principle of party autonomy does not apply.

In the first instance, the default rule is always central in knowing the jurisdiction over any agreement or contract and the second, as to which law will be applicable if the parties did not

---

- *Formal conditions - Effects. Case C-387/98*. Curia Europa. http://curia.europa.eu/juris/ [Accessed 8 April 2016]. par. 19.

[23] *Regulation (EU) No. 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast)*. Eur-Lex. http://eur-lex.europa.eu/ [Accessed 18 January 2016]. Article 25.

[24] *Federal Public Service Justice [C - 2004/09511] F. 2004 - 2935 16 JULY 2004. - Law Bearing the Code of Private International Law (1)*. Reflex Chrono. http://reflex.raadvst-consetat.be/ [Accessed 23 March 2016]. Article. 97. Para 3. An agreement conferring international jurisdiction produces its effects with regard to the worker or consumer if it has arisen after the dispute. See also FIORINI, A. (2008) *The codification of private international law in Europe*. Electronic Journal of Comparative Law, 12 (1). https://www.ejcl.org/ [Accessed 23 March 2016].

[25] *European Commission. Decision of 28 January 1992 establishing transitional measures for trade in bovine animals in relation to the cessation of vaccination against foot-and-mouth disease and revoking Decisions 91/13/EEC and 91 /177/EEC*. Eur-Lex. http://eur-lex.europa.eu/ [Accessed 23 March 2016]. With respect to 'Unfair terms in consumer contracts'.

[26] *Federal Public Service Justice [C - 2004/09511] F. 2004 - 2935 16 JULY 2004. - Law Bearing the Code of Private International Law (1).* Reflex Chrono. http://reflex.raadvst-consetat.be/ [Accessed 23 March 2016]. Article 7.

agree on authority, apart from the maxim or general rule *actor-sequitur-forum-rei* which provides that the jurisdiction of a Court of a defendant's domicile shall normally have jurisdiction.[27] If the respondent is not domiciled in the area of jurisdiction of the matter, then the national law of the jurisdiction involved will determine a competent judge.

In non-consumer contracts, if the defendant is domiciled in the RSA, the Courts of the area of execution of the responsibility in question are competent. That is unless otherwise agreed and the Courts, where the cloud services were provided or should have been provided under the contract, are competent. Otherwise, national law again determines the competent Court.

Where is a cloud service performed or provided? Can this question be answered for all cloud services such as SaaS, PaaS and IaaS at once? Technically, cloud services are carried out in data centres. Taking into consideration the locations of the IaaS or sites of the hardware where PaaS or SaaS are conducted would be simple, but these sites can be irrelevant. In such a case, should the place where a service is accessed by the user be relevant? The universal access to cloud services removes the viability of such a condition. Pleading the contrary would certainly lead to unwanted jurisdictional selectivity. If clouds rather argued that the service is provided where the user typically uses the service, where the cloud service provider supervises and manages the service, or even partially at each place, then it shows the importance of including an appropriate provision in the contract, keeping in mind that such a clause may not circumvent the legal regime of the jurisdiction selection clauses.

7.8. Conflict of the Rules of Law

Two kinds of rules or methods exist to determine the applicable law, both of which are used in the RSA as well as the EU. These are bilateral or multilateral rules and the unilateral rules.[28]

The Regulation (EC) No. 864/2007 and the Regulation (EC) No. 593/2008 defining the law applicable to non-contractual and contractual obligations, respectively reflect the multilateral method; they describe which law applies in which situation in the EU. Member states, however, nevertheless retain some margin to apply their own 'provisions that cannot be derogated[29] from by agreement' or their own 'overriding mandatory provisions' and to safeguard the public

[27] *Mayne v. Main (182/99) [2001] ZASCA 35; [2001] 3 All SA 157 (A)*. Southern African Legal Information Institute. http://www.saflii.org/za/ [Accessed 23 April 2016].
[28] DUGARD, J. (2013) *International Law, A South African Perspective. 4th ed*. Cape Town: Juta & Co.
[29] *Regulation (EC) No. 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations (Rome II)*. Eur-Lex. http://eur-lex.europa.eu/ [Accessed 4 April 2016].

policy of the forum.[30] Such requirements, for instance, data protection,[31] consumer protection, online gambling regulations, relating to public policy aspects, in principle, depend on a single rule of applicability.

In contractual matters, Regulation (EC) No. 593/2008 enshrines the principle of the freedom to choose the applicable law.[32] Another law will supplant the law selected in the contract for instance, if mandatory provisions, as just evoked, apply. For example, if a cloud service provider guides his service to the state of habitual residence of a consumer, a choice of law, cannot deprive the consumer of the safeguard provided to him by the conditions that cannot be derogated from by agreement according to the legislation of this country. For instance, the prohibition of unfair terms in consumer contracts,[33] unless it is considered that the service is to be supplied solely in a country other than in which the consumer has his habitual residence.[34]

Outside the material scope of Regulation (EC) No. 593/2008 for instance, regarding agreement on the choice of a Court,[35] member states' CPIL will apply. The CPIL, however, makes Regulation (EC) No. 593/2008 rules applicable in matters excluded from Regulation (EC) No. 593/2008, unless it says otherwise.[36]

In non-contractual matters, the general rule of Regulation (EC) No. 864/2007 provides that the law pertinent to a non-contractual obligation arising out of a delict (tort) shall be the law of the

---

[30] Idem. *Article 16 and 26. See also Regulation (EC) No. 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I)*. Eur-Lex. http://eur-lex.europa.eu/ [Accessed 2 April 2016]. Article 6.2, 9 and 21.

[31] *The European Parliament and the Council of April 2016, 2016 Regulation 16/679, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation*). EC Europa. http://ec.europa.eu/justice/ [Accessed 25 May 2016]. See also *European Parliament. (1995) EU Data protection 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*. Eur-lex. http://eur-lex.europa.eu/ [Accessed 6 February 2016].

[32] *Regulation (EC) No. 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I*). Eur-Lex. http://eur-lex.europa.eu/ [Accessed 2 April 2016]. Article 3.1.

[33] Idem. Article 6.2.

[34] Idem. Article 6.4(a).

[35] Idem. Article 1.2 (e).

[36] *Federal Public Service Justice [C - 2004/09511] F. 2004 - 2935 16 JULY 2004. - Law Bearing the Code of Private International Law (1)*. Reflex Chrono. http://reflex.raadvst-consetat.be/ [Accessed 23 March 2016]. See also IPR. (2004) *The Code of Private International Law (CPIL)*. University of Gent. Institute for International Private Law. http://www.ipr.be/ [Accessed 2 May 2016]. Article 98, par. 1, alinea 2.

country in which the damage occurs.[37] Cloud service providers and users are less free; they may agree on an applicable law 'before' the event giving rise to damage only if they pursue a commercial activity.[38] Otherwise, for instance, if the user is a consumer, parties may choose the applicable law 'after' this event has occurred. [39] Furthermore, in both cases, depending on the location of the elements of the situation, the choice of law shall not prejudice the application of certain legal provisions.[40]

Copyright and privacy are especially at stake in the cloud. Regarding the former, Regulation (EC) No. 864/2007 contains a special mandatory rule: the 'Law appropriate to a non-contractual obligation ascending from an infringement of an IPR shall be the law of the country for which protection is claimed'.[41] This rule is a consequence of the territorial scope of IP. The location of the establishment of the cloud service providers and users, therefore, do not matter.

Concerning privacy and rights relating to personality, Regulation (EC) No. 864/2007 does not apply,[42] but the member states' CPIL would apply. The CPIL specifies that the law applicable to a breach of privacy or of a personality right is the law of the country in which the causal event or the damage occurred or may occur, at the choice of the victim. The exception is if the infringer can show that they could not foresee that the damage would arise in the country at stake.[43] For instance, a cloud service provider established in the USA who makes information relating to a Belgian user public, could face a claim based on the horizontal effect of article 8 of the European Convention on Human Rights (ECHR)[44] combined with the civil liberty rules. However, if the users falsely represented themselves as USA residents, notably by using a proxy server, when they joined the service, the cloud service provider may argue that they were not able to foresee the occurrence of damage in the country of the user's residence (in

[37] *Regulation (EC) No. 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations (Rome II)*. Eur-Lex. http://eur-lex.europa.eu/ [Accessed 4 April 2016]. Article 4.1.
[38] Idem. Article 14.1(b).
[39] Idem. Article 14.1(a).
[40] Idem. Article 14.2-3.
[41] Idem. Article 8.1.
[42] Idem. Article 1.2(g).
[43] IPR. (2004) *The Code of Private International Law (CPIL)*. University of Gent, Institute for International Private Law. http://www.ipr.be/ [Accessed 2 May 2016]. Article 99, para 2; Article 100.
[44] *European Court of Human Rights. (2010) European Convention on Human Rights as amended by Protocols Nos 11 and 14 supplemented by Protocols Nos 1, 4, 6, 7, 12 and 13*. ECHR. http://www.echr.coe.int/ [Accessed 2 May 2016].

this case Belgium). Neither will the law of the place in which the injury occurs apply if the parties chose another applicable law 'after' the dispute has arisen.[45]

Regarding data protection, a single mandatory rule[46] applies in the EU and member states' laws, more specifically in the European Economic Area (EEA) countries. Briefly, a cloud service provider who processes personal data and therefore, a data controller, has to apply the national implementation of regulation 2016/679 (Directive 95/46 1995 repealed) entirely. The Belgian Privacy Act should for instance be applied in two situations.[47] Firstly, if data processing is part of the activities of a Belgian established provider, and secondly, if the latter is set up outside the EU. In case a cloud service provider uses equipment, for instance, a data centre, cars with cameras, such as Google street view cars, uses mobile phones, a data processor and so forth, located in Belgium for the purpose of that processing. This latter criterion was abandoned in the draft EU data protection regulation in support of a targeting approach.[48]

7.9. Substantive International Obligations

Just like the conflict of laws rules, international commitments of a material or practical nature could 'require' an exercise of jurisdiction or limit it or possibly even forbid it. Such commitments positively influence the conflict of law determination.

For illustration, it can be argued, that the parties to the European Court of Human Rights have an affirmative obligation to apply the Convention to international situations involving private persons such as cloud service providers and users, leading to the horizontal effect.[49]

---

[45] IPR. (2004) *The Code of Private International Law (CPIL)*. University of Gent, Institute for International Private Law. http://www.ipr.be/ [Accessed 2 May 2016]. Article 101.

[46] *European Parliament. (1995) EU Data protection 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*. Eur-lex. http://eur-lex.europa.eu/ [Accessed 6 February 2016]. Article 4.

[47] Data Protection Working Party (2010) *WP 179 Opinion 8/2010 on applicable law*. EC Europa. http://ec.europa.eu/justice/ [Accessed 17 February 2016] Article 29.

[48] *European Commission (2012) Proposal for a Regulation of the European Parliament and of the Council 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)*. Eur-Lex. http://eur-lex.europa.eu/ [Accessed 6 February 2016].

[49] DUDLEY, A. et al. (2012) *Investigating cyber law and cyber ethics: Issues, impacts and practices*. Hershey PA: Information Science Reference. p. 73.

In a certain way, privacy applies to individuals in the information society through the prism of data protection.[50] European data protection provisions, 'convention 108 of the Council of Europe[51] and the European Union Regulation 2016/679 (Directive 95/46 1995 repealed)', can be seen as fulfilling such an affirmative obligation through the cross-border data flows regime or through the full application of the EU data protection directive to data controllers established outside the member states. The cross-border data flows administration aims at enabling the international movement of information without jeopardising the European data protection rules. To this end the EC and the Council of Europe accept that personal data leaving Europe is subject to effective, but not equivalent data protection rules. The jurisdictional assertion exists, but is smoothed.[52] Such a reserve in international situations also appears in the case law of the European Court of Human Rights, 'only' when flagrant breaches of the European Court of Human Rights are condemned to permit international cooperation.[53]

To summarise, the European Court of Human Rights is neither absolute nor universal.[54] Nevertheless, internationality certainly does not provide a general and automatic excuse to ignore it.[55] Furthermore, the positive obligations to apply the European Court of Human Rights to international private situations remains bordered.

7.10. Conclusion

Authorities may be required to refrain from using national law. The creation of the EU internal market and the integration of marketplaces pursued by the World Trade Organization (WTO) are excellent illustrations. For instance, the internal market clause of the e-commerce directive limits the applicability of national law between EU member states. In the legal domain coordinated by the Directive, the law applicable to the provision of an information society

[50] European Court of Human Rights. (2010) *European Convention on Human Rights as amended by Protocols Nos 11 and 14 supplemented by Protocols Nos 1, 4, 6, 7, 12 and 13*. ECHR. http://www.echr.coe.int/ [Accessed 2 May 2016]. Article 8.
[51] European Treaty Series. (1981) *No 108 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*. RM Council of Europe. https://rm.coe.int/ [Accessed 8 February 2016].
[52] Idem. Article 12.1.
[53] European Court of Human Rights. (2010) *European Convention on Human Rights as amended by Protocols Nos 11 and 14 supplemented by Protocols Nos 1, 4, 6, 7, 12 and 13*. ECHR. http://www.echr.coe.int/ [Accessed 2 May 2016].Case law ECHR, 130-74.
[54] *Bankovic and Others v. Belgium and Others (Application No. 52207/99). Grand Chamber 1. Decision of 12 December 2001*. ECHR. http://echr.coe.int/ [Accessed 4 May 2016].
[55] *Matthews v. the United Kingdom. (Application No. 24833/94 39, Grand Chamber. ECHR 1999-1*. ECHR. http://echr.coe.int/ [Accessed 4 May 2016].

service may not be ‘stricter’ than the legislation of the member state in which the provider is established.

Finally, the GDPR 2016/679 (Directive 95/46 repealed) also contains an internal market clause; member states may not restrict or prohibit the free flow of personal data between themselves for data protection reasons.

8. Cloud Cross-border Data Flow

8.1. Introduction

An important part of understanding cross-border data flows comes from outside the RSA where regulation is more firmly imposed. It also starts with some historical introduction which took place over two decades ago. Having had an introduction to the implications of cross-border data flows at international level, it is of particular interest to explore the cross-border data flows between the EU and the USA, as this poses significant challenges for cloud service providers and businesses alike. Problems of this nature can assist other governing bodies in drafting rules on cross-border data flows. The critical but unresolved issues include agreeing on standards for the required data protection, which must be observed with respect to the identifiability of personal data, as well as the contractual rights granted to the cloud service provider and its customers under the various 'Terms of Service'.[1] Moreover, the required level of control and the associated grade of responsibility under EU data protection laws also require closer scrutiny in the context of cloud services.

With the enormous strides in technology development over the past two decades and in particular relation to the cloud environment, laws relating to data protection have had to constantly be adapted for their regulatory purpose to be efficient and achievable. The challenge with the legal process is that any Act or amendment of law requires a significant period to be promulgated. A good example is the Data Protection Directive 95/46/EC,[2] which was enacted in 1995 to investigate the concerns raised around the transfer of personal data to countries outside the EU. During the period of adoption of the new Directive, cloud-based services had not truly existed, and the main application of the Directive was focused on simple point-to-point transfers from European senders to an external receiver.[3] In the early 2000s the

[1] ROLF, H. et al. (2014) *Cloud computing: A cluster of complex liability issues*. European Journal of Current Legal Issues. http://webjcli.org/ [Accessed 14 May 2016].

[2] *EU Data protection Directive 95/46/EC of the European Parliament and 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).* Eur-Lex. http://eur-lex.europa.eu/ [Accessed 6 February 2016]. Article 2, Definitions.

[3] *Proposal for a Regulation of the European Parliament and the Council 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)*. Eur-Lex. http://eur-lex.europa.eu/ [Accessed 6 February 2016].

situation had changed dramatically. Now, not only has the potential of cloud been recognised, the challenges that it poses have urged legislators to respond to the rapid developments.

The European Parliament acknowledged the issues created by the cloud and initiated a regulatory transformation process which resulted in the first draft of the new Proposed European Data Protection Regulation[4] in 2012. The proposed regulations identified issues that related to the transfer of personal data to locations outside the EU. However, some matters that were identified remain unresolved. The research discussion focuses on the data protection problems and implications that stem from personal data which is transferred from the EU to the USA. Moreover, it should be noted that the following discussion is driven by the Proposed Data Protection Regulation, revised in 2013 (referred to as PDPR), and not the newly adopted regulation, Regulation (EU) 2016/679, of the European Parliament and of the Council of 27 April 2016 (referred to as GDPR), on the protection of natural persons about the handling of personal data and the free movement of such data.[5] Segments of the discussion will also reference the previous Data Protection Directive 95/46/EC, as this was still in force during that period.

8.2. Framework for Data Protection in the EU

8.2.1. Definition of Personal Data

Central to the EU data protection framework is the definition of personal data, which was formulated in 1995. The core of the definition includes any data from which a person is identifiable.[6] Regardless of the fact that the definition is seemingly simple, technology development continues to create challenges for this interpretation today. For instance, anonymous data does not lead to the identification of an individual. However, by merging a set of anonymous data with another set of anonymous data, a person could potentially be identified through computation processes such as is commonly used in 'Big Data'[7] technologies. Therefore a person may become identifiable when three independent variables

[4] *Ibid.*
[5] *GDPR. Regulation (EU) 2016/679*. EC Europa. http://ec.europa.eu/justice/ [Accessed 25 May 2016].
[6] Idem. Definitions, Article 4(2).
[7] SAS. (n.d.) *Big Data, What it is and why it matters. Big data is a term that describes the large volume of data – both structured and unstructured – that inundates a business on a day-to-day basis. But it's not the amount of data that's important. It's what organizations do with the data that matters. Big data can be analysed for insights that lead to better decisions and strategic business moves*. SAS. https://www.sas.com/ [Accessed 29 May 2016].

are known.[8] For instance, hair colour, age and favourite restaurant.[9] (The re-identification of personal data will be discussed in more detail in the next section.)

Additionally, personal data can be altered to prevent or hinder identification. The three most common approaches employed in this regard are encryption, pseudonymised or anonymised data.[10]

8.2.2. Anonymisation, What is it?

The definition for anonymisation is provided as follows by the EU Data protection commission.

> 'Anonymisation' of data means processing it with the aim of irreversibly preventing the identification of the individual to whom it relates. Data can be considered anonymised when it does not allow identification of the individuals to whom it relates, and it is not possible that any person could stand identified from the data by any further processing of that data or by processing it together with other information which is available or likely to be available.[11]

At present considerable research is being performed around anonymisation, together with knowledge on the effectiveness of the various techniques of creating anonymisation, alongside the constant changes in this domain. With current information at hand, it would be near impossible to state that a particular mode of anonymisation would be completely effective in protecting a data subject's information. However, the regulation attempts to provide guidance on identification while minimising the risks attached to the data subject when performing anonymisation of the data. In cases of anonymisation through 'identification' the regulation means the possibility of recovering an individual's name and address, in conjunction with the possible identifiability of a single person or linking and inference.[12]

---

[8] HRYNASZKIEWICZ, I. et al. (2010) *Preparing raw clinical data for publication: guidance for journal editors, authors, and peer reviewers. Comment in BMJ policy on data sharing*. US National Library of Medicine National Institutes of Health. https://www.ncbi.nlm.nih.gov/pubmed/ [Accessed 29 May 2016].

[9] HON, W.K., MILLARD, C. and WALDEN, I. (2011) *The problem of 'personal data' in cloud computing - what information is regulated? The cloud of unknowing, Part 1*. SSRN. http://papers.ssrn.com/ [Accessed 9 March 2016]. pp. 211–215.

[10] Data Protection Commissioner. (n.d.) *Anonymisation and Pseudonymisation*. Data Protection. https://www.dataprotection.ie/ [Accessed 10 May 2016].

[11] *Ibid.*

[12] *Ibid.*

8.2.3. Pseudonymisation, What is it?

The definition for pseudonymisation is provided as follows by the EU Data protection commission.

> 'Pseudonymisation' of data means replacing any identifying characteristics of the data with a pseudonym, or, in other words, a value which does not allow the individual concerned to stand directly identified. Although pseudonymisation has many uses, it should be distinguished from anonymisation, as it only provides limited protection for the identity of data subjects in many cases as it still allows identification using indirect means. Where a pseudonym stands used, it is often possible to identify the person concerned by analysing the underlying or related data.[13]

Anonymised and Pseudonymised Data

When data is encrypted, it is usually no longer classed as personal data because 'if one cannot view the data, then one cannot identify the individual concerned'.[14] Nevertheless, such an assessment will strongly depend on the type of encryption used and the level of security that the encryption provides.[15] Anonymised and pseudonymised data stand changed through a one-way medium which cannot easily be reversed. The query in this instance is whether or not a person may remain identified through identifiers which are directly or indirectly linked. In typical scenarios, the use of the same variable will enable identification through external data sets when comparing the variables and derive a pattern from which the process cannot easily be reversed.[16] Deleting such direct identifiers was previously considered as adequate regarding the European courts. Nonetheless, this view may change going forward, based on technology development within the cloud environment, which allows a much easier identification base point of the vast amount of available data.[17] The volume of data actually

[13] *Ibid.*

[14] HON, W.K., MILLARD, C. and WALDEN, I. (2011) *The problem of 'personal data' in cloud computing - what information is regulated? The cloud of unknowing, Part 1.* SSRN. http://papers.ssrn.com/ [Accessed 9 March 2016]. p. 211.

[15] HON, W.K. et al. (2014) *Cloud accountability: The likely impact of the proposed EU data protection regulation*. Research Gate. https://www.researchgate.net/ [Accessed 19 March 2016].

[16] European Union. (2012) *Article 29 Data Protection Working Party Opinion 05/2012 on Cloud Computing Adopted July 1st 2012*. EC Europa. http://ec.europa.eu/justice/ [Accessed 6 January 2016].

[17] *Volker und Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v. Land Hessen. References for a preliminary ruling: Verwaltungsgericht Wiesbaden - Germany. Joined cases C-92/09 and C-93/09*. Eur-Lex. http://eur-lex.europa.eu/ [Accessed 30 May 2016].Protection of natural persons with regard to the processing of personal data - Publication of information on beneficiaries of agricultural aid - Validity of the provisions of European Union law providing for that publication and laying down detailed rules for such publication - Charter of Fundamental Rights of the European Union - Articles 7 and 8 - Directive 95/46/EC - Interpretation of Articles 18 and 20.

processed in the cloud is growing exponentially. Invariably the accumulation of data will slowly but steadily decrease the efforts required to identify and attribute specific characteristics to an individual.

Personal data is defined by the regulation as data from which a natural person 'can' be identified.[18] In the light of the forms mentioned above, additional clarification would be necessary to safeguard legal confidence for cloud service providers. It is crucial for cloud service providers to know that the data, which they store or handle, is in fact personal data. Having the information about the personal data would then ensure that they observe the requirements regarding the Data Protection Regulation to transfer the data to the USA in compliance with the EU data protection laws. Compared to the Data Protection Regulation and including an exclusive definition of pseudonymous data,[19] it appears to be a positive step towards the realisation that the cloud is evolving and that legislative action is necessary to address the requirements of the market. At the time the proposed definition of pseudonymous data required that additional data which in combination with other data could identify a person must be stored separately and subjected to special protective measures.[20]

Also, a definition of encrypted data remained, which required the data to be unintelligible to any unauthorised persons.[21] However, maintaining a definition of personal data which depends on encryption or anonymization techniques used by a customer is unsatisfactory as it also affects the cloud service provider's classification as controller or processor.[22]

In addition to the general classification of personal data regarding a person's quality of being identifiable, the Data Protection Regulation also addressed the problems associated with the genetic and biometric data by including a definition in the Data Protection Regulation and imposing special requirements on processing this type of data. It is well known that Facebook can run biometric identification through facial recognition[23] over their user profiles, allowing for the identification of a person. The physical characteristics of an individual may also be analysed by this method. To what extent this data can be used for commercial purposes is

[18] PDPR. (2013). Eur-Lex. http://eur-lex.europa.eu/ [Accessed 6 February 2016]. Article 4(2).
[19] Idem. Article 4(2a).
[20] Idem. Article 83(1b).
[21] Idem. Article 4(2b).
[22] HON, W.K., MILLARD, C. and WALDEN, I. (2012a) *Who is responsible for 'personal data' in cloud computing? The cloud of unknowing, Part 2*. Queen Mary School of Law, Legal Studies. https://papers.ssrn.com/ [Accessed February 2016].
[23] WILSON, S. (2014) *Facebook's facial recognition technology is a massive surveillance project*. ZDNET. http://www.zdnet.com/ [Accessed 21 November 2016].

subject to the contract governing the relations between the parties. Access to this data by governmental agencies and departments is also possible under certain circumstances.[24]

The Data Protection Regulation provides a further distinction as to particular categories of personal data.[25] Categories included in the definition relate to race origin, political opinions, religion, philosophical beliefs, sexual orientation, trade union activities, genetic or biometric data, data concerning health or sex life, administration sanction judgements, criminal convictions or suspended offences.

Such data cannot be processed unless specific requirements remain fulfilled.[26] The provision is of particular importance for cloud service providers which offer social media services as part of the service offering, including the processing of such data. However, there are exceptions which apply to the handling of personal data, in particular where the individual or data subject has made the data public. The Data Protection Regulation states that the processing of data that relates to personal data and which has been 'manifestly made public by the data subject'[27] is excluded from the restrictions as mentioned above. Cloud service providers are then no longer under a general prohibition regarding the processing of such data.

For a better understanding of a controller and processor, the definitions provided by Directive 95/46/EC are as follows.

> …'controller' means the natural or legal person, public authority, agency or another body which, alone or jointly with others, determines the purposes and means of the processing of personal data. Where the objectives and means of such processing stand set by Union or Member State law, the controller or the specific criteria for its nomination may stand provided for by Union or Member State law;[28]

---

[24] *The USA PATRIOT Act 2006: Preserving Life and Liberty (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism*). Department of Justice. https://www.justice.gov/ [Accessed 26 February 2016].

[25] 2TWENTY4CONSULTING. (2017) *GDPR and cloud service providers.* Legal Technology. https://www.legaltechnology.com/. [Update-Accessed 18 March 2017]. See also DPR Article 9(1).

[26] *Proposal for a Regulation of the European Parliament and the Council 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)*. Eur-Lex. http://eur-lex.europa.eu/. [Accessed 6 February 2016]. Article 9(1).

[27] Idem. Article 9 (2) e.

[28] *EU Data protection 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)*. Eur-Lex. http://eur-lex.europa.eu/ [Accessed 6 February 2016]. Article 2, Definitions.

> …'processor' means a natural or legal person, public authority, agency or another body which processes personal data on behalf of the controller;[29]

8.2.4. Definition of Processing

The term 'processing' as defined by the Data Protection Regulation is of core importance to cloud service providers as it triggers the data protection law the moment the cloud service provider commences the handling of personal data. The data protection law covers a vast array of operational methods of information processing for the cloud service providers and their operations. The definition of 'processing' is like any procedure or set of processes, which is executed on personal data, irrespective of the method:

> …either manually or automated, such as the collection, retrieval, organisation, recording, alteration or adaptation, utilisation, consultation, storing, transmission, dissemination or making the data available, as well as combining or aligning data, restriction and destruction or erasure.[30]

All these modes of operation will invariably be applicable at some point or form in the supply of cloud services. In the real world, these methods impact on every business model offered as a cloud service, in particular, the commonly used three primary models SaaS, PaaS and IaaS. It may as well be recognised that the impact of the operational methods will substantially cover 'X-as-a-Service', which means 'providing of any form of capability across a communications link'. More importantly, the cloud service providers must remain aware that when any European personal data is involved in the cloud process, such data will usually trigger the Data Protection Regulation.

8.3. EU Personal Data Transfers

When personal data is identified as being in the EU territory or that the PDPR applies, based on the targeted exceptions, particular limitations will apply to the data. Data may be transferred freely within the EU as the protection level will stay balanced across all EU member states. Article 1(3) of the PDPR points out that there are no restrictions or prohibitions for any reason regarding the processing of personal data in connection with the protection of a natural

[29] *Ibid.*

[30] *Proposal for a Regulation of the European Parliament and the Council 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)*. Eur-Lex. http://eur-lex.europa.eu/ [Accessed 6 February 2016]. Article 4 (2) and (3).

person.[31] Therefore, any processing or storage of personal information in the cloud, which remains operated in the EU carries no limitation, provided the data stay within the EU.

8.4. EU Personal Data Transfers from the EU to the USA

Cloud-based computing has many attributes. One of the cloud's core attributes is the ability to be scalable and processor based at locations where provisioning will cost the least. Personal data will invariably need to be transferred outside the cloud service provider's local domain to benefit and maximise on the lower service cost gains provided by the cloud technology. For instance, personal data could be processed at a lower rate in a country where it is night-time and server processing power and capacity is not required by the local businesses and their employees.

To take advantage of the lower cost position offered through external cloud systems, an EU based company must be able to transfer the data to another more cost-efficient country. The problem is that the data protection standards in the majority of these low-cost countries are often lower than the EU PDPR and in conjunction with this also very difficult to enforce. The problem of enforceability has been addressed in the PDPR in Article 25 (1), which requires that the controller who does not have an establishment in the EU has to appoint a representative within the EU. This requirement is in line with the previous Data Protection Directive's Article 4(2). Exceptions to this rule apply if the external country provides adequate standards of data protection or if the controller processes data of 5 000 data subjects within a twelve month period.[32]

The territorial scope of the PDPR extends to the processing of all personal information in the context of an institution of a controller or processor in the EU, irrespective of where the processing is performed. Likewise, when the personal information of a data subject in the EU is handled by a controller or processor who is not established in the EU, it will be exposed to the PDPR if the processing is related to the offering of goods or services to the data subjects in the EU or the observing of such persons.[33] This leads to the PDPR having a very broad territorial scope as even a USA-based cloud service provider offering services to the EU customers must adhere to the data protection requirements imposed by the EU laws. The provisions of the PDPR clarify the rule by requiring it to be ostensibly clear that a controller foresees that the service offerings are to data subjects who may reside in one or more of the

[31] Idem. Article 1(3).
[32] Idem. Article 27 (2)(a) and (2)(b).
[33] *Ibid.*

EU member states.[34] Furthermore, if there are no EU subsidiaries of the company or any other physical presence in the EU, the enforcement of any claim will remain a challenge.[35]

The extension of the scope of monitoring activities will in the future pose some challenges for cloud service providers as well as data protection authorities. It includes the tracking of data as well as the gathering of data which is related to a data subject in the EU with the intention of utilising or potentially using the data to create a profile of that person or making a decision about that person. More importantly, it also extends to predicting personal preferences, market behaviours and attitudes. Nowadays, most social cloud service providers already gather data about their customers to fine tune the services and cater to the customers' needs, more specifically to the needs of individual customer's and so will fall under the PDPR definitions.[36]

8.5. EU Law – Requirements for Transferring Personal Data

As a first step, a cloud user should determine where the equipment of the cloud service provider is located to ascertain whether or not a cross-border transfer of data outside the EU will occur. A party transmitting personal data from the EU into the cloud, which is not established on EU servers, must meticulously scrutinise how the service is provided. Subsequently, as a second step, the different server locations must be ascertained to determine which transfer method under EU law is available and most appropriate to the circumstances.

Any transfer outside of the EU must fall under one of the exceptions provided by the PDPR. These include transfers under an adequacy decision by the EU, transfers by way of appropriate safeguards and transfers by way of binding corporate rules. There is a further exception regarding Article 44, which deals with the general principles for transfers.

The concept of determining adequacy by the EC as well as the BCRs[37] and the appropriate safeguards or contractual terms has already been employed by the Data Protection Directive Articles 25 and 26. Principally, the EC will decide based on a list of factors mentioned in Article 41 of the PDPR, which deals with the monitoring of approved codes of conduct, whether or

[34] Idem. Article 3.
[35] BLACK, J. (2008) *Constructing and contesting legitimacy and accountability in polycentric regulatory regimes.* Journal Regulation and Governance. Blackwell Publishing Asia Pty Ltd. pp. 137–143.
[36] Facebook. (n.d.) *Facebook data collection and use policy*. Facebook. https://www.facebook.com/ [Accessed 12 December 2016].
[37] European Commission. (2016) *Overview on binding corporate rules*. EC Europa. http://ec.europa.eu/justice/ [Accessed 12 December 2016].

not an external country fulfils an adequate standard of data protection which would allow the transfer of personal data to that country. In so doing the Commission must define the territorial and sectorial application of their decision.

One of the most commonly used data transfer mechanisms is the 'safe harbour' agreement,[38] which, previously allowed personal data transfers from the EU to the USA. In essence, it required the USA counterpart, receiving the information to have conducted a self-assessment of its data protection systems and be registered with the Department of Commerce. However, in October 2015, the ECJ issued a judgement,[39] which declared the EC's decision 2000/520/EC invalid, 'on the adequacy of the protection provided by the safe harbour privacy principle' as well as the 'frequently tendered questions issued by the USA Department of Commerce'.[40] The result was that the USA-EU Safe Harbour Framework became an invalid mechanism to comply with the PDPR requirements when transferring personal data from the EU to the USA.

In July 2016, the USA Secretary of Commerce and the EU Commissioner jointly announced the approval of the new EU-USA Privacy Shield Framework as a valid legal mechanism, which will comply with the PDPR requirements when transferring personal data from the EU to the USA. The new Privacy Shield Framework replaced the old USA-EU Safe Harbour Framework. Although the USA Department of Commerce has stopped accepting all USA-EU Safe Harbour Certifications, the department continues to maintain the USA-EU Safe Harbour list of participants. Subsequently, the USA-Swiss Safe Harbour agreement has also been amended, with the announcement in January of 2017 that the USA-Swiss Privacy Shield Framework was accepted as the new valid legal mechanism to comply with the Swiss law. The new USA-Swiss Privacy Shield Framework commenced operation in April 2017.

The new Privacy Shield Framework continues in a similar fashion to the Safe Harbour agreement, with safety certification now being provided under the new framework. Nevertheless, it should be noted that the data protection standards in the USA are much lower than the data protection standards in the EU, which are sectoral in nature and varying between

[38] *Safe Harbour Agreement*. http://2016.export.gov/safeharbor/ [Accessed 22 November 2016].
[39] *Maximillian Schrems v. Data Protection Commissioner, joined party: Digital Rights Ireland Ltd, Case C 362/14 2015. (Reference for a preliminary ruling, Personal data, Protection of individuals with regard to the processing of such data, Charter of Fundamental Rights of the European Union, Articles 7, 8 and 47, Directive 95/46/EC, Articles 25 and 28, Transfer of personal data to third countries, Decision 2000/520/EC, Transfer of personal data to the United States, Inadequate level of protection, Validity, Complaint by an individual whose data has been transferred from the European Union to the United States, Powers of the national supervisory authorities)*. Curia Europa. http://curia.europa.eu/juris/ [Accessed 15 April 2016].
[40] *Ibid.*

the different states. Some concerns have been raised regarding the compatibility with EU law where the data is accessed by USA intelligence agencies and used for their purposes. The EC was aware of the USA surveillance framework and still continued to allow transfers under the agreement, although, taking into account the adjustments made under the new arrangement for adequate protection

8.5.1. Personal Data Transfers to a Representative Processor

The cloud environment is often multi-layered, including various cloud service providers, such as an IaaS provider supplying the platform infrastructure to run the software of a SaaS cloud service provider. In such instances, the user must consider the subsequent processing that takes place once the personal data has left the EU under one of the PDPR mentioned exceptions.

New requirements were introduced in the PDPR, including the obligation to seek approval before using a representative processor[41] as the utilisation of a representative processor is the general practice in the cloud environment, especially in multi-layered cloud services. For a SaaS service running on an IaaS platform in the EEA,[42] imposing such a restriction will likely deprive the users of cloud technologies of some of the cloud's main advantages unless a right to do so can be included in the standard contract terms.[43]

Article 30 'Records of processing activities' of the PDPR imposes additional security obligations on processors.[44] The requirements apply to the cloud service providers being processors despite the fact that they may not know that the controlling customer is processing

[41] *PDPR.* (2013). Eur-Lex. http://eur-lex.europa.eu/ [Accessed 6 February 2016]. Article 27.
[42] Government of United Kingdom. (2017) *Countries of the EU and EEA, Countries in the EU and EEA, The European Union (EU) is an economic and political union of 28 countries. Government of the United Kingdom*, UK Government. https://www.gov.uk/eu-eea. [Accessed 12 March 2017]. It operates an internal (or single) market which allows free movement of goods, capital, services and people between member states. EU countries are: Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the UK. The European Economic Area (EEA) includes EU countries and also Iceland, Liechtenstein and Norway. It allows them to be part of the EU's single market. Switzerland is neither an EU nor EEA member but is part of the single market - this means Swiss nationals have the same rights to live and work in the UK as other EEA nationals. There has been no change to the rights and status of EU nationals in the UK, and UK nationals in the EU, as a result of the referendum.
[43] Ministry of Justice. (2012) Summary of Responses, Call for Evidence on Proposed EU Data Protection Legislative Framework. Consult Justice. https://consult.justice.gov.uk/ [Accessed 12 March 2016].
[44] *PDPR.* (2013). Eur-Lex. http://eur-lex.europa.eu/. [Accessed 6 February 2016]. Article 30.

personal data as they are only supplying the capabilities for various possible processing activities.

However, the processor must ensure that it has retained the right to transfer the data to a representative processor under the contract with the controller. In any case, the representative processor must adhere to the minimum data protection requirements set by the controller in its contract with the processor.

No further extension of powers is allowed as the processor cannot transfer more authority to the representative processor than what the processor has been given by the controller. Consequently once personal data is transmitted to the USA from an EU controller under the Privacy Shield Framework, the USA processor must ensure that its subsequent representative processor in the USA is correspondingly registered with the Department of Commerce under the Privacy Shield Framework. If the successive processor intends to transfer the data abroad to a third country, one of the exceptions under the PDPR must also apply to the transfer as if the data were transferred from the EU location directly. Such an approach is necessary to ensure that the data protection level advocated by the EU is upheld.

In practice, there is no possibility of legally imposing those obligations directly through the PDPR on such a third party.[45] However, the processor could be liable as a party to the Privacy Shield Framework or for a breach of the contractual arrangement or a BCR entered into with the controller. Article 83 of the PDPR allows for administrative fines of up to ten million Euro or up to two percent of the total global annual turnover of the preceding financial year, whichever is the higher amount to be imposed on the infringing party. The administrative fines should act as a strong deterrent.[46]

8.5.2. Information Policies

For a cloud customer to exercise his rights, knowledge of the actions undertaken by the cloud service provider is necessary. In this regard, the PDPR requires that the data subject is informed about the purpose, type and duration of the data collected as well as any disclosure to third parties or the sale of data.[47] The information is essential for the individual concerned to determine whether or not the agreed use of their data has been violated and for the person involved to enforce and protect their rights. Once the individual involved is aware of a third-

[45] This may possibly be achieved through contractual agreement. A third party independent certification is often agreed too.
[46] *PDPR*. (2013). Eur-Lex. http://eur-lex.europa.eu/. [Accessed 6 February 2016]. Article 83.
[47] Idem. Article 13.

party data disclosure or transfers to another country with which the person concerned does not agree, the previously given consent can be withdrawn.[48] The right to withdraw such consent is a mainstay of the data subject's rights. Unless one of the standard scenarios of data transfers to third countries under the adequacy decision is present, the person concerned might find that the safeguards taken in an individual case are inadequate and thus object to the transfer on these grounds.[49] In addition, the controller must provide information where it has identified through an impact assessment that the data subject's personal data may be at high risk.[50]

Any withdrawal of consent must be made as easy as was giving consent to the processing of the personal information in the first instance.[51] To comply with this requirement, cloud service providers must establish procedures for the withdrawal of consent, for illustration through the completion of an online consent withdrawal form. Nevertheless, once approval is withdrawn, in most cases, the cloud service provider will no longer be able to offer its services to the customer. Therefore a right to terminate the relationship must be included in the cloud services agreement with the user.[52]

Once the particulars mentioned above, regarding the provisions have remained supplied, the controller must provide accurate information as to whether or not transfer to a third country is intended. This includes information as to whether or not an adequacy decision exists regarding the country in question, alternatively, whether a transfer stands anticipated under Articles 42 (2) or 44 of the PDPR, in which case reference to the appropriate safeguards has to be made together with the means to obtain a copy of such.[53]

8.5.3. Disclosure to Third Parties

Given the present-day international developments in surveillance, in particular recent incidences which involve the USA Central Intelligence Agency and the security breaches linked to the National Security Agency,[54] cloud users must inform themselves about third-party access when storing or processing data in the cloud. Under current USA law, the Foreign

[48] Idem. Article 7.
[49] *PDPR*. (2013). Eur-Lex. http://eur-lex.europa.eu/ [Accessed 6 February 2016]. Article 14 (1)(f).
[50] *Ibid.*
[51] Idem. Article 7(4).
[52] *Ibid.*
[53] *PDPR.* (2013). Eur-Lex. http://eur-lex.europa.eu/ [Accessed 6 February 2016]. Article 14 (1)(f).
[54] SZOLDRA, P. (2016) *This is everything Edward Snowden revealed in one year of unprecedented top-secret leaks.* Business Insider. http://www.businessinsider.com/ [Accessed 28 October 2016].

Intelligence Surveillance Act (FISA)[55] and Patriot Act[56], give government agencies extensive rights in accessing data on USA servers as well as data stored internationally by any USA company. The access rights to the data of USA citizens are limited. However, there are no boundaries to the right to access the data of foreign nationals or for that matter foreign companies once it is determined that no infringement of a USA citizen's constitutional rights are likely to be involved.[57]

As current developments have shown, personal data will need further protection going beyond Safe Harbour and Privacy Shield Frameworks as the current legal boundaries are not sufficient to protect a party from government and third party access. A cloud contract should address these issues and in particular the extent and support of the cloud service provider in resisting a request for information from third parties. Under no circumstances should the cloud service provider contractually be allowed to disclose information voluntarily. The USA has permitted such disclosure and excluded any liability by the cloud service provider under the FISA disclosure provisions or for that matter under the Patriot Act, even though in section 223 the Act does allow for civil liability for the unauthorised disclosure of personal data. To date there have been no procedural actions either through administration or public initiated suites raised under section 223.[58] This is in strong contrast with the European requirements under which the controller must inform the data subject of any disclosure to public authorities regarding Article 13.

Beside the straightforward distinction between a cloud service provider requiring access to data during the cloud hosting and primary data storage, another dimension that needs to be considered is social media in the cloud. In this context, the disclosure of personal data is essential for the cloud service to work as the received data forms an integral part of the business concept of the cloud service provider.[59] The situation is further complicated through

---

[55] *The Foreign Intelligence Surveillance Act of 1978* (FISA) https://it.ojp.gov/ [Accessed 25 February 2016].

[56] *The USA PATRIOT Act 2006: Preserving Life and Liberty (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism)*. Department of Justice. https://www.justice.gov/ [Accessed 26 February 2016].

[57] CORNELL UNIVERSITY. (2012) *Chapter 36 – Foreign Intelligence Surveillance Subchapter IV – Access to certain Business Records for Foreign Intelligence Purposes, S 1861. Access to certain business records for foreign intelligence and international terrorism investigations*. Cornell University Law School. https://www.law.cornell.edu/ [Accessed 26 February 2016].

[58] The USA PATRIOT Act: *MYTH VS. REALITY.* Justice Department. https://www.justice.gov/ [Accessed 25 February 2016].

[59] SHELTON, T. (2013) *Business models for the social mobile cloud transform your business using social media, mobile internet and cloud computing. Hoboken New Jersey*: John Wiley and Sons Inc., http://adnanalhashmi.weebly.com/ [Accessed 14 October 2016].

the increased haze of social media hosting services. For instance extensions of Facebook and WhatsApp, with additional social media services offered to different interest group interactions.[60]

Where the data is more sensitive for business, it becomes more of a contractual issue and other technical methods need to be employed to ensure the protection of the data.

Not only third parties, but also the cloud service provider has an interest in accessing and monitoring the data of its customers. In the one instance, it has to ensure that the data complies with the terms, such as that it contains no copyright infringement or criminal data, and in a second instance, the information can also be useful for marketing and business analytics.

The PDPR requires cloud service providers, as controllers, to ensure that only personal data necessary for the particular purpose is processed and that no data is retained, disseminated or collected beyond the minimum required for that purpose.[61] This provision aims at ensuring that personal information is not distributed to an indefinite number of parties and that the individual concerned is able to retain some level of control. In a cloud environment, the effects of such a limitation strongly depend on the type of cloud service offered. If personal data is processed within a company structure such as for marketing statistics, the processing objectives and mechanisms are much clearer as compared to a situation in which a cloud service provider offers a cloud social media service directly to a large number of individuals. In the particular user context, the cloud service provider will be processing the data on behalf of a series of different purposes, such as marketing, the supply of services and security reasons. The more complex and multi-layered a service offering becomes, the harder it will be for the cloud service provider to ensure that the data is only processed for the specific purpose of providing the service, especially since the service might be linked to the cloud service provider's right to supply tailored advertisements. This provision requires additional clarification.

8.6. Conclusion

In light of the above analysis, it has become clear that personal data transfers in the cloud from the EU to the USA are far more complicated than the old Safe Harbour agreement would have suggested. Going forward, cloud service providers must keep up to date with any

[60] GEBHART, G. (2016) *What Facebook and WhatsApp's data sharing plans really mean for user privacy. Electronic Frontier Foundation.* EFF ORG. https://www.eff.org/ [Accessed 16 October 2016].
[61] *PDPR.* (2013). Eur-Lex. http://eur-lex.europa.eu/ [Accessed 6 February 2016]. Article 23.

changes made to the regulations between the EU and the USA, in particular now with the introduction of the Privacy Shield Framework and how this law will be implemented. Self-assessment of one's data protection compliance carries an inherent incentive only to keep costs down. As there are no regular independent tests of company data protection standards, the risk of detection remains low. EU regulators are faced with the difficulty of enforcing personal data protection abroad in a country where such protection does not exist. Commercial realities, however, place a limit on the extent to which data flow can be controlled as all the main cloud providers are predominantly USA based. Therefore, without allowing transfers to the USA, EU based companies would not be able to participate in the benefits of cloud services. An EU cloud is possible, but would substantially increase costs based on limited user volumes and cloud infrastructure investment and low capacity as well as competing with the cloud service providers in the USA and cost is one of the main reasons for using the cloud in the first instance. Innovative methods will need to be developed to bridge the gap between the legitimate interests of individuals and the commercial realities of the cloud, especially in respect to social media, which is one of the primary drivers of personal data disbursement and needs to be firmly addressed by regulations. Most cloud users are often not aware of the information disclosure involved when utilising cloud-based social media. Therefore, proper safeguards must continue to be developed by regulators and cloud service providers as the boundaries of technology change.

9. Personal Data in the Cloud and Re-identification

9.1. Introduction

What is personal data?

Any personal information legal regime hinges upon whether personal information stands utilised. As basic and obvious as that statement may seem, identification of common constitutive elements of personal information has proved to be a difficult task.[1]

A study covering thirty-six information and data protection laws from thirty countries provides an illustration of the lack of consensus as to what is defined as 'personal data'.[2] In spite of the absence of harmonisation, the study also found the definitions of personal data in most countries revolve largely around the notion of 'identified' and 'identifiable' individuals.[3] The current definition in the EU, as an example, incorporates both categories of people while in the USA legal system, protection is only afforded to the former 'identified' individuals.[4]

Even though the discussion about the concept and definition of personal data has wide-ranging consequences for the governance of such personal data in general, it is particularly relevant to the cloud setting, where data is vulnerable on a global scale, irrespective of the service or business model of the cloud involved. The data rights of individuals or businesses, the duties of a data controller and the host, together with other regulations, are issues of concern when personal data is handled, gathered, stored, or utilised.[5] Naturally, data subjects such as individuals, are inclined to see all their data as personal data, while the cloud service providers tend to think differently about their struggles to save costs and further facilitate business and technology development through the utilisation of the data.[6]

---

[1] *The Protection of Personal Information Act No. 4 of 2013 of South Africa, Policy, Law, Economics and Politics.* http://www.polity.org.za/ [Accessed 6 December 2015].

[2] REIN, W. (2011) *The changing meaning of "personal data"*. Lexology. http://www.lexology.com/ [Accessed 22 February 2016].

[3] *Ibid.*

[4] *The European Parliament and the Council of April 2016. 2016 Regulation 16/679, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*. EC Europa. http://ec.europa.eu/justice/ [Accessed 25 May 2016]. Recital 26.

[5] Idem. Article 12.

[6] COLUMBUS, L. (2013) *Making cloud computing pay*. Forbes. https://www.forbes.com/. [Accessed 23 April 2016].

A plausible solution that may balance the interests of data subjects and cloud operators is to bring personal data protection in line with technological innovation. Encryption technology has contributed significantly to the confidentiality of personal data,[7] but strongly encrypted data take much longer to process and render applications difficult to run.[8] A more viable option is to anonymise data in such a way that individuals are de-identified. Although data anonymization remains extensively used in medical research, the findings of various studies suggest that data can rarely be truly anonymized using current technology.[9] Furthermore, the explosion of information in the big data zone has further shown perfect anonymization to be an illusion.[10] The situation requires us to question our current understanding of the character of personal data and the possible risks their use or misuse entails. Therefore, one of the burning legal issues in the personal data protection arena is whether anonymous, anonymised and pseudonymised data should still be seen as personal data.

While some law reformers in Europe argue that none of the three categories of data should remain branded as personal data,[11] American scholars have proposed some chiefly risk-based regimes.[12] Together with the review of the problems involved in the ongoing discussion, there are areas which support a multilayer legal description and understanding of the so-called privacy component taking into account the various layers of data personalisation. The argument about the contextual approach towards personal data protection should be factored in around the continuous technological assessment of the nature of the data.

Keeping in mind what is usually considered as personal data and that the personal data protection laws in South Africa are still in their infant stage and not yet thoroughly tested, as well as the shifting legal topology of the definition of personal data, it is important to provide a

---

[7] HON, W.K., MILLARD, C. and WALDEN, I. (2011) *The problem of 'personal data' in cloud computing - what information is regulated? The Cloud of Unknowing, Part 1*. SSRN. http://papers.ssrn.com/ [Accessed 9 March 2016]. p. 17.

[8] HON, W.K. et al. (2014) *Cloud accountability: The likely impact of the proposed EU data protection regulation*. Research Gate. https://www.researchgate.net/. [Accessed 19 March 2016].

[9] OHM, P. (2010) *Broken promises of privacy: Responding to the surprising failure of anonymization.* UCLA Law Review. http://www.uclalawreview.org/ [Accessed 11 March 2016]. p. 1704.

[10] SCHONBERGER, V.M. and CUKIER, K. (2013) *Big Data: A revolution that will transform how we live, work.* London: John Murray Publishers.

[11] *Committee on Civil Liberties. Justice and Home Affairs. (2013) on the proposal for a regulation of the European Parliament and of the Council 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) (COM (2012)0011 – C7-0025/2012 – 2012/0011(COD))*. European Parliament. http://www.europarl.europa.eu/ [Accessed 10 March 2016].

[12] SCHWARTZ, P.M. (2013) *Information privacy in the cloud*. Berkeley Law. http://scholarship.law.berkeley.edu/ [Accessed 20 March 2016].

more focused view of two elements of personal data namely that of identified and identifiable data personal data. Some examples coming from various jurisdictions will be presented. However, the focus is best shown using cases from the EU and the USA, considering that the EU law has as a wide selection on the topic of personal data protection. Furthermore, the EU has a comprehensive and elaborate legal system governing personal data protection, in particular the extraterritorial effect of requiring an adequate level of protection in countries to which the EU citizens' data are transferred.[13] In conjunction with the EU perspective and given the global nature of the technology businesses, it simultaneously becomes necessary to include and comprehend the USA legal system on this topic, to present a clearer understanding of personal data protection.

Looking into the blurred shifting lines of what personal data are and what is supposed to be completely anonymised data by assessing the various discussions of re-identification of individuals from so-called anonymous data, the conceptual distinction between anonymous, anonymised and pseudonymous data becomes clearer. Furthermore, a view of judicial decisions which reflect the increasing number of legal practitioners' appreciation and recognition of the categories of personal data brings one to the point where technology development progressively means that every element of data has the potential to constitute personal data. Such an understanding of the nature of personal data has broad implications for cloud service providers.

The current approaches to personal data protection reform are inadequate and suggest that such methods present risks in the assessment rules governing cloud service providers. Moreover, new views suggest that a continuous assessment rules system governing cloud service providers is necessary.

9.2. The Ever-changing Legal Landscape of Personal Data

Identified versus Identifiable. Central to the legal regime governing personal data is the definition of such data. Cloud storage providers are reported to have delivered more than one Exabyte of data under contract in 2012 alone.[14] However, it remains unclear as to precisely how much of the vast amount of data is personal data and how much of this data should still

[13] *EU Data Protection 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).* Eur-Lex. http://eur-lex.europa.eu/ [Accessed 6 February 2016]. Article 2, Definitions.

[14] NASUNI White Paper: *The state of cloud storage*. http://www6.nasuni.com/ [Accessed 8 February 2016].

viewed as personal data. Whether this information becomes personal data is dependent on the decisions made throughout the data processing process in the cloud environment.[15] Therefore the meaning of 'personal data' is fundamental to the debate on IPRs, in particular with the emphasis on the cloud. The POPI Act provides a definition of personal data as the following:

> 'Personal information' effectively stands for information connecting to an identifiable, living, natural person, and also applies to juristic persons where applicable.[16]

The EU GDPR 2016/679 in Article 4 provides a more extensive view of the concept of personal data and states:

> 'Personal data' means, any information relating to an identified or identifiable natural person ('data subject'). An identifiable natural person is one who can be identified directly or indirectly, in particular by reference to an identifier. Such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;[17]

A natural person is denoted as the 'data subject' in both the RSA's and EU context. The POPI Act also expands on the framework of a 'data subject' through numerous supplementary items about personal identification. Particular attention has been given to identification numbers as well as including other factors such as physical, psychological, mental, economic, social and cultural information. In other words, while 'identified' in this context refers to data being used to determine the specific identity of an individual or to distinguish the individual from other members of a group or groups, identifiable points only to the possibility of being identified.[18]

Personal data legislation is similar in various jurisdictions, sharing the same framework for distinguishing between identified and identifiable persons. As an illustration, the Australian Privacy Act defines personal information as the following:

> Information or an opinion, whether factual or not, and whether recorded in a material form or not, about an identified individual, or an individual who is reasonably identifiable.[19]

---

[15] SCHWARTZ, P.M. (2013) *Information privacy in the cloud*. Berkeley Law. http://scholarship.law.berkeley.edu/ [Accessed 20 March 2016].
[16] *The Protection of Personal Information Act No. 4 of 2013 of South Africa, Policy, Law, Economics and Politics*. http://www.polity.org.za/ [Accessed 6 December 2015]. Chapter 1, Definitions.
[17] *GDPR. Regulation (EU) 2016/679*. EC Europa. http://ec.europa.eu/justice/ [Accessed 25 May 2016].
[18] *The Protection of Personal Information Act No. 4 of 2013 of South Africa, Policy, Law, Economics and Politics*. http://www.polity.org.za/ [Accessed 6 December 2015]. Chapter 2.
[19] *Australian Government Privacy Act 1988*. https://www.oaic.gov.au/ [Accessed 6 February 2016].

Further illustrations, which are different from South African legislation and Australia as well as most other laws, are accepted from the USA law term of 'personally identifiable information' or a close variation thereof. This refers to information that identifies a person or a list of specific types of data that constitutes personally identifiable information or PII.[20] In conjunction with the personal data described, there are other Acts such as the Health and Insurance Acts that stipulate similar identifiable personal data or information that identifies the person (data subject).

Clearly, data that does not constitute personal data are subject to far less if any legal regulation. Therefore, if 'identified' refers to specific individuals getting recognised, whereas 'identifiable' points to the possibility, then the former term is inevitably narrow and the secondary is the broad sense and inclusive. One could argue this point, even with an ever-expanding view given the continual advancing nature of cloud technologies.[21] The POPI Act, scope and definition of 'identifiable' personal data,[22,] which 'means likely reasonably to be used' either by the data controller or by any other person to identify the said data subject, also relates to the same in the European Union Data Protection Regulation of 2016 (or previous Directive of 1995).[23.] The primary considerations are what resources are available to identify an individual and the extent to which such resources are readily accessible to the data controller. A hint provided in the POPI Act Definitions is that one should look for such nominative identifiers as identification numbers, addresses or health data. Within the EU Data Protection Directive at Article 26, it envisages the need to allow room for some flexibility and technology innovation by exempting from the need for protection any 'data rendered anonymous' in such a way that the data subject is no longer identifiable.

However, such approaches based on established categories of identifiers and existing anonymisation technology may no longer be helpful. As will be set out in the next section, technology advances now render it common practice to aggregate and combine pieces of seemingly non-personal data to identify individuals and in some cases, contact them or profile them. One can argue that any data may constitute a form of personal identifier, and

---

[20] *Guidance on the Protection of Personal Identifiable Information (PII).* United States Department of Labour. https://www.dol.gov/ [Accessed 7 February 2016].

[21] *European Commission. Proposal for a Regulation of the European Parliament and of the Council 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) [SEC (2012) 73 final]*. European Parliament. http://www.europarl.europa.eu/ [Accessed 6 February 2016].

[22] *The Protection of Personal Information Act No. 4 of 2013 of South Africa, Policy, Law, Economics and Politics*. http://www.polity.org.za/ [Accessed 6 December 2015]. Chapters 1–3.

[23] *GDPR. Regulation (EU) 2016/679*. EC Europa. http://ec.europa.eu/justice/ [Accessed 25 May 2016].

anonymization techniques have become so powerful in the twenty-first century that it makes complete anonymity difficult to guarantee.[24]

The EU GDPR, to a significant extent addresses the various concerns raised and challenges posed by the rapid advancement of technology, including the need to formulate a new definition of personal data as per Article 23. Article 4(2) of the Regulation, which describes personal data as 'any information relating to a data subject' in turn gives the following definition of a data subject, as provided for in Chapter 1, Article 4(1):

> …'data subject', means an identified natural person or a natural person, who can stand recognised, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person. In particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical physiological, genetic, mental, economic, cultural or social identity of that person.[25]

Taking into account the current POPI Act, personal data definitions as well as the proposed new definitions, the concept of personal data has been expanded to include 'any information' relating to a data subject, whereas the standard for 'identifiable' is now substituted with any, direct or indirect means that are reasonably likely to be used. The list of nominative identifiers has also been expanded to include new categories such as biometrics, location data and online identifiers. Nevertheless, to a large extent, Recital 23 of the new GDPR merely reiterates Recital 26 of the Directive by continuing to rely on the concept of 'identifiable' and excluding the category of anonymous data defined as data that can no longer be recognisable from the regulatory regime.[26] Recital 24 of the GDPR also stipulates that 'identification numbers, location data, online identifiers or other specific factors as such need not necessarily be considered as personal data in all circumstances.'[27]

---

[24] OHM, P. (2010) *Broken promises of privacy: Responding to the surprising failure of anonymization*. UCLA Law Review. http://www.uclalawreview.org/ [Accessed 22 July 2017]. p. 1710. See also, *European Commission. Proposal for a Regulation of the European Parliament and of the Council 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) [SEC (2012) 73 final]*. European Parliament. http://www.europarl.europa.eu/ [Accessed 6 February 2016].

[25] Idem. Article 4(1).

[26] *Committee on Civil Liberties. Justice and Home Affairs. (2013) on the proposal for a regulation of the European Parliament and of the Council 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) (COM (2012)0011 – C7-0025/2012 – 2012/0011(COD))*. European Parliament. http://www.europarl.europa.eu/ [Accessed 10 March 2016]. Recital 23.

[27] Idem. Recital 24.

Therefore, it can be seen that the GDPR offers more protection to personal data by broadening the very concept of personal data to include all information, while allowing room for flexibility by taking into consideration the 'indirect resources' likely to be used to identify individuals. Still, the critical issues remain as to whether a person is capable of being recognised based on all means probable to be used and by reference to available information. There is still a comprehensive range of identifiable information, including anonymous or pseudonymous information which requires different levels of identification effort.[28] Furthermore, the explicit exclusion by both, Directive 95/46/EC and the GDPR of the regulation of anonymous data without clarifying the detailed requirements of what constitutes such data, indirectly provides the industry with a powerful incentive to develop and apply more efficient anonymization techniques.[29] At the same time, as the following discussion demonstrates, whether data can be sufficiently anonymised to render the actual data to form non-personal data, remains highly debatable.

9.3. What is Data Anonymisation when all Data is Considered Personal?

Anonymisation is defined as:

> Definitions (online 2016), Anonymization (Noun): The act or process of making secret, of hiding or disguising identity. This anonymization site is supposed to keep emails from being tracked back to you.[30]

The apparent assumption in excluding anonymous data from legal regulation is that data records can be irreversibly anonymous and that data subjects can be rendered non-identifiable.[31] When the Article 29 Working Party (2012) gave its opinion on cloud, it placed the anonymisation of data on a disparity level with their term of erasure. Likewise, regarding security and control in the cloud environment the European Commissioner for Digital Agenda, pressed the following issue.

---

[28] SCHWARTZ, P.M. and SOLOVE, D.J. (2014) *Reconciling Personal Information in the United States and European Union*: Berkeley University. http://scholarship.law.berkeley.edu/ [Accessed 7 February 2016].

[29] *GDPR. Regulation (EU) 2016/679*. EC Europa. http://ec.europa.eu/justice/ [Accessed 25 May 2016]. Recital 26.

[30] Definitions. (2016) *Anonymization. Definitions*.net. http://www.definitions.net/ [Accessed 11 January 2016].

[31] *European Union. Article 29 Data Protection Working Party Opinion 05/2012 on Cloud Computing Adopted July 1 2012*. EC Europa. http://ec.europa.eu/justice/ [Accessed 6 January 2016].

As with any real life scenario, a user cannot assume that when presenting themselves on any net, there will be no history of their past actions existing in the net. More importantly, where there are incidences with data files, any such data records must be made irretrievably anonymous before further utilisation of the data. What is more significant in cases of data files is that such data records are made as irreversibly anonymous before further utilisation of such data.[32.] Anonymisation is thought to be the perfect 'silver bullet' solution for the reuse of data for privacy, security, innovation and business purposes. With the continued advancement of re-identification technology and resources, however, such data is not what they say it used to be.

9.4. Anonymous versus Anonymised Data.

As discussed, both Article 26 of the Directive 95/46/EC and Article 23 of the GDPR, define anonymous data as 'data rendered anonymous in such a way that the data subject is no longer identifiable' by all resources reasonably possible to be used either by the controller or by any other person, able to identify the individual in question.[33]

In response to the GDPR the European Parliament has formulated another definition, taking anonymous data to be 'personal data that has been collected, altered or otherwise processed in such a way that it can no longer stand accredited to a data subject,'[34] specifically stipulating that 'anonymous data shall not be considered personal data.'

The POPI Act shares a similar regulation regarding the data subject rights and identifying data, in so far as the data is rendered as anonymous once it is no longer identifiable to a data subject. The European Parliament has also proposed that there could be 'alleviations' concerning the use of pseudonymous data in Amendment 36, 61 and 77 of the prior mentioned report of which the proposed definitions were submitted.

> Amendment 36
>
> Proposal for a Regulation Article 4 – point 3 a (new) (3a), 'pseudonymous data' means, any personal data that has been collected, altered or otherwise processed so that it of itself cannot remain attributed to a data subject, without the use of additional data. Which, is subject to separate and distinct technical and organisational controls to ensure such non-attribution.

[32] KROES, N. (2010) *Cloud computing and data protection*. Europa Press. http://europa.eu/rapid/ [Accessed 8 January 2016].
[33] *EU Data protection Directive 95/46/EC*. Eur-Lex. http://eur-lex.europa.eu/ [Accessed 6 February 2016]. Article 23.
[34] *GDPR. Regulation (EU) 2016/679*. EC Europa. http://ec.europa.eu/justice/ [Accessed 25 May 2016]. Article 26.

Amendment 61

Proposal for a Regulation Article 4 – point 3 b (new) (3b) 'pseudonymous data' means any personal data that has been collected, altered, or otherwise processed so that it of itself cannot remain attributed to a data subject without the use of additional data. Which is subject to, separate and distinct technical and organisational controls to ensure, such non-attribution or that such attribution would require a disproportionate amount of time, expense, and effort.

Amendment 77

(2a) 'pseudonymous data' means any personal data that has been collected, altered without the use of additional data which is subject to separate and distinct technical and organisational controls to ensure such non-attribution;[35]

In other words, the use of pseudonymised data involves explicit identifiers being replaced with codes, thus rendering the link of the data to the particular data subject concerned possible.

The preceding legal definitions are based on the notions that

a) 'Data can be made non-identifiable',

b) 'That particular means are more likely than others to be used', and

c) 'That relevant perspective is that of the data controllers or similar persons or entities'.

However, actual data analysis and research call these presumptions into question. For instance, Sweeney (1997) from Harvard University, who specialises in data re-identification research, reminds us that the term 'anonymous' implies that the data can no longer be manipulated or linked in such a way as to identify an individual or data subject.[36] An obvious instance is when data is collected with no identifiers and never related to a person, such as in the case of questionnaires returned by mail without a name or return address.[37] Nonetheless, for data analysis to have a practical use one cannot get rid of all identifiers. Sweeney (1997)[38]

[35] *Committee on Civil Liberties. Justice and Home Affairs. (2013) on the proposal for a regulation of the European Parliament and of the Council 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) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD))*. European Parliament. http://www.europarl.europa.eu/ [Accessed 10 March 2016].

[36] SWEENEY, L. (1997) *Weaving technology and policy together to maintain confidentiality*. Journal of Law, Medicine and Ethics. http://onlinelibrary.wiley.com/ [Accessed 11 February 2016]. p. 100.

[37] The Boston Consulting Group. (2012) The value of digital identity. Liberty Global. http://www.libertyglobal.com/ [Accessed 11 February 2016].

[38] SWEENEY, L. (1997) *Weaving technology and policy together to maintain confidentiality*. Journal of Law, Medicine and Ethics. http://onlinelibrary.wiley.com/ [Accessed 11 February 2016]. pp. 100–101.

shows that in most cases there are significant difficulties in ensuring that data is completely anonymous because of the unusual or unique information appearing within the anonymous data itself. Additionally, different sets of data can often easily be matched to re-identify the individuals or data subject owing to the presence of certain personal characteristics.[39] Although there are various ways of maintaining personal confidentiality to varying degrees, Sweeney (1997) persuades against describing the process as the 'de-identification' of data and the final product as 'de-identified' data.[40] The use of such terminology stays reflected in areas of USA legislation. For instance, the Department of Health and Human Services Administrative Simplification Rules require the 'de-identification of protected health information' before such data is used or further disclosed.[41] However, the more frequently used term when personal identifiers such as names, identity numbers or any forms of credit card numbers are removed is referred to as 'anonymised data'.[42]

9.5. The Deliberation over Anonymised Data

The current and suggested definitions for personal data, data subjects, anonymous data and pseudonymous records in the EU regime, in essence refer to anonymised data. The critical issue remains the regulation of the 'identifiability' of data, which is dependent on the means that are likely and reasonably available and the parties with the ability to use them. It is thus rather unsurprising that the European Parliament's proposals to exempt anonymous data from the regulatory regime and to introduce a lesser standard for pseudonymous data have been met with caution by more than 100 leading European academics[43] from various disciplines such as Computer Science, Economics, Business Administration and Law. Such a position has been described as 'dangerous' by these scholars, as it would allow seemingly protected data to be used to re-identify individuals.[44] The European Commissioner for Justice, Fundamental Rights and Citizenship has warned against the simple use of pseudonymous

[39] Idem. p. 100.
[40] Idem. p. 101.
[41] Department of Health and Human Services: *45 CFR Parts 160 and 164 Standards for Privacy of Individually Identifiable Health Information; Final Rule*. HHS Government. http://www.hhs.gov/hipaa/ [Accessed 12 February 2016]. See also Section 164.514a. Government Publishing Office. https://www.gpo.gov/ [Accessed 12 February 2016].
[42] HON, W.K., MILLARD, C. and WALDEN, I. (2011) *The problem of 'personal data' in cloud computing - what information is regulated? The cloud of unknowing, Part 1.* SSRN. http://papers.ssrn.com/ [Accessed 9 March 2016]. p. 214.
[43] CEPIS. (2013) *Statement on the draft EU general data protection regulation*. CEPIS Council. http://www.cepis.org/ [Accessed 24 February 2016].
[44] *Ibid.*

data to bypass legal regulation for the same reason, that is, individuals may be easily identified.[45]

Nature of Identifiers

Inherent in the legal definition of personal data is the reliance on specific data identifiers to distinguish individuals. As previously mentioned, the POPI Act gives an indicative explanation of personal data typically being information and unique identifiers about the person concerned. Furthermore, the Act also indicates that the identifiers listed in the Act are not limited to those identifiers. The POPI Act list of identifiers for a living, natural person and juristic persons includes the following:

(a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic, or social origin, as well as 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 individual;
(c) any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other, particular assignments to the person;
(d) the biometric information of the person;
(e) the personal opinions, views, or preferences, of the person;
(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 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 individual;[46]

[45] TAYLOR, S. (2013) *Reding warns against identity changes to bypass data privacy. Commissioner gets tough on pseudonymous data.* European Voice. http://www.politico.eu/ [Accessed 15 March 2016].
[46] *The Protection of Personal Information Act No. 4 of 2013 of South Africa, Policy, Law, Economics and Politics.* http://www.polity.org.za/ [Accessed 6 December 2015]. Chapters 1–3.

Furthermore, on the meaning of a 'unique identifier', it is important to understand the description as set out by the POPI Act.

> 'Any identifier that is assigned to a data subject and is used by a responsible party for the purpose of the operations of that responsible party and that *uniquely* identifies that 'Data subject' about that responsible party.[47]

The POPI Act and the EU laws mention the resources reasonably likely to be used whether automated or non-automated when processing specific identifiers, which include identification numbers and location data. The USA legal system has a similar approach, where it singles out unique identifiers. However, the Department of Health and Human Services: 45 CFR Parts 160 and 164 Standards for Privacy of Individually Identifiable Health Information; Final Rule lists categories of information to be removed to avoid identification.[48] These are the following:

> *Limited data set:* is protected health information, that excludes the following direct identifiers of the individual or relatives, employers, or household members of the individual. Such as Names, Postal address information, other than town or city, State, and zip code.
> Including, phone numbers; Fax numbers; Electronic mail addresses; Social Security numbers. Including, Medical record numbers; Health plan beneficiary numbers; Account numbers. Including, Certificate/license numbers; Vehicle identifiers and serial numbers, including license plate numbers. Including, Device identifiers and serial numbers; Web Universal Resource Locators (URLs); Internet protocol (IP) address numbers. Including, Biometric identifiers, including finger and voice prints; and Full face photographic image and any comparable images.[49]

The belief in this form of legislation is that once these identifiers are detached, data can be anonymised or de-identified and are no longer personal. Another fundamental issue is that the list of identifiers is far from exhaustive. Rather, it should be presumed as wide-ranging, and data that is yet to be considered can, in fact, contain revealing identifiers.

a) Browser-generated behaviour. There have been a few controversial related cases in both cloud and internet usage of general browsing conducts. Notably in the landmark judgement of the Court of Appeal in *Google Inc. v. Vidal-Hall Neutral Citation Number: [2015] EWCA Civ 311*, which may signal a new beginning for data protection litigation.

---

[47] *Ibid.*
[48] Department of Health and Human Services: *45 CFR Parts 160 and 164 Standards for Privacy of Individually Identifiable Health Information; Final Rule.* HHS Government. http://www.hhs.gov/hipaa/ [Accessed 12 February 2016]. See also Section 164.514a. Government Publishing Office. https://www.gpo.gov/ [Accessed 12 February 2016].
[49] *Ibid.*

> The appeal, in this case, raises two important issues of law. The first is whether the cause of action for misuse of private information is a tort, specifically for the rules providing for service of proceedings out of the jurisdiction. The second is the meaning of damage in section 13 of the Data Protection Act 1998 (the DPA); in particular, whether there can be a claim for compensation without pecuniary loss.[50]

The question was whether the tracking and collating of information relating to internet users' usage on a particular web browser by Google constituted misuse of personal data under the United Kingdom Data Protection Act of 1998.[51] To determine the answer the Court had to decide whether the claimants could establish a good case that personal data was involved. The case came about from a complaint that Google had been collecting information from the plaintiffs' computers or other devices used to access the internet, including their personal characteristics, interests, wishes or ambitions, and then later sold this to various firms that subsequently sent targeted advertisements to the claimants. The form of information is known as browser-generated information: 'information which is, automatically submitted to websites and services by the browser on connecting to the internet',[52] which are governed by the conditions in the POPI Act[53].

Google's defence was that browser-generated information is not private, but rather anonymous, as the information is collected and aggregated before being sent on to separate websites and advertising services.[54] The Court was far from convinced by the argument for the simple reason that if there were no personal value in the information, then Google would not have collected and collated the data, as well as earned spectacular returns by selling the data to target advertising organisations.

Mainstream use of browser behaviour to identify individuals and clients has become a normative practice in the marketing field, inviting one to question the entire notion of anonymous or anonymised data. An article, in *The Wall Street Journal* titled 'They know what you are shopping for', reported that more than 75 percent of the top one thousand websites

---

[50] *Google Inc. v. Vidal-Hall Neutral Citation Number: [2015] EWCA Civ 311*. Royal Court of Justice. Government. https://www.gov.im/ [Accessed 12 February 2016].
[51] *United Kingdom Data Protection Act of 1998.* United Kingdom Government. http://www.legislation.gov.uk/ [Accessed 12 February 2016].
[52] *Google Inc. v. Vidal-Hall Neutral Citation Number: [2015] EWCA Civ 311*. Royal Court of Justice. Government. https://www.gov.im/ [Accessed 12 February 2016].
[53] The Protection of Personal Information Act No. 4 of 2013 of South Africa, Policy, Law, Economics and Politics. http://www.polity.org.za/ [Accessed 6 December 2015]. Chapter 2.S2 (4).
[54] *Google Inc. v. Vidal-Hall Neutral Citation Number: [2015] EWCA Civ 311.* Royal Court of Justice. Government. https://www.gov.im/ [Accessed 12 February 2016].

include code from cloud and social networks, such as Facebook's 'Like' and Twitter's 'Tweet' buttons and the code then identifies the individuals along with their internet browser behaviour on a massive scale.[55] There are in fact specialist firms that track particular categories of shoppers to mine their data for third parties.

For instance, GfK is a global full-service market research agency with a more than 13 000 market research experts and is a trusted source of various relevant market data together with a variety of customer data. This data enables the GfK clients to make more profound market-related business decisions.[56] Through the use of ground-breaking technology and data knowledge, GfK converts big data into smart data thus empowering their customers to enhance their competitive advantage and improve on customers' experiences and selections. The company uses original customer data as well as additional data sourced from 'Cookies' or E-Tracker technology. Such data are made available when the users access the internet via various online sites and leave behind the users' 'data fingerprint'.

b) Data fingerprints. It is understood that users and clients provide personal data to companies, whether such information is provided through the web or other electronic means, such as emails. These companies may then forward the personal data to advertisers and marketing agents for various forms of analysis, to extrapolate information about the client's interests. The analysed data is then used to enhance the companies' market research and sales.[57] The data fingerprint information is then easily linked back to the person concerned.[58]

In a study by Cambridge University it was proven that the 'Likes' feature on Facebook could reveal an individual's personality and identity within an accuracy of eighty-five percent and by default, the information is available publicly.[59] This is in contradiction to Facebooks claim that the information or digital records gathered are for use by Facebook and their generic data. The Cambridge study also demonstrated startlingly accurate assessments of Facebook users' personal information such as 'race, age, sexuality, personality and including items such as substance usage and political views',[60] all of which had been inferred from the automated

[55] VALENTINO-DEVRIES, J. and SINGER-VINE, J. (2012) *They know what you're shopping for*. The Wall Street Journal. http://www.wsj.com/ [Accessed 7 March 2016].
[56] GfK. (2016) *Marketing research-specializations*. GfK. http://www.gfk.com/en-za/ [Accessed 23 March 2016].
[57] *Ibid.*
[58] OHM, P. (2010) *Broken promises of privacy: Responding to the surprising failure of anonymization*. UCLA Law Review. http://www.uclalawreview.org/ [Accessed 11 March 2016]. p. 1704.
[59] University of Cambridge Research. (2013) *Digital records could expose intimate details and personality traits of millions*. Cambridge Press. http://www.cam.ac.uk/research/ [Accessed 12 March 2016].
[60] *Ibid.*

analysis of the 'Likes' feature on their Facebook accounts. The researchers also found that the personal information could be extracted from the 'Likes' feature using relatively simple methods, which have significant ethical implications when utilising the data for target advertising and consumer profiling. Together these examples provide substantial evidence that the dependency on identifiers as a reference to benchmark subject data is likely to be under-inclusive and no longer accommodating.

9.6. Data Aggregation and Combination for Re-identification

Beyond the ever-advancing technologies that enable one to unlock the personal side of previously hidden or seemingly meaningless data, re-identification techniques have also been widely used to identify individuals through the aggregation and combination of data or datasets.

(a) *The power of data combination.* Data mining technologies allow the amalgamation of data from different sources, which then freely sanctions the identification of individuals.[61] Two infamous cases of data mining are the 'America Online (AOL) study of search queries' and the 'Netflix movie ratings'.

In 2006, AOL launched the AOL Research Project with the stated aim to support an open research community by posting on its website approximately 20 million search queries made by close to 650 000 AOL search engine users, documenting their online activities over a three-month period.[62] All the data was pseudonymised in the sense that clearly identifying information such as usernames and IPs addresses had been replaced by unique identification numbers. However, this veil of pseudonymous anonymity was quickly lifted by reporters who used pieces of seemingly non-revealing topics, such as 'numb fingers' to '60 single men' to

[61] NETLINGO, N.D. (n.d.) *Data mining*, a.k.a. Knowledge Discovery in Databases (KDD) Netlingo. http://www.netlingo.com/ [Accessed 26 March 2016]. The practice of massaging data to extract value from the numbers, statistics, and information found within a database and to predict what a customer will do next. Data mining software works like this: in the first stage, "data collecting", information is gathered from Website logs and databases; in the second stage, "data refining", user profiles are compared with recorded behaviour to divide the users into groups and to predict their behaviour; in the final stage, "taking action", the business or Website answers a user's question on the fly or sends a targeted online ad to a browser, based on the results in the database. Data mining also refers to gathering and presenting on a Website as much information on one particular topic as possible (this is similar to a guru site).

[62] Nol, M.G. (2006) *AOL research publishes 650,000 user queries. Applied Research. Big Data Distributed Systems.* Open Source. http://www.michael-noll.com/ [Accessed 8 February 2016].

'dog that urinates on everything' and 'landscapers in Lilburn, GA' to trace a sixty-two-year-old widow who lives in Lilburn, Georgia.[63]

The company assigned numbers to the searchers to protect their anonymity. However, this was not much of a protection shield. The number allocated to the user in the discussion was No. 4417749, who had conducted several hundred online searches over a three-month period. With searched topics ranging from '60 single men', 'numb fingers', to 'dogs that urinate on everything'. Furthermore, with every search and every click entry, 'user No. 4417749' grew that much easier to distinguish, with additional online queries such as 'Landscapers in Lilburn, Ga' and several persons with a surname of 'Arnold', together with 'homes sold in shadow lake subdivision Gwinnett County Georgia'. Tiny investigation work had to be performed to narrow down the data trace, which ended in the identification of one 'Thelma Arnold', a 62-year-old widower, living in Lilburn, Georgia and who frequently researched her friends, medical ailments and issues related to her three pet dogs. The discovery principally ended with the eventual dismissal of the AOL researchers responsible for the project and the resignation of the chief technical officer.[64]

In a similar fashion to that of AOL and ironically in the same year, Netflix, the largest online film rental service in the world, also publicly released over a hundred million film rating records, thereby exposing approximately half a million users and movie rankings from the previous five years[65]. Netflix offered a one million dollar prize to anyone who could improve on their film recommendation system by ten percent. Moreover, like AOL, Netflix had apparently pseudonymised all the rating information. While it took three years for the winner to claim the one million dollar prize, it took only two weeks for researchers to announce that they could identify individual subscribers from the film rating records which Netflix had released.[66]

In addition to the current debacle from Netflix, a couple of university researchers in Texas compared the data from Netflix with the data from Internet Movie Database (IMDb), another film rental service, where users of this service also have a rating system for films viewed. The comparison identified individuals to an eighty-four percent accuracy. The researchers say that

---

[63] BARBARO, M. and ZELLER, T. (2006) *A face is exposed for AOL searcher no. 4417749*. Research Gate. https://www.researchgate.net/ [Accessed 28 March 2016].
[64] LEYDEN, J. (2006) AOL sued over search engine data release, Privacy breach suit launched. The Register. https://www.theregister.co.uk/ [Accessed 29 March 2016].
[65] SINGEL, R. (2009) Netflix spilled your Brokeback Mountain secret, lawsuit claims. Wired. https://www.wired.com/. [Accessed 28 March 2016].
[66] OHM, P. (2010) *Broken promises of privacy: Responding to the surprising failure of anonymization*. UCLA Law Review. http://www.uclalawreview.org/ [Accessed 11 March 2016].

with one additional piece of data, such as the date on which a rating was posted, their identification accuracy would be in the region of ninety-nine percent accurate on individual identification.[67]

The two cases illustrate that with sufficient pseudonymous information it is possible to identify individuals. The information in the AOL case was capable of targeting individuals, whereas in the Netflix case, it showed that by cross-referencing databases one could achieve the same results. These examples indicate how combination or amalgamation technology is being used to unlock information which is dormant in databases to trace and target specific individuals.[68]

b) The legal response. Realising the potential and risks of merging and cross referencing data, a number of judges and legislators have attempted to tackle the problem. In *Northwestern Memorial Hospital v. Ashcroft*[69] as an example, the USA Appeals Court Judge ruled that even redacted medical records, those from which protected information identifying individual patients has been removed, are a form of PII because of the potential for the information therein to be easily amalgamated with information available on the internet to identify particular individuals. The case arose from a challenge by the applicant hospital against a Department of Justice subpoena seeking the medical records of individual patients upon whom late-term abortion procedures had been performed. Although all of the medical records sought had been redacted, the court held that most medical records are sensitive by nature, with that sensitivity lying beyond the Health Insurance Portability and Accountability Act's responsibility,[70] particularly in the case of controversial issues such as abortion.[71]

In endorsing the decision of a previous authority, the court explicitly stated that 'whether the patients' identities would remain confidential by the exclusion of the persons concerned names and identifying numbers is questionable … information that in the cumulative can make the

[67] NARAYANAN, A. and SHMATIKOV, V. (2007) *Robust de-anonymization of large sparse datasets. Austin*. The University of Texas. https://www.cs.utexas.edu/ [Accessed 2 April 2016].
[68] SCHONBERGER, V.M. and CUKIER, K. (2013) *Big Data: A revolution that will transform how we live, work.* London: John Murray Publishers.
[69] *NORTHWESTERN MEMORIAL HOSPITAL v. John ASHCROFT, United States Court of Appeals, Seventh Circuit, Attorney General of the United States, Defendant-Appellant. No. 04-1379. Court Decision: 362 Federal Reporter, 3d Series 923; 2004 Mar 26 (date of decision).* Case Law. http://caselaw.findlaw.com/ [Accessed 28 March 2016].
[70] *The Health Insurance Portability and Accountability Act of 1996*. GPO. https://www.gpo.gov/ [Accessed 29 March 2016].
[71] OMSTEIN, C. (2015) *How private is sensitive abortion information?* Pacific Standard. https://psmag.com/ [Accessed 28 March 2016].

possibility of recognition very high'.[72] The judge offered sympathy for the patients concerned. Saying that it was entirely understandable that the women involved would be scared of having the details of such records being redacted and entered into the trial record. The judge stated that persons of their acquaintance or even any experienced Net surfer could swiftly scan through the data and combine the search results information with that of others to expose the women and subject them to threats, humiliation or defamation.[73] The judge made it quite open that such types of medical data should be seen as extremely sensitive and even if anonymized or de-identified, should not be disclosed to the public due to the potential for combination with other data to identify and possibly cause harm to the individuals concerned. The rationality of this reasoning is likely to have wider implications for research using medical data and for the processing of personal data in cloud-based medical databases. (The discussion on genomic or so-called DNA databases in the cloud is not part of this study.)

9.7. Conclusion

Despite the difference between the concepts of personal data in the USA and the EU, the differences between the two methodologies can be reconciled to a certain extent. PII markers, rationalise the current inconsistent USA method to defining personal data. The methods are compatible with essential principles of USA privacy law by focusing on the risk of harm to individuals. PII also is consistent with the methodologies of EU privacy law of the need to provide different categories of information with various classes of protection. In the EU it would provide more custom-made and distinct safeguards. Most importantly, in both the EU and the USA it would improve the personal data protection and privacy aspects by establishing incentivised programmes for companies to maintain information at the lowest form of identifiability. The PII programme would be a starting point for the reconciliation of the deviations in the laws discussed.

Simple re-identification represents a vast change in technology as well as in the current understanding of privacy. Re-identification destabilises years of assumptions around active anonymisation, assumptions that have mapped the channels of government regulations, individuals and business relationships. Notably, governments should react swiftly and forcefully towards such disruptive technology swings to maintain the balance of law and to safeguard communities from impending damage.

---

[72] *Parkson v. Central DuPage Hospital Nos. 80-503, 80-504 cons. 105III. Appellate Court of Illinois, First District third division. 435 N.E.2d 140*. Leagle. http://www.leagle.com/decision/ [Accessed 22 March 2016].

[73] *Ibid.*

Regulators should perform the changes without the reliance of easy application, alluringly non-disturbing, moreover, the desperately weak support of PII. The regulators should use factors which provide a proper assessment of the risks of re-identification while balancing the risks against countervailing principles.

Re-identification technology presents unique new challenges, at the same time unveiling obscurities around the discussions on privacy. The focus of the regulators and other stakeholders on the debates, apparently look at costs and unhindered data flows, whereas questions around re-identification are avoided. The new challenges direct all parties to re-examine the old privacy issues, given the new information about re-identification.

10. Traversing the Cloud

10.1. Introduction

The power of re-identification technology urges the reconsideration of what is termed or defined as personal data or information. The present understanding that such data are any data or information, which relates to an identified or identifiable natural person or juristic person by resources likely to be used by a data controller or another individual or entity in the cloud, is unsurprisingly very broad for several reasons.

Firstly, technology has rendered any form of information potentially identifiable. Most information can now be readily re-personalised, either through in-depth analysis of the information itself or its combination with other data or datasets. With sufficient information, the data in question can be linked back to the individual concerned.

Secondly, the resources reasonably likely to be used are evolving so rapidly that they are often not even contemplated when the data is collected.

Thirdly, data controllers may not be the party that will reuse the anonymised or pseudonymised data for secondary use.

The Netflix case demonstrates that bloggers, reporters and computer science researchers can easily re-identify individuals from a pool of statistical data within a short period. In light of these factors, the European Parliament proposed an amendment to redefine a data subject as, 'an identified natural person or natural person who can get identified, directly or indirectly, by resources reasonably likely to be used by the data administrator or by any other natural or legal person.' On the one hand '*Working together with the controller'* is liable to give inadequate protection to the individuals concerned. On the other hand, if the definition is too sweeping, it will impose an undue burden on the many data controllers or processors in the cloud.

Confining the definition to identified persons and known categories of identifiers or imposing restrictions only on administrators and those working with them is too narrow. The test of whether any data constitute personal data, needs to be dynamic, as even information that is not initially personal in nature may become so if the holders of that information process it for purposes to identify individuals.

Many scholars have pointed to the urgent need to ask hard questions about the nature of data and the realistic risks of people being identified by any given data. For instance some scholars suggest that when a person's identity may not realistically get extracted from anonymized, pseudonymised, encrypted or fragmented data, such different sets of data should not be seen as personal data.[1] In such cases, they say cloud processors are often in the 'cloud of the unknown' and should not be asked to shoulder all of the legal duties under the EU Data Protection Directive. Thus, rather than applying the simple test of identification, these scholars argue that the definition of personal data should stem from the realistic risk of identification after taking into account all means reasonably likely to be used to identify an individual.[2]

On the other side of the Atlantic, American scholars have proposed entirely different regimes that are widely risk-based in nature. One scholar[3] argues that the power of re-identification technology and the 'fragility of anonymization' have rendered the classification of personal data meaningless and that we should move to a cost and harm model in regulating data flows instead.[4] Different scholars[5] offer the alternative model of PII, a so-called PII 2.0, with a different set of legal rules to apply to the range of identified and identifiable data.[6] They further advocate that within the context of cloud, the focus of legal regulation should be about the risks of decision-making with personal data rather than on the mere automation of processing choices.[7]

Building on the work of those and other academics, it contends that there is a need that regimes adopt a nuanced definition of personal data. The definition has to take into account different levels of data personalisation, incorporate regular assessments of the risks associated with the identification, including the reuse of data and the factors in a policy of accountability, based on the harm and benefit to society as a whole rather than on the data subjects' content.

---

[1] HON, W.K., MILLARD, C. and WALDEN, I. (2011) *The problem of 'personal data' in cloud computing - what information is regulated? The cloud of unknowing, Part 1*. SSRN. http://papers.ssrn.com/ [Accessed 9 March 2016]. p. 17.

[2] *Ibid.* See also BRADSHAW, S. MILLARD, C. and WALDEN, I. (2010) *Contracts for clouds: Comparison and analysis of the terms and conditions of cloud computing services*. SSRN. http://papers.ssrn.com/ [Accessed 11 March 2016].

[3] OHM, P. (2010) *Broken promises of privacy: Responding to the surprising failure of anonymization.* UCLA Law Review. http://www.uclalawreview.org/ [Accessed 11 March 2016]. p. 1704.

[4] *Ibid.*

[5] SCHWARTZ, P.M. and SOLOVE, D.J. (2011) *The PII problem: Privacy and a new concept of personally identifiable information.* SSRN. http://papers.ssrn.com/ [Accessed 19 March 2016]. p. 1817.

[6] *Ibid.*

[7] SCHWARTZ, P.M. (2013) Information privacy in the cloud. Berkeley Law. http://scholarship.law.berkeley.edu/ [Accessed 20 March 2016].

10.2. Innovative Methods for De-identified Personal Data

Despite the current paradigm and definition of personal data being problematic, it would be impractical to get rid of the concept of personal data entirely as we need a yardstick for legal regulation. As previously noted, because most data are potentially personal data, the EU's General Regulation has rightly defined personal data as any information relating to an individual. However, to prevent the adoption of an over-encompassing approach, the focus must then be on the regulation of the potential to re-identify individuals. At one end of the spectrum should be identified data, data that clearly identify or single out people, subject to clear regulations and at the other end should be anonymous data. The very few exceptional cases in which data cannot remain connected to any individuals should be excluded from regulation. Most cases are likely to fall in the category of pseudonymised data, such as anonymised or de-identified data, which require careful consideration.

In the proposals of the European Parliament and Council,[8] pseudonymised data may fall in a type of midway category intended for less stringent regulation.[9] The emphasis in the proposals is rightly on the non-attribution to a specific data subject without the use of additional information, 'as long as such additional information stands retained independently and conditional to technical and organisational measures to ensure non-attribution.'[10] Submissions were made that pseudonymised data can be put into storage in the cloud, while the resources utilised to decouple reference values of the data or to re-identify individuals need to be stored and applied only on physical premises.[11]

The subsequently re-identified data can be used only in secure transactional systems.[12] However, the duty of non-attribution and overall duty of confidentiality within the proposals seems to apply only to organisations internally. In a variation, the USA Federal Trade

---

[8] *Council of the European Union. (2014) Proposal for a regulation of the European Parliament and of the Council 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)-Pseudonymised*. Euro privacy. http://register.consilium.europa.eu/ [Accessed 21 March 2016].

[9] HON, W.K. et al. (2014) Cloud accountability: *The likely impact of the proposed EU data protection regulation.* Research Gate. https://www.researchgate.net/ [Accessed 19 March 2016].

[10] *Council of the European Union. (2014) Proposal for a regulation of the European Parliament and of the Council 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)*-Pseudonymised. Euro privacy, http://register.consilium.europa.eu/ [Accessed 21 March 2016]. Article 4.

[11] MURPHY, A. (2012) *Storing data in the cloud raises compliance challenges*. Forbes. http://www.forbes.com/ [Accessed 22 March 2016].

[12] *Ibid.*

Commission has recommended a more robust system of de-identification and accountability.[13] Rather than toiling with the concepts of anonymous or anonymised and pseudonymised data, the USA Federal Trade Commission acknowledges that the de-identification of data is not foolproof and thus there is always a possibility that individuals will be re-identified. Accordingly, it recommends that firms robustly de-identify and publicly commit to making no attempts to re-identify data and contractually require the same public commitment from any downstream users with which they share information. Such requirements should extend to the sharing of data with third parties owing to the possibility of successive attribution by following parties.

10.3. Data Quality and Quantity

When considering threats external to organisations, data quality and quantity also need to be taken into account. Data quality refers to the nature, sensitivity and connection of data to individuals,[14] with the latter referring to the different degrees of data identifiability or levels of effort required to identify an individual. An illustration of quality and quantity of data is the information presented in 'Google Flu Trends', regardless of whether its predictions are accurate.[15] The information that Google gathered from the online web search queries submitted by millions of individuals were abstracted at a high level and safely aggregated.[16] Data quality is affected by data quantity, as mentioned earlier in the discussion and the volume of a database is determinative of how easy it is to link the information therein to an individual.

The greater in substance it is, the easier that link is to make. However, the law seems to be silent on the amount of data that data controllers may collect, how long they may retain the data and what data may or may not be combined and whether stricter security measures are necessary for large databases. A scholar argues that new quantitative limits and guidelines should be enacted to address these issues.[17] Such restrictions and directives would undoubtedly have an impact on cloud services given the vast quantity of data stored in the cloud, but certainly deserve further consideration.

---

[13] Free Trade Commission. (2012*) Protecting consumer privacy in an era of rapid change*. FTC. https://www.ftc.gov/reports/ [Accessed 19 March 2016]. p. 56.
[14] OHM, P. (2010) *Broken promises of privacy: Responding to the surprising failure of anonymization.* UCLA Law Review. http://www.uclalawreview.org/ [Accessed 11 March 2016].
[15] WILCOX, M. (2016) *The real reason why Google Flu Trends got big data analytics so wrong.* Forbes. http://www.forbes.com/ [Accessed 20 March 2016].
[16] SCHWARTZ, P.M. and SOLOVE, D.J. (2011) *The PII problem: Privacy and a new concept of personally identifiable information*. SSR. http://papers.ssrn.com/ [Accessed 19 March 2016]. p. 1882.
[17] OHM, P. (2010) *Broken promises of privacy: Responding to the surprising failure of anonymization.* UCLA Law Review. http://www.uclalawreview.org/ [Accessed 11 March 2016]. p. 1767.

In summary, when determining what constitutes personal data, one must also consider the quality and quantity of the data in question. Ultimately the core issue in personal data protection is identity protection.

10.4. Risk Assessment of the Disclosure and Reuse of Data

Equally important is the regulation of the disclosure and reuse of personal data, including pseudonymised data, because third parties may identify the individuals concerned through data combination. The risks and adverse effects of profiling through data mining and data combination are well recognised. Data brokers have been collecting, analysing, selling and linking consumer identities without the users' knowledge for some time.[18] For instance, Acxiom, the largest data broker in the USA and a marketing giant, holds an average of 1 500 pieces of information on each of more than 200 million Americans.[19] A projection that each piece of information that users post on Facebook is worth five USA cents and that each Facebook user is worth USA$100 as a source of information.[20] When cloud services are provided, the internet becomes a rich source and pool of data.

At present, there is a limited regulation of the secondary use of data in most jurisdictions, particularly when they take the ostensible form of non-personal data such as anonymised or pseudonymised data. Ultimately this is an issue of data security, relating to the obligations of data controllers to protect against unauthorised data access, use and disclosure by third parties.

However, it can be argued that there remain legitimate reasons to reuse pseudonymised data, such as in pharmaceutical trials and medical data research or for other legitimate purposes that serve the public interest. In such cases scholars have recommended that clear guidelines are set, with minimum standards established for the de-identification before data disclosure.[21] Many have advocated that a particular model should be used to measure the range of risk involved. Different academics have views such as the utilisation of the *'realistic risk of*

[18] Free Trade Commission. (2014) *Data brokers: A call for transparency and accountability*. FTC. https://www.ftc.gov/ [Accessed 23 March 2016]. p. IV.
[19] KROFT, S. (2014) *The data brokers: Selling your personal information.* CBS News. http://www.cbsnews.com/ [Accessed 24 March 2016].
[20] SCHONBERGER, V.M. and CUKIER, K. (2013) *Big Data: A revolution that will transform how we live, work. London*: John Murray Publishers. p. 155.
[21] HON, W.K., MILLARD, C. and WALDEN, I. (2011) *The problem of 'personal data' in cloud computing - what information is regulated? The cloud of unknowing, Part 1*. SSRN. http://papers.ssrn.com/ [Accessed 9 March 2016]. p. 17.

identification"[22] as a benchmark and others suggest the '*substantial risk of being identified."*[23] Ohm provides an aligned opinion (2010) and recommends that any risk assessment take account of

a) the data handling techniques used by the database owners,
b) the nature of information release, with the public disclosure of data being subject to stricter scrutiny,
c) the quality of data involved,
d) the likely motives and economic incentives for anyone to re-identify the data, and
e) the trust culture in a particular industry or sector that is the existing standard of fiduciary duty or duty of confidentiality in that sector.[24]

Furthermore, as data identification and combination technologies are advancing at a rapid pace, it is contended that any risk assessment concerned should be carried out on a regular basis rather than only at the stages of data collection, de-identification and disclosure.

10.5. Accountability

Many of the previous measures are dependent on the compliance framework of the data controllers and the organisations or firms concerned. Individuals often have no idea that their information is being collected, used and processed or that they have been re-identified, let alone being asked to give their informed consent for the unknown, future and secondary use of those data. It is, therefore, important to formulate an alternative privacy framework that is based less on consent and more on holding data controllers accountable for a particular reuse of data based on risk and the likely adverse impact or harm on the data subjects when the unauthorised disclosure and use of data take place. The EU currently affords sensitive personal data special protection. Recital 51 of the EU Data Protection Regulation 2016/679 (Directive) specifies that,

> Personal data which are, by their nature, particularly sensitive about fundamental rights and freedoms merit special protection as the context of their processing could create significant risks to the basic rights and liberties. Those personal data should include personal data revealing racial or ethnic origin, where the use of the term 'racial origin' in this Regulation does

[22] Idem. p. 40.
[23] SCHWARTZ, P.M. and SOLOVE, D.J. (2011) *The PII problem: Privacy and a new concept of personally identifiable information.* SSR. http://papers.ssrn.com/ [Accessed 19 March 2016]. p. 1878.
[24] OHM, P. (2010) *Broken promises of privacy: Responding to the surprising failure of anonymization*. UCLA Law Review. http://www.uclalawreview.org/ [Accessed 11 March 2016]. p. 1765.

not imply an acceptance by the Union of theories which attempt to determine the existence of separate human races.[25]

Personal data 'which are capable by their nature of … infringing on fundamental freedoms (rights) or privacy', should not be processed. Unless the data is likely to be controversial in different contexts and cultures,[26] the sensitive nature of detailed data reveals an individual's religious beliefs, race and health. Particularly sensitive health information such as HIV status may lead to discrimination against that person.[27]

Google's online advertisement Google AdSense is accused of racial bias against African Americans,[28] thus arguably violating the rights to equality and autonomy.[29] Similarly, data that points to age may lead to targeted advertisements against children, the elderly or other vulnerable groups in society, reflecting an imbalance of power. Bearing in mind the threat of harm arising from the re-identification of individual data, organisations need to ensure that sensitive data which may perhaps be better described as critical data are stored separately from the general network. They also need to ensure that access to such data stays cautiously observed, that their combination with other data cannot easily take place and that their public disclosure is impossible.

10.6. Conclusion

Users leave 'data footprints', or also referred to as 'fingerprints', all over the internet, just like a set of prints on a hiking trail, of all the sites which the users have accessed including footprints in the cloud, without even realising that they have left such 'data footprints'.[30] The personal data privacy that has long been appreciated or which the users thought was personal data appears to be distorted. Personal data as such has a distinct life cycle, given that personal data which was once de-identified can be re-identified. Moreover, re-identification technology

[25] *The European Parliament and the Council of April 2016, 2016 Regulation 16/679, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).* Europa. http://ec.europa.eu/justice/ [Accessed 25 May 2016]. Recital 51. See also *Directive 95/46/EC.* EC Europa. http://ec.europa.eu/justice/ [Accessed 22 April 2016].
[26] *Ibid.* See also *Directive 95/46/EC.* EC Europa. http://ec.europa.eu/justice/ [Accessed 22 April 2016].
[27] *The Protection of Personal Information Act No. 4 of 2013 of South Africa, Policy, Law, Economics and Politics*. http://www.polity.org.za/tion-of-personal-information-act-no-4-of-2013-gazette-37067-2013-11-26 [Accessed 6 December 2015]. p. 14.
[28] SWEENEY, L. (2013) *Discrimination in online ad delivery*. SSRN. http://papers.ssrn.com/ [Accessed 23 March 2016].
[29] *Chapter 2 Bill of Rights 1996*. Department of Justice. http://www.justice.gov.za/. [Accessed 25 March 2016].
[30] OHM, P. (2010) *Broken promises of privacy: Responding to the surprising failure of anonymization*. UCLA Law Review. http://www.uclalawreview.org/ [Accessed 11 March 2016].

has become increasingly advanced and fairly commonly used now with big data and cloud computing, where data is handled and processed on a global level. Understandably, data subjects would like all of their data which is stored in the cloud to effectively be treated as personal data and thus be entitled to personal data protection, including retaining control over such information in the form of consent, accessibility, security and notifications of any data breach. Data controllers such as businesses, organisations and researchers feel differently. To ensure that data protection and responsible use of personal data continues and takes into account the life cycles of such data, proper personal data management and technology tools need to address the increased concerns over data quality and quantity as well as the associated risks and harm created by the shifts in personal data protection. It also promotes a move from consent-based governance to accountability-based governance regulation of personal data.

11. Cloud Borders, Territorial Locations, and Private International Law

11.1. Introduction

In most jurisdiction the law takes into consideration the mere accessibility of a cloud service and its targeting of various countries. As a consequence, if a cloud service provider wishes to avoid a particular jurisdiction, it has to territorially limit its offerings, also commonly known as 'bordered cloud.' Targeting, expresses the geographic location and determination of the cloud service provider as the mere accessibility of a service in that geographical location. Similarly, as with the cloud service provider, the regional location and determination of the user could be relevant as well.

11.2. Competent Court

The necessity for a cloud service provider to 'direct their activities to a State' or targeting, is required by the rules protecting consumers in respect of the Regulation (EC) No. 44/2001 Agreement (updated Regulation (EU) No. 1215/2012).[1] These rules apply if there is an explicit or implicit *intention* of the professional to reach the consumers of member states (or of the RSA and other countries outside the EU) at stake and to contract with them. Moreover, it can also be seen as a 'Territorial location determination' intent, a kind of subjective regionalism that can be identified in the facts of a case by the National Courts through the combination of unbiased essentials manifested by the ECJ, as demonstrated in the joined cases of *Peter Pammer v. Reederei Karl Schlüter GmbH & Co KG (C-585/08), and Hotel Alpenhof GesmbH v. Oliver Heller (C-144/09), 2010.*[2]

[1] *The Council of the European Union. (2000) Council Regulation (EC) No. 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters*. Eur-Lex. http://eur-lex.europa.eu/. [Accessed 15 January 2016]. Part 2.1. Read in conjunction with the new regulation. Regulation (EU) No. 1215/2012. Eur-Lex. http://eur-lex.europa.eu/ [Accessed 18 January 2016].

[2] *Peter Pammer v. Reederei Karl Schlüter GmbH & Co KG (C-585/08), and Hotel Alpenhof GesmbH v. Oliver Heller (C-144/09), 2010. (Jurisdiction in civil and commercial matters – Regulation (EC) No. 44/2001 – Article 15(1)(c) and (3) – Jurisdiction over consumer contracts – Contract for a voyage by freighter – Concept of 'package travel' – Contract for a hotel stay – Presentation of the voyage and the hotel on a website – Concept of activity 'directed to' the Member State of the consumer's domicile*

The ECJ at the date of the case had to judge whether Article 5.3 of Regulation (EC) No. 44/2001,[3] jurisdiction, recognition and execution in civil and commercial matters, needed such a 'Territorial location determination' intent to justify competence at the site where the harm had transpired. According to Article 5.3, as interpreted by the judgement of the court in *Handelskwekerij G.J. Bier B.V. v. Mines de Potasse d'Alsace S.A.,*[4] in the problems related to *delict* or *quasi-delict* a wrongdoer residing in the EU may be sued, at the option of the harmed party, in the court of law of the member state where the injury transpired or may transpire, or in those member sates in which a causal event took place or may happen. In Joined Cases, C-509/09 and C-161/10, *E-Date Advertising GmbH v. X and Olivier Martinez and Robert Martinez v. MGN Limited,*[5] which involved the breach of personality rights using content placed on an internet website, the ECJ decided to a given extent that the accessibility of the site and the content in the region of a member state at stake could lead to damage there.

Furthermore, the ECJ has maintained its jurisprudence since the *Fiona Shevill, Ixora Trading Inc., Chequepoint SARL, Chequepoint International Ltd v. Press Alliance SA.* C-68/93[6] case, by adopting this decision and interpretation of Article 5(3) to the issues related to the internet. A person who claims a breach of his or her rights of personality can submit a liability claim to the court of each member state in which litigious content is accessible, but only in respect of the damage directly caused in that specific member state. The harmed party can also submit the claim in respect of all damage caused to a law court of the member state in which the publisher of the content stands established.[7] The ECJ then added a new forum; the alleged harmed party has the right to submit his or her claim 'in respect of all damages caused' to the court of the place of their 'centre of interest'. Centres of interest are defined as the location of

– *Criteria – Accessibility of the website).* Curia Europa. http://curia.europa.eu/juris/ [Accessed 18 January 2016]. par. 65–8 and 75–94.

[3] *The Council of the European Union. (2000) Council Regulation (EC) No. 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters.* Eur-Lex. http://eur-lex.europa.eu/ [Accessed 15 January 2016]. Article 5.3. In conjunction with the new *Regulation (EU) No. 1215/2012 of the European Parliament and of the Council of 12 December 2012, on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast)*. Eur-Lex. http://eur-lex.europa.eu/ [Accessed 18 January 2016].

[4] *Handelskwekerij G.J. Bier B.V. v. Mines de Potasse d'Alsace S.A. Case 21/76*. Curia Europa. http://curia.europa.eu/juris/ [Accessed 16 January 2016].

[5] *Court of Justice of the European Union PRESS RELEASE No. 115/11 Luxembourg, 25 October 2011. Europa*. Rapid Press. europa.eu/rapid/ [Accessed 15 January 2016]. See also Judgement based on Regulation (EC) No. 44/2001. Curia Europa. http://curia.europa.eu/juris/ [Accessed 15 January 2016]. Article 7.2.

[6] *Fiona Shevill, Ixora Trading Inc., Chequepoint SARL and Chequepoint International Ltd v. Presse Alliance SA. Case C-68/93*. Eur-Lex. http://eur-lex.europa.eu/ [Accessed 23 March 2016].

[7] *E-Date Advertising GmbH v. X and Olivier Martinez and Robert Martinez v. MGN Limited*. Europa Rapid Press. europa.eu/rapid/ *[Accessed 15 January 2016].*

his or her habitual residence or even a place where other factors, such as a professional activity, may establish the existence of a particularly close link with that place.[8]

The absence of a specific 'Territorial location determination' of a website is not decisive about the use of Regulation (EC) No. 44/2001, Article 5 in IP matters, as shown by the ECJ in the two cases that follow relating to Trademark and Copyright respectively in *Wintersteiger AG v. Products 4U Sondermaschinenbau GmbH*, C-523/10),[9] (referred to as *Wintersteiger*) and *Peter Pinckney v. KDG Mediatech AG, Case C-170/12*[10] (referred to as *Pinckney*).

In the *Wintersteiger* case, involving the use of Google, Ad Words, the court concerning the competence based on the place where the damage occurred deemed that:

> At paragraph 29; Therefore it must be held that an action relating to infringement of a trade mark registered in a Member State through the use, by an advertiser, of a keyword identical to that trade mark on a search engine website operating under a country-specific top-level domain of another Member State may be brought before the courts of the Member State in which the trade mark is registered. '*The place where the event giving rise to the damage occurred'*

Likewise in the *Pinckney* case, at paragraph 41, the ECJ considered that:

> At the phase of examining the jurisdiction of a court to adjudicate on damage caused. The identification of the place where the unfortunate event giving rise to that injury occurred for the determinations of Article 5 of the Regulation '*can not depend on criteria which are particular to the examination of the substance and which do not appear in that provision'*. Article 5 sets down, as the sole condition that a harmful event has occurred or may occur.[11]

In the case of 'Territorial location determination' intent of the cloud service provider, it only matters that the unfortunate event '*may happen*' in the regional area at stake. In the *Pinckney*

---

[8] *E-Date Advertising GmbH v. X and Olivier Martinez and Robert Martinez v. MGN Limited.* Europa Rapid Press. europa.eu/rapid/ *[Accessed 15 January 2016].* par. 48–9.

[9] *Wintersteiger AG v. Products 4U Sondermaschinenbau GmbH, C-523/10*. (Regulation (EC) No. 44/2001, Jurisdiction and the implementation of judgments in civil and commercial matters.) Jurisdiction 'in matters relating to tort, delict or quasi-delict'. Determination of the location where the harmful event occurred or may occur. Website of a referencing service provider operating under a country-specific top-level domain of a Member State. Use by an advertiser of a keyword matching to a trade mark registered in another Member State. Curia Europa. http://curia.europa.eu/juris/ [Accessed 18 January 2016].

[10] *Peter Pinckney v KDG Mediatech AG, Case C-170/12.* (Regulation (EC) No. 44/2001, Jurisdiction. Matters relating to tort, delict and quasi-delict.) Copyright, Material support reproducing a protected work. Placing online, Determination of the place where the harmful event occurred. Curia Europa. http://curia.europa.eu/juris/ [Accessed 18 January 2016].

[11] *Peter Pinckney v. KDG Mediatech AG, Case C-170/12*. Curia Europa. http://curia.europa.eu/juris/ [Accessed 18 January 2016]. par. 41.

case, that likelihood may arise 'from the probability of obtaining a reproduction of the work to which the rights trusted on by the defendant relate from an internet site accessible within the jurisdiction of the court seized'.[12] Then, if the protection granted by the state of the court seized 'is applicable only in that Member State, (meaning this court) only has jurisdiction to determine the damage caused inside (that) Member State'.[13] Consequently, a cloud service provider runs the risk of being obliged to appear before a member state's court to respond to claims under the copyright law of that state, if the cloud service provider is accessible in that region.

As previously noted, the member states' PIL applies if the defendant is not domiciled within the EU. In Belgium, the legislator had the intention that Article 96.2 of the PIL is understood in the same way as Article 5 of the Regulation (EC) No. 44/2001.

Nevertheless, Belgium courts might consider that the case law of the ECJ would ostensibly be the incorrect way to address cases involving non-EU domiciled defendants and that the mere accessibility of a cloud service provider is not sufficient, no matter what kind of legal claim is at stake.

11.3. Applicable Law and Territorial Location Determination

As opposed to global competence a geographic location determination could be required more often regarding applicable law. Rome I relating to consumer contracts may need the 'Territorial location determination' of the cloud service provider to apply. In that regard, the case law of the ECJ under Regulation (EC) No. 44/2001 rules protecting consumers can be transposed, *mutatis mutandis.*

The 'Territorial location determination' intent of a website provider has especially been required in IP matters. In the judgement of *L'Oréal v. eBay,*[14] the Court emphasised that by simply having access to a website inside the EU is insufficient grounds to find a breach of a Trademark law due to an online offer for sale or advertisement of a product protected by a Trademark. Such an offer or advertisement has to target consumers in the territory of the

[12] Idem. par. 96.
[13] Idem. par. 47.
[14] *L'Oréal SA and others v. eBay International AG and Others*. Reference for a preliminary ruling: High Court of Justice (England & Wales), Chancery Division - United Kingdom. Case C-324/09. Curia Europa. http://curia.europa.eu/juris/ [Accessed 21 January 2016].

national Trademark or in one or more regions covered by the community Trademark, depending on the right at stake.[15]

In a copyright case, the Donner judgement,[16] the Court considered that

> 30. Consequently, the response to the first part of the question referred, is that 'a trader who aims his advertising at members of the public residing in a given Member State'. Furthermore, creates or makes available to them. A particular delivery system and payment method. Alternatively, allows a third party to do so. Thereby enabling those members of the public to receive delivery of copies of works protected by copyright. As in that same Member State creates, in the Member State where the distribution takes place, a 'delivery to the public' under Article 4(1) of Directive 2001/29.[17]

Considering the *sui generis* right on databases, the ECJ again referred to the 'Territorial location determination' to localise an act of re-utilisation within the meaning of Article 7 of the Directive 96/69[18] in the Football Dataco case as illustrated below.[19]

> 36. Accordingly, the mere fact that the website comprising the data in question is reachable in a particular national region is not an adequate basis for concluding that the operator of the Website is carrying out an act of re-utilisation caught by the National law applicable in that territory concerning protection by the sui generis right …
>
> 39. The localisation of a deed of re-utilisation in the region of a Member State to which the information in question, is sent depends on there being evidence of which it may stand determined that the deed discloses an intention on the part of its performer to target persons in that territory …
>
> (See also 'Pammer and Hotel Alpenhof' cases, paragraph 69, and C a se C -324/09 L'Oréal and Others [2011] EC-R I-6011, paragraph 64.)[20]

The 'Territorial location determination' of the cloud service provider could normally be decisive about national public policy law rules applicable to the national territory. This has been the

---

[15] Idem. par. 62–7.

[16] *Case C-5/11 criminal proceedings against Titus Alexander Jochen Donner [2012] ecr Judgment of the Court (Fourth Chamber) of 21 June 2012*. Curia Europa. http://curia.europa.eu/juris/ [Accessed 21 January 2016].

[17] *Ibid.*

[18] *Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of database*s. Eur-Lex. http://eur-lex.europa.eu/ [Accessed 12 March 2016].

[19] *Football Dataco Ltd, Scottish Premier League Ltd, Scottish Football League, PA Sport UK Ltd v. Sportradar GmbH, Sportradar AG, Case C-173/11 ECLI:EU:C:2012:642, 2012*. Eur-Lex. http://eur-lex.europa.eu/ Accessed 12 March 2016].

[20] Idem. par. 39.

case in Belgium concerning the applicability of market practices and consumer protection legislation.

The new European Union Data Protection Regulation 2016/679 (referred to as DPR), aims to lock-in a data controller that is not established in the EEA, but nevertheless offering services to data subjects in the EU.[21] The 'Territorial location determination' will become relevant to define the offer and supply of facilities to these data users as could be the case with the e-privacy directive applying to the handling of individual data about *the provision of* publicly available electronic communications services *in public communications networks in the community.*[22]

11.4. Territorial Location Determination – Intent Evidence

The international nature of the activity of cloud service providers and the use of language or currency other than the currency or language commonly utilised in the territory in which the cloud service provider is established are relevant given the 'Territorial location of determination'.[23]

a) These references for an initial ruling concerning the clarification on Article 15(1)(c) & (3) of Committee Regulation (EC) No. 44/2001 of 22 December 2000 On authority and the recognition and enforcement of judgments in civil and commercial matters (OJ 2001 L 12, p. 1).
b) The references made (i) in proceedings between 'Pammer and Reederei Karl Schlüter GmbH & Co KG ('Reederei Karl Schlüter')', concerning the latter's refusal to reimburse Mr Pammer in full. The cost of a voyage by freighter described on the internet, which he did not undertake (Case C-585/08). Moreover, (ii) in proceedings between 'Hotel Alpenhof GesmbH ('Hotel Alpenhof') & Heller' regarding his rejection to pay his hotel charges for a stay reserved on the internet (Case C-144/09).

[21] *European Parliament and the Council of April 2016, 2016 Regulation 16/679*. EC Europa. http://ec.europa.eu/justice/ [Accessed 25 May 2016].
[22] *Directive 2002/58/EC of the European Parliament and of the Council of 12 July, Official Journal L 201, 31/07/2002 P. 0037 – 0047.* Eur-Lex. http://eur-lex.europa.eu/ [Accessed 25 May 2016].
[23] *Peter Pammer v. Reederei Karl Schlüter GmbH & Co KG (C-585/08), and Hotel Alpenhof GesmbH v. Oliver Heller (C-144/09), 2010*. Curia Europa. http://curia.europa.eu/juris/ [Accessed 18 January 2016].

Likewise, the use of a country code top-level domain (referred to as ccTLD),[24] seems 'in the absence of any evidence to the contrary', for instance a ccTLD utilised for a pun, 'to be, targeted at the customers in the Territory' of the country code.[25] The formation of remote dealings together with services and merchandise reservations or a *fortiori* as well as the remote closure of a customer contract are also relevant.[26] Interpreting Article 15.1 (c) of Regulation (EC) No. 44/2001, the ECJ considered the presence of a connection or causal link between the resources utilised by the professional to aim their undertakings and the closure of an agreement with the consumer, establishing evidence of a 'Territorial location determination'.[27] These elements are of course not exhaustive.[28] It can be asked whether or not a cloud service provider would be considered to have a geographic location determination as soon as it effectively knows or has substantial grounds to know, that it offers its service to inhabitants of a particular territory and nevertheless carries on providing the service. On the one hand, there is a presumption that it does not have such knowledge if users circumvent the 'Territorial location barriers' it sets. On the other hand, measures faking the geographic location, as a small unapplied disclaimer, will never prevent the finding of a geographic location determination.

Svantesson (2012),[29] points out that website providers have many technical means at their disposal to define the audience of their websites.

> 'Territorial Location determination' services, as well as location-alert software applications, have become progressively popular over the past decade. Equally for mobile phones and online applications. The applications cover a vast array of service offerings which include, mapping and navigation, (such as Google Maps and OVI from Nokia), social networking (the likes of Facebook

[24] SVANTESSON, D.J.B. (2014) *Delineating the reach of internet intermediaries' content blocking – "ccTLD Blocking", "Strict Geo-location Blocking" or a "Country Lens Approach"? 11 (2)*. Scripted. https://script-ed.org/ [Accessed 12 April 2016].
[25] *L'Oréal SA and others v. eBay International AG and Others*. Reference for a preliminary ruling: High Court of Justice (England & Wales), Chancery Division - United Kingdom. Case C-324/09. Curia Europa. http://curia.europa.eu/juris/ [Accessed 21 January 2016].
[26] *Daniela Mühlleitner v. Ahmad Yusufi & Wadat Yusufi,* (Jurisdiction in civil and commercial matters – Jurisdiction over consumer contracts – Regulation (EC) No. 44/2001 – Article 15(1)(c) – Possible limitation of that jurisdiction to distance contracts) Case C-190/11. Curia Europa. http://curia.europa.eu/juris/ [Accessed 21 January 2016].
[27] *Lokman Emrek v. Vlado Sabranovic. Case C-218/12*. Curia Europa. http://curia.europa.eu/juris/ [Accessed 18 January 2016].
[28] *Football Dataco Ltd, Scottish Premier League Ltd, Scottish Football League, PA Sport UK Ltd v. Sportradar GmbH, Sportradar AG, Case C-173/11 ECLI:EU:C:2012:642, 2012*. Eur-Lex. http://eur-lex.europa.eu/ [Accessed 12 March 2016]. ECJ noted re-utilisation of database, par. 40–42.
[29] SVANTESSON, D.J.B. (2012). *Time for the Law to take internet geolocation technologies seriously*. Journal of Private International Law, 8 (3), pp. 473–487.

and Foursquare) including safety for stolen or misplaced mobile phones (such as HTCSense.com). Services such as these tell users (and others if required) where the user is as well as allowing them to receive their location relevant content automatically, without the need of an address or postal code. These are the benefits and convenience aspects of 'Territorial location determination' services and location-alert software applications, which, has become an essential and expected aspect of being a mobile phone or online user.

In that regard, one might contemplate that the sheer ease of accessing a service does amount to geolocation determination more often than expected.[30] Most probably, cloud service providers will block access to their services to users in certain locations if the cloud service providers do not want to be subjected to the respective jurisdictional assertions of those territories. The question of the 'Territorial location determination' of cloud service providers is certainly not settled and in most instances they would need to be addressed on a particular case basis.

11.5. Territorial Location Determination of Users

There could be an interest in having cloud services not territorially determined to users in various territories, but nevertheless accessible to them. This could suggest to the user the possibility of subjecting themselves knowingly and wilfully to the different rules of another authority, to take advantage of an opportunity they value, such as a service, which is not available in their national market. In this context, could the 'Territorial location determination' of the users be relevant in jurisdictional issues?

Firstly, consumer protection is not absolute.[31] If a user travels to another country to buy something, their national consumer protection law is not supposed to protect them in the place of purchase of another National law.[32] Figuratively speaking, should the user not be able to 'travel' over the internet as well? If yes, it would be critical that the user knowingly and purposefully crosses the borders (in this instance territorial location). The consumer would know if the services in question are not targeted at those users, in other words, no 'Territorial location determination' from the cloud service provider, in contrast to the commodities on the market in their home market, where national location determination from the cloud service

[30] *Ibid.*
[31] *Peter Pammer v. Reederei Karl Schlüter GmbH & Co KG (C-585/08), and Hotel Alpenhof GesmbH v. Oliver Heller (C-144/09), 2010*. Curia Europa. http://curia.europa.eu/juris/ [Accessed 18 January 2016]. par. 70.
[32] *Daniela Mühlleitner v. Ahmad Yusufi & Wadat Yusufi, Case C-190/11*. Curia Europa. http://curia.europa.eu/juris/ [Accessed 21 January 2016].

provider is expected. A consumer could be interested in accessing a cutting-edge cloud service which is not available or designed for their residential market and knowingly accepts different consumer protection laws.

Secondly, the human rights are also not absolute; individuals may in some circumstances renounce some of these rights.[33] In that regard consent plays a crucial role. The data protection, 'Cross-border Data Flows' also called 'Transborder Data Flows', regime constitutes another illustration. Remarkably, an individual's information may be transmitted to a foreign country without sufficient levels of data protection if the person concerned granted their unmistakable consent.[34] In other words, a user may knowingly and freely consent to the application of less favourable rules of data protection outside their national laws. The proposed regulation upholds that expectation.[35] Some 'Territorial location determination' of the user, the consent to the processing of personal data abroad, is therefore taken into consideration.

11.6. Conclusion

It was shown that authorities may exercise their jurisdiction over the cloud and the internet according to public international law. The conflicts arising from concurrent assertions of courts are solved through PIL in civil cases. These rules permit but not limit the cloud providers' and cloud users' ability to choose the competent Court and applicable law. In PIL the accessibility of a cloud service or territorial location determination intent of its provider may be decisive. It is therefore suggested that the national location determination intent of users could matter if a cloud service is simply accessible to these users.

Finally, as a consequence of the way jurisdiction is asserted and the way cloud or internet service providers may not want to avoid the jurisdiction of some authorities, the cloud and internet are already purposefully and legally 'bordered'. Users have experienced these issues. Moreover, these aspects are not new and will continue to be developed since global harmonisation of laws and values remain as interests in the visions of individuals of a fully protected internet and cloud service.

---

[33] *European Convention on Human Rights*. Council of Europe. http://www.echr.coe.int/ [Accessed 18 February 2016]. Article 8.

[34] *GDPR. Regulation (EU) 2016/679*. EC Europa. http://ec.europa.eu/justice/ [Accessed 25 May 2016]. Recital 26. See also *Directive 95/46*. Article 26.1.

[35] *Proposal for a Regulation of the European Parliament and the Council 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*). Eur-Lex. http://eur-lex.europa.eu/ [Accessed 6 February 2016]. Article 3.2a.

12. Cloud Data, Ownership Rights of Information in the Cloud

12.1. Introduction

Information in the cloud - how does it all interact with its ownership rights, placement of and generation in the cloud? Information control and accountability features related to cloud service users and those users whose information is processed by the cloud are all naturally concerned that they might in one way or another lose their legal rights to their information as soon as it goes into the cloud. The users are also worried or at least ought to be concerned, about who has the rights to the metadata and other analytical information which cloud service providers generate from the user's information. To focus on the legal rights may not necessarily be the most advantageous way to address the ownership issue. Most countries' copyright laws, much like the RSA's copyright laws[1] and confidentiality laws,[2] provide clear guidelines as to who possesses these rights and using the cloud does in no way alter the ownership rights.

However, the cloud performs a different action, which dramatically changes the 'control' regime that a rights owner has over the usage and disclosure of the information. The control of the information which is typically considered in the contract, creating a contractual structure which incorporates all the significant cloud players such as the cloud customers, service providers, carriers, auditors and brokers, is burdensome and problematic. A vast majority of these problems could be more suitably determined through cloud community norms, merged in proper governance instruments and by way of accountability on the part of the cloud performers as to how the information will be exploited.

12.2. Ownership

The belief of proprietorship is deeply rooted in an individual's mindset. This makes it so important that such person's tendency is to place a greater importance on objects which they

[1] *Copyright Act, 1978 (Act No. 98 of 1978 as amended up to Copyright Amendment Act 2002) 2002*, National Legislator SA. http://www.nlsa.ac.za/ [Accessed 3 May 2015].
[2] South African Law Reform Commission. (2005) *Privacy and Data Protection Discussion Paper 109 Project 124*. Justice Department. http://www.justice.gov.za/ [Accessed 6 January 2016].

already own as opposed to identical objects which they do not own.[3] This is related to the so-called 'endowment effect.'

> 'A wine-loving economist we know purchased some agreeable Bordeaux wines years ago at low prices. The wines have significantly appreciated in value so that a bottle that cost only ten dollars when purchased would now fetch two hundred dollars at public sale.
>
> The same economist still drinks some of this wine on occasions, nevertheless would neither be eager to sell the wine at the public sale price nor buy an additional bottle at that price. Thaler (1980) called this pattern, the fact that individuals often petition much more to give up an article than they would be prepared to pay to acquire it, *'the endowment effect.'*

The so-called *'endowment effect'* is much greater when the individual contemplates that he has earned or deserved the owned object.[4]

> Source dependence has numerous implications for human behaviour. A case in point, a policy advanced by the Reagan administration conferred home-ownership on previous renters of public housing. The expectation was that ownership would cause people to value their homes more highly and to treat them better regarding upkeep. Although the current studies do not challenge the logic behind this policy, they do suggest that one's valuation of a home will not increase as much if one is, merely endowed with it, as opposed to feeling that one has earned it (for example: by purchasing it).

This phenomenon has also been apparent about incorporeal objects such as IP, to which authors of IP, assert a greater value on their creations more than individuals who have acquired IP created by another.[5]

These items cause problems when creating cloud services relationships. Customers will be using cloud service providers' platforms to store information in, which they have created or acquired and to generate new data. However, the cloud platforms are owned and operated by the cloud service provider and not the customer. Consequently, clients are inclined to become anxious on the subject of losing ownership of their highly prized information.

---

[3] KAHNEMAN, D., KNETSCH, J.L. and THALER, R.H. (1991) *Anomalies: The endowment effect, loss aversion, and status quo bias. The Journal of Economic Perspectives, 5 (1). pp. 193–206*. Princeton. https://www.princeton.edu/ [Accessed 16 March 2016].

[4] LOWENSTEIN, G. and ISSACHAROFF, S. (1994) *Source dependence in the valuation of objects. Journal of Behavioural Decision Making, 7. pp. 157–168.* CMU. http://www.cmu.edu/ [Accessed 16 March 2016].

[5] BUCCAFUSCO, C. and SPRIGMAN, C. (2010) *Valuing intellectual property: An experiment.* SSRN. Social Science Research Network. http://papers.ssrn.com/ [Accessed 16 March 2016]. p. 7.

The persistent overvaluation of proprietorship leads to a disproportionate importance on maintaining IPRs, although there are no noteworthy possibilities of any loss of proprietorship. The disproportionate level of attention to the IPRs' valuation means that inadequate thought is given to the driving question of control over the information. This is a significant part of where cloud use realistically presents risks, which need to be safeguarded against and achieving a solution to these risks is a challenge.

Cloud customers are inclined to think of information ownership in the same manner as being like the ownership of other types of property. Unquestionably this is not strictly correct. As is well known, information in electronic or digital format is usually not any form of personal property. Nevertheless it is protected by a combination of IP law, confidentiality and contract law amongst others.[6] The combined result of these statutes provides customers with an established set of rights in respect of their information, which is highly comparable in effect to that of owning territorial property. At this juncture and as part of the discussion the combined set of rights shall be referred to as 'ownership' of the information, even though this term is not strictly correct. 'Privacy rights' may also enhance this 'proprietorship' by providing additional control over the information use.

12.3. Uploading Data in the Cloud

Information which is produced external to the cloud will already have an established ownership status. The information will in all probability take the form of data, which the customer intends to process using one or more of the cloud services, typically a software service which will run on the cloud platform. Uploading the information into the cloud will not by itself necessarily change the data ownership.

The primary system of proprietorship remains by way of IP. The IPRs most likely to be relevant are copyright and database rights, which are both mainly found in the EU,[7] as well as personal data protection rights. Notification should also provide that information may also receive trademark and patent protection.

[6] South African Law Reform Commission. (2005) *Privacy and Data Protection Discussion Paper 109 Project 124*. Justice Department. http://www.justice.gov.za/ [Accessed 6 January 2016]. See also *Copyright Act, 1978 (Act No. 98 of 1978 as amended up to Copyright Amendment Act 2002) 2002.* National Legislator SA. http://www.nlsa.ac.za/ [Accessed 3 May 2015].
[7] *Directive 96/91 EC of the European Parliament of 11 March 1996 on the legal protection of database*s. Eur-Lex. http://eur-lex.europa.eu/ [Accessed 16 March 2016].

National copyright laws in South Africa and across the world recognise that copyright subsists in works in a digital form. Nevertheless, these laws vary in their conceptions of what constitutes a 'work'. In the first instance, the South African copyright law definition of a 'work' is best described in *Galago Publishers (Pty) Ltd & another v. Erasmus*.[8]

> In a copyrighted work, what must be considered the product of the author's skill and labour? Noticeably, competent skill and manual labour are required of the author not merely to express the thoughts or ideas which the work contains, but also to arrive at those thoughts or ideas in the first place. For instance, the writing of a Play requires skill and labour on the part of the playwright not only in putting the plot and dramatic incidents into words but also in the initial conception of the plot and events. From this it follows that the product of an author's skill and labour has two components:
>
> The thoughts or ideas contained in the work, and
>
> The form of resources of which the thoughts or ideas stand provided with outward expression.
>
> Together, these two components constitute the 'work' as such. We submit that, together, these are the real objectives of the law's protection and the particular legitimate object of copyright.

In the second instance, English common law and the Commonwealth and other countries whose law originated from English common law, protect all works[9] where sufficient labour, skill or judgement has been used in their creation.[10] There is no requirement for creativity by itself. Nonetheless, information will be protected if its production required minimal effort[11] or not protected if what is produced is too negligible to be recognised as a work.

> In the case of Exxon Corporation v. Exxon Insurance Consultants International Limited [1982] Ch. 119 an original attempt was made to claim copyright protection for the name "Exxon" as a copyrighted work in its right. The challenge was unsuccessful in the Court of Appeal, and copyright has since then stood abandoned as a defence in the name protector's armoury.

---

[8] *Galago Publishers (Pty) Ltd & another v. Erasmus 1989 (1) SA 276 (A) at 283 C*. Law Blog SA. https://lawblogsa.files.wordpress.com/ [Accessed 1 May 2016].

[9] *The Copyright and Rights in Databases Regulations 1997 No. 3032 as amended*, Legislation UK. http://www.legislation.gov.uk/ [Accessed 16 March 2016].

[10] *Ladbroke v. William Hill [1964] 1 All ER 465, 1964*. CIPIL. University of Cambridge. Centre for Intellectual Property and Information Law. http://www.cipil.law.cam.ac.uk/ [Accessed 16 March 2016].

[11] *Cramp & Sons Ltd v. Frank Smythson Ltd [1944] AC 329, 1944*. CIPIL. University of Cambridge. Centre for Intellectual Property and Information Law. http://www.cipil.law.cam.ac.uk/ [Accessed 16 March 2016].

> However, no one seems to have noticed that following modifications in the regulation have reversed Exxon, and copyright can once more be available to protect a name.[12]

It follows that in countries where the civil law protects author's rights as opposed to copyright, these countries lean towards a minimum level of creativity of a work for it to qualify for copyright protection. This is seen in Germany where they possibly have the clearest example of the minimal level requirement in their copyright system as it only requires that there be an inventive step to differentiate a work from simple information.[13] Before the European Union Software Directive 91/250/EEC of 1991, later amended in 2009 (2009/24/EC),[14] the German Courts had held that some forms of software and to an extent operating systems, were functional rather than creative and were thus not protected by author's rights.[15]

Similarly, in the RSA and before the 1992 Copyright Amendment Act,[16] the Courts had initially held that a computer program was a literary work for the purpose of copyright. The Courts have since provided a different view on the definition and translation of a computer program.[17] The Courts have also drawn a further distinction between computer aided and computer generated works.[18] However, the copyright for purely functional information such as data tables is still likely to be seen as a literary work and be afforded copyright protection.

In the USA common law jurisdiction the Supreme Court has rejected the difficult problem of when an author creates a work in a mechanical or functional manner, which entails significant 'sweat of the brow' (*Feist Publications Inc. v. Rural Tel. Svc. Co., Inc.*).[19] It is found in English common law and now requires a minimal level of creativity for copyright protection such as

---

[12] Ernest. (n.d.) *Copyright in names*: Ernest. http://www.ernest.net/ [Accessed 16 March 2016].
[13] Dejure. (1983) *BGH decision BGH GRUR 1983, 377 – Brombeer-Muster*. Dejure. http://dejure.org/ [Accessed 18 March 2016].
[14] *Directive 2009/24/EC of the European Parliament and the Council of 23 April 2009, on the legal protection of computer programs*. Eur-Lex. http://eur-lex.europa.eu/ [Accessed 18 March 2016]. p. L111/18.
[15] Idem. Article 1(3).
[16] *Copyright Amendment Act 125 of 1992*. http://www.gov.za/ [Accessed 3 May 2015].
[17] *Haupt t/a Soft Copy v. Brewers Marketing Intelligence (Pty) Ltd and others 2006 (4) SA 458 SCA. 2006*. Southern African Legal Information Institute. http://www.saflii.org/za/ [Accessed 16 March 2016]. par. 23.
[18] *Payen Components South Africa Ltd v. Bovic Gaskets CC and Others (448/93) [1995] ZASCA 57; 1995 (4) SA 441 (AD); [1995] 2 All SA 600 (A) (25 May 1995)*. Southern African Legal Information Institute. http://www.saflii.org/za/ [Accessed 18 March 2016]. par. 13.
[19] *Feist Publications Inc. v. Rural Tel. Svc. Co., Inc. Supreme Court of the United States, 499 U.S. 340 (1991*). JUSTIA US Supreme Court. https://supreme.justia.com/ [Accessed 22 March 2016].

that in the EU. However, the level of creativity required is lower than that of the requirements of other countries, for instance, Germany.

The EU member states' applicable law for creation provides that if the information is in the form of a database, such database will receive *sui generis* protection on the Database Directive. The situation differs slightly in the RSA as database protection and security are listed as literary work. Computer programs which are in their final stages of source code or object code are afforded *sui generis* treatment.[20] Regarding the European Database Directive, for a database to qualify for protection, there must have been significant quantitative and qualitative mannered outlay in obtaining either verification or presentation of the contents.[21] Therefore, the architect of the database has the right 'to circumvent extraction and reuse all or an extended part of the database, which will be evaluated quantitatively and or qualitatively against the contents of that database.[22]

By also considering the various countries' copyright and database rights regulations, it is assumed that for the mainstream of information which customers upload into the cloud, they will have some form of protection either by copyright or database rights. It should be kept in mind that the scope of those rights will vary according to the applicable law of each country.

The IP privileges of proprietorship will vest in the original authors, or more likely either the proprietor and or assignees of those authors. These principles will also apply to information uploaded into the cloud by service providers, third parties and software houses as well as other database property owners. The only way ownership of IP capitulates, is through a formal assignment of proprietorship or in some countries a dedication of the work to the public domain. The simple uploading of information into a cloud platform or service does not release the rights as described.

It is always possible that the contract between the customer and the cloud service provider might contain terms affecting information ownership. However, if a sample of these terms is scrutinised, it becomes clear that service providers make no attempt to assert proprietorship rights in the customer's IP.[23] Indeed, they are more likely to state explicitly, that ownership

[20] KLOPPER, H.B. et al. (2011) *Law of Intellectual Property in South Africa*. Cape Town: LexisNexis. p. 159.
[21] *Directive 96/91 EC of the European Parliament of 11 March 1996 on the legal protection of databases*. Eur-Lex. http://eur-lex.europa.eu/ [Accessed 16 March 2016].
[22] *Ibid.*
[23] CORDELL, N. (2013) *Intellectual property in the cloud.* Allen and Overy. http://www.allenovery.com/ [Accessed 4 January 2016].

remains with the client. Google terms make it reasonably clear with their clause which stipulates as follows.

> Some of our Services allow you to upload, submit, store, send or receive content. You retain ownership of any intellectual property rights that you hold in that content. In short, what belongs to you stays yours.[24]

However, all service providers use their terms to obtain permission to make certain use of the customer's IP, a case of this is the clause employed by Facebook:

> For content, that is covered by intellectual property rights, like photos and videos (IP content), you specifically give us the following permission, subject to your privacy and application settings. You grant us a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content that you post on or in connection with Facebook (IP License). This IP License ends when you delete your IP content or your account unless your content has been communal with others, and they have not deleted it.[25]

About copyright ownership, there is a second aspect of the law that is relevant to the protection of information and needs to be considered namely confidentiality and trade secrets. A global accord for the minimum level of privacy and confidentiality and trade secrets protection is set out in the Agreement on Trade-related Aspects of Intellectual Property Rights (referred to as TRIPS),[26] which states that protection must extend to information.

> Section 7: Protection of Undisclosed Information. Article 39.2
>
> (2) Natural and legal persons shall have the possibility of preventing information lawfully within their control from being disclosed to, acquired by, or used by others without their consent in a manner contrary to honest commercial practices so long as such information:
>
> (a) is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;
>
> (b) has commercial value because it is secret; and

[24] GOOGLE Inc. (2014) *Terms of service. Your, content in our services*. Google Inc. https://www.google.com/ [Accessed 12 March 2016].
[25] FACEBOOK. (2015) *Terms of service, sharing your content and information.* Facebook. https://www.facebook.com/ [Accessed 12 March 2016].
[26] *Agreement on Trade-related Aspects of Intellectual Property Rights (TRIPS). World Trade Organization. 1994*. WTO. https://www.wto.org/ [Accessed 5 January 2016].

(c) has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.[27]

The RSA together with many other jurisdictions similarly protects non-commercial information which is confidential in nature and has been received subject to an obligation of confidence, expressly or tacitly as in *Vanguard Rigging (Pty) Ltd v. Nordengen and Another*.[28]

A considerable amount of the information uploaded into the cloud, which may or may not be covered by either IP or confidentiality rights, will be confidential in nature and the owners of the information will, therefore, need protection against actual or anticipated unauthorised or otherwise unlawful disclosure. Diligent management and continued maintenance of confidential information are imperative as from the time when the information comes to be known outside of the privacy relationship and it will no longer have protection[29] except in some instances where the information has been 'wrongfully disclosed' such as in breach of confidence. In his judgment in the initial case, *Sage Holdings Ltd and Another v. Financial Mail (Pty) Ltd and Others* Joffe J held that:

> In exercising the right to trade and carry on a legitimate business, a company or other juristic person would be entitled to regard the confidential oral or written communications of its directors and employees as sacrosanct and would in appropriate circumstances stand the right to enforce the confidentiality of those mentioned above verbal and written communications. To my mind, such right would in appropriate circumstances be enforceable against whosoever is in possession thereof and whosoever seeks to utilise it.

A responsibility of confidentiality may arise due to the information communicated in situations where the recipient would presume to be obliged to maintain confidence.[30] Nonetheless, cloud service providers will have no means of determining which portions of the customers' information are confidential. Likewise, the customers will not necessarily understand to what level the information made accessible by the cloud service provider is of a private nature. To

---

[27] OECD. (2015) *Chapter 3. Approaches to the protection of Trade Secrets*. OECD. http://www.oecd.org/ [Accessed 23 January 2016].
[28] *Vanguard Rigging (Pty) Ltd v. Nordengen and Another (983/2012) [2012] ZAGPJHC 284 (30 November 2012)*. Southern African Legal Information Institute. http://www.saflii.org/za/ [Accessed 14 March 2016].
[29] *Financial Mail (Pty) Ltd and Others v. Sage Holdings Ltd. and Another (612/90) [1993] ZASCA 3; 1993 (2) SA 451 (AD); [1993] 2 All SA 109 (A) (18 February 1993)*. Southern African Legal Information Institute. http://www.saflii.org/za/ [Accessed 14 March 2016]. par. 5–10.
[30] *Ibid.*

this end, confidentiality obligations would best be maintained by contractual terms and agreements.[31]

Following the status quo of IPRs ownership in the cloud, owners of privacy rights will not be affected when uploading information into the cloud. As with IP, confidentiality should remain intact, provided that all who will be working with or managing the information remain subject to maintain confidentiality as per the agreement or contract terms.

Privacy in the commercial and public cloud appears to take on an implied manner by the way in which the cloud service provider undertakes to ensure or maintain the confidentiality of the customers' information and may be precisely captured in the agreement or contract terms of service. Services provided by public cloud service providers such as Amazon Web Services and Google cloud storage,[32] as well as Facebook, are more composite due to the multifaceted method of operation of the public cloud, where the model instrument is a point-to-multipoint play, using a friendship relationship which includes other networks and members. In this scenario, confidentiality obligations for the cloud services provider are less palpable. Also, because of the clear operational model of the service and the relationship between the users, drafting privacy or confidential agreements or contractual terms which relate to standard confidence terms and typical user expectations is most likely unsuitable. The terms may also prove to be tremendously difficult to manage and maintain.

To settle any differences with the role of ownership rights in the cloud service relationship, contract law should be able to determine the position through the terms and conditions of the services contract. In all probability, the contract will clarify the copyright and confidentiality relationships in two customs. In the first instance, it is conventional for a contract or agreement to recognise the IPRs that the various parties own, thereby preventing any question of IP freedom bias arising. In the second instance, the contract or agreement may define specific confidential obligations for each party, including any limitations on those obligations.[33] Furthermore, the agreement or a contract may also specify the confidentiality position of the information on termination of the relationship especially on how the customer's information will be handled, deleted or even latently used within the public or commercial cloud contracts.

---

[31] *Vanguard Rigging (Pty) Ltd v. Nordengen and Another (983/2012) [2012] ZAGPJHC 284 (30 November 2012)*. Southern African Legal Information Institute. http://www.saflii.org/za/ [Accessed 14 March 2016]. par. 3.

[32] BUTLER, B. (2013) *Gartner: Top 10 cloud storage providers.* Net Work World. http://www.networkworld.com/ [Accessed 21 March 2016].

[33] South African Law Reform Commission. (2005) *Privacy and Data Protection Discussion Paper 109 Project 124*. Justice Department. http://www.justice.gov.za/ [Accessed 6 January 2016].

12.4. Data and Information Produced in the Cloud

The application of IP laws to information produced in the cloud, whether by the customer or the cloud service provider, provides the same proprietorship results as seen in the above discussion of proprietorship and confidentiality in so far as copyright is concerned. The author of information will be the customer or cloud service provider, or more likely a team member carrying out work instructions during the ordinary course of duty and subject to *'locatio conductio operarum'*, which means that copyright in the information will belong to the author or his or her employer.[34] As long as the applicable law is that of a Berne Convention country,[35] copyright comes into existence immediately when the work is produced. Under the RSA law it is when the ideas which relate to a particular work are reduced to an outwardly visible form, the form with the ideas are entitled to copyright protection and that copyright subsists in all other Berne countries without the requirement for further procedures.

The lack of a fixed territorial nature of the cloud means that it may be hard to discover precisely *'where'* the first recording of the information was made. The footage is unlikely to be a problem as far as the subsistence of copyright is concerned because the national treatment provisions of the Berne Convention depend only on the work having a 'country of origin' in a Convention member state. If the work is published or printed, for instance an online blog posting, then the place of publication is its country of origin, which is almost certainly the location of the server from which its availability was initially made to others, if this is known. If it is unpublished, as is likely for documents produced for internal purposes, then the country of origin would be that of the author's nationality and thus the place of the first recording is irrelevant for the question whether copyright subsists.[36]

Problems of location will thus only arise in respect of non-Berne Convention countries or in a Berne jurisdiction which imposes formalities and requirements for reasons other than qualifying for copyright protection.

The EU, *sui generis* database right is more problematic when databases are hosted in cloud infrastructure. Database rights subsist if the database's makers or the rights holders are

[34] *King v. South African Weather Services (716/07) [2008] ZASCA 143; 2008 BIP 330 (SCA); 2009 (3) SA 13 (SCA); [2009] 2 All SA 31 (SCA) (27 November 2008)*. Southern African Legal Information Institute. http://www.saflii.org/za/ [Accessed 20 March 2016]. par.9.
[35] *Bern Convention Contracting Parties. World Intellectual Property Organization*. WIPO. http://www.wipo.int/ [Accessed 20 March 2016].
[36] Idem. Article 5(4)(c).

nationals of a member state or reside daily in the territory of the Community.[37] The wording has some unexpected consequences, for instance, a UK national who had been living in Hong Kong for several years and created a database there would still benefit from the database right if illegal extraction or re-utilisation occurred in an EU member country. The anomalies of this kind can be expected from legislation which substantially pre-date the arrival of the cloud. More challenging is the question of infringement where either the hosting of the database itself or the persons extracting or re-utilising the contents are located outside physical territories of the EU.

A more likely scenario involves the USA, as they are a major player amongst cloud service providers, with most of the USA corporations and much of their cloud infrastructure located in the USA. USA law provides no *sui generis* protection for databases which consist of factual information and only limited copyright protection for any elements of creativity in a database's structure.[38] Thus, if a database protected by the EU Database rights is hosted on a USA-located cloud server, the rights will only be infringed if the acts of extraction or re-utilisation take place in the EU, rather than at the server. A similar though reversed problem arises if a database is hosted by a cloud server located in the EU and acts of extraction or re-utilisation are carried out by a person located in the USA.

A suspected infraction by Sportradar of the *sui generis* right to which Football Dataco and Others assert to have in a database relating to league football matches in progress 'Football Live' as available in *Football Dataco Ltd, Scottish Premier League Ltd, Scottish Football League, PA Sport UK Ltd v. Sportradar GmbH, Sportradar AG*,[39] (referred to collectively as 'Football Dataco and Others') is reported on below.

The *sui generis* database right under Article 7 of the Database Directive is only provided to databases in which there has been a 'qualitatively or quantitatively' considerable outlay or investment in obtaining either the 'verification or presentation of the contents'. The Court recognised that whether a website operator is jointly liable for infractions which occur by the unassuming opening of their site is a 'significant' question (put plainly), least of all because

[37] *Directive 96/91 EC of the European Parliament of 11 March 1996 on the legal protection of databases*. Eur-Lex. http://eur-lex.europa.eu/ [Accessed 16 March 2016].
[38] *Feist Publications Inc. v. Rural Tel. Svc. Co., Inc. Supreme Court of the United States, 499 U.S. 340 (1991)*. JUSTIA US Supreme Court. https://supreme.justia.com/ [Accessed 22 March 2016].
[39] *Football Dataco Ltd, Scottish Premier League Ltd, Scottish Football League, PA Sport UK Ltd v. Sportradar GmbH, Sportradar AG, Case C-173/11 ECLI:EU:C:2012:642, 2012*. Eur-Lex. http://eur-lex.europa.eu/ [Accessed 12 March 2016].

the answer applies in the same way to claims of copyright infraction. It is best set out in the Court's answer at paragraphs 96 and 97:[40]

> Para 96. If the answer is yes, then the owner of any website anywhere in the world will be a joint tortfeasor with a UK user of that website if the inevitable consequence of access to that site by the user is infringement by that user.
>
> Para 97. I would hold the answer to be yes. The provider of such a website is causing each and every UK user who accesses his site to infringe.

A Court decision of this type of closure means that Courts may fundamentally apply jurisdiction over practically any website operators globally. Moreover, what is particularly relevant for the outcome, is that orders for 'damages' and 'injunctions' may be issued to these website operators. Disappointingly, any further examination of developments in this domain of law are complicated and fall outside of the scope of the current study.

The ECJ refused to make a decision where cross-border acts of extraction took place. However, it did consider the question of re-utilisation by means making the database content available to the public. The Court decided to adopt a pragmatic approach to the issue. In that case the Austrian defendant, Sportradar, hosted extracts from the claimant's database in its home country, from which it was then made available to persons in the UK. The Court held that the process of making available consisted of numerous connected acts some of which occurred in Austria and others where the targeted recipients had remained situated, the UK. Consequently, re-use of content took place in both Austria and the UK.

It is unclear whether this reasoning should apply to acts of extraction, but a plausible case can be produced. Copyright parts of a database in the country (A) has a higher potential impact on the database owner's economic interests[41] if those parts remain logged to permanent storage for subsequent re-utilisation. Thus, a recording in the country (B) is a continuing part of the extraction process so that removal should be considered to have occurred in both (A) and (B).

However, none of these difficulties about infringement affects the necessary conclusion that IPRs subsist in information produced within the cloud and their ownership is no different than if the information had been produced outside.

---

[40] Idem. par. 96 and 97.

[41] *The British Horseracing Board Ltd v. William Hill Organisation Ltd, C-203/02, 2004.* Curia Europa. http://curia.europa.eu/juris/ [Accessed 27 March 2016].

What is potentially different, or perhaps more accurately an entirely new issue, is the question of ownership of metadata and derived information which cloud service providers generate using information owned by their customers. In this instance 'metadata' is referred to as data about the client's data. This is information about the relationships between the user's data and the user and applications together with any provider or third party applications or data such as logs of data access or application usage by the customer or their individual employees or end consumers. The 'derived information' is new information produced by the provider through analysis of customer data or its metadata. The dividing line is of course very blurred.

Cloud service providers will also be producing and storing various types of data, such as operational, billing and metadata while providing their services.[42] The primary function of providing these forms of data is to enable and enhance the customer's use of the cloud service and also for the cloud provider's management purposes, such as charging or billing customers. Additionally, the fact that cloud service providers have possession of and technological control over the information of the client allows them to use data mining[43] tools to trawl through customers' information, either individually or on a combined basis and thereby generate new and potentially valuable information. As a hypothetical example, a cloud service provider to various vehicle underwriters as customers could dig up their data to excerpt information on the accident rates and categories for different brands and models of cars.[44] As a real example, Facebook and Google collect metadata and 'mined' customer information to generate new data about their clients' interests, activities and preferences. The new data can be exploited commercially, often for marketing purposes and is part of the 'price' which customers, to an extent unknowingly, pay for their use of these ostensibly 'free' services.

None of these activities presents any threat to a customer's ownership of their IPRs in information, but they do have a potential impact on its confidentiality. That effect is small if the provider is only using this derived information for its internal use or has implied authorisation to do so. The danger of breach of confidentiality is increased once the provider discloses the derived information to third parties.

There is unsurprisingly no known instance of a cloud service provider deliberately exploiting derived information which recognisably links to its customers without first obtaining the consent of the client, as do Google and Facebook. Taking this path would be commercial suicide once the fact becomes known. Instead, cloud service providers aggregate customer

[42] REED, C. (2010) *Information 'ownership' in the cloud*. SSRN. http://papers.ssrn.com/ [Accessed 14 March 2016]. pp. 8–9.
[43] *Idem*. p. 9.
[44] *Ibid.*

information, analyse that data and exploit the results. In theory, the data remains anonymised, so there is no risk of a breach of confidence.

Unfortunately, anonymised data is not a complete safeguard against confidentiality breaches. In an article by Ohm[45] which has alerted the legal fraternity to advances in re-identification science, which utilises amalgamation of unconnected databases to construct links between pieces of data and thereby identify the person to whom they relate.[46] A cloud service provider's obligation is probably only to take reasonable care to preserve confidentiality[47] and not absolute. Therefore the cloud service provider will have fulfilled this duty if the derived information cannot, in light of the state of technology at the time, foreseeably identify the customer via the use of re-identification technology. However, a wise cloud service provider will need to remain alert to Cloud technology developments in re-identification as a failure to adapt to new technologies can also amount to a failure to take reasonable care.[48]

12.5. Cloud Information Control

If cloud use presents few threats to the ownership of information, what are the real problems? To answer this, a switch in mindset from ownership to a question of use is required.

One important side effect of owning something is that the owner can control its use by others. Information presents a particular difficulty here because it is by nature a *non-rivalrous* good. Its possession, use or enjoyment by one person does not prevent any other person from also possessing, using or enjoying it. Thus, to restrict the use of information by others, something needs to be done to make the work capable of being excluded, or to ensure that re-utilisation

[45] OHM, P. (2010) *Broken promises of privacy: Responding to the surprising failure of anonymization*. UCLA Law Review. http://www.uclalawreview.org/ [Accessed 11 March 2016].
[46] *Ibid.*
[47] *South African Law Reform Commission. (2005) Privacy and Data Protection Discussion Paper 109 Project 124*. Justice Department. http://www.justice.gov.za/ [Accessed 6 January 2016].
[48] *The T.J. Hooper. The Northern No. 30 and No. 17. The Montrose. In re Eastern Transp. Co. New England Coal & Coke Co. v. Northern Barge Corporation. H.N. Hartwell & Son, Inc. v. Same. No. 430. Circuit Court of Appeals, Second Circuit. July 21, 1932. 60 F.2d 737 (1932)*. Harvard Law. https://h2o.law.harvard.edu/ [Accessed 18 February 2016]. Special Note: A company operates two tugs, each towing three barges full of coal for delivery. En route, the tugs encountered a storm which sank the last barge of each tug's tow. The evidence suggests that there was a weather report broadcast over radio which would have warned the tug-captains of the weather and persuaded them to put into harbour. However, the tug-captains only had private radio receiving sets which were broken and their employer did not furnish them with sets for work. At the time of the incident, there was no industry standard or custom of furnishing all boats with radio receivers. If use of a new technology is not standard across an industry, should courts nevertheless require the use in an industry-member's duty of reasonable care? More generally, should the *non*-existence of industry standards limit what courts recognize as reasonable care

of the information is not implemented unless the owner agrees. One way in which a cloud user might do this is via technical restrictions such as encrypting the information so that no one else can use it. However, encryption has drawbacks as well as advantages, and so users often rely on the laws of IP or confidence, each of which grants rights which enable the owner of the information to control some or all the use of that work.

For a cloud service to work, the cloud service provider must necessarily make some use of the customer's information. The terms of facilities will grant permission for this in the form of a license. As far as the client is concerned, ownership of the information now becomes irrelevant as a means of controlling its use. Instead, the customer needs to be confident that the license does not permit applications which the client would wish to constrain.

Such licensing is where the real problem lies and there are several reasons why it is a stubborn problem. First, the actual use of information by the cloud service provider is largely invisible to the customer, based on the information's non-competitiveness. No matter what the cloud service provider is doing with the information, the customer can continue to use it unhindered. This is very different from territorial property, for instance, if one lends one's vehicle to another, one cannot use the vehicle oneself but can to some extent monitor the borrower's use, perhaps by checking the distance driven and inspecting the car for damage. All that most cloud customers can do to discover the possible uses of their information is to read the disclosures made by the cloud service provider, either regarding service or the service description itself. As shall be seen, these are unlikely to be very informative of the uses.

Secondly, the cloud service provider is likely to have little knowledge of any limitations the customer would aspire to place on the use of information. Indeed, each customer is likely to desire different restrictions or at least would do so if the problem was considered. Furthermore, the cloud service provider will possibly be very unsure about their plans and how they will require the use of the customers' information. Cloud business models are evolving rapidly and are very different from what they were a couple of years ago. All this leads to the very open drafting of license terms under which the cloud service provider establishes a broad range of permissions to use customer information.

Finally, even if customers were to stop relying on information ownership to control use, there is little or no scope to negotiate terms of service. The vast majority of cloud services are offered

as commodities, which customers can either take or leave. Even in major commercial cloud transactions, the scope for negotiating limitations on information use is very limited.[49]

Revisiting the cloud service provider terms mentioned before, one can see that these license terms define the cloud service provider's use rights very broadly. Dropbox takes the least extended licence, but even thus is entitled to do anything with the customer's information which is necessary to provide their service.[50] Google goes substantially further also taking rights to do whatever is needed to develop new services:

> The rights you grant in this licence are for the limited purpose of operating, promoting, and improving our Services, and development [of] new ones.[51]

It is worth noting that neither Dropbox nor Google gives any details about what uses they might make of customer information. These license terms are therefore no more than promises about the motives and purposes behind whatever usages they may adopt.

Facebook takes by far the most extensive use rights over its customers' information (See section 12.3). The terms allow Facebook to make any use of the information, for whatever purpose it desires, without limitations of any kind except after the information or the customer's account has been deleted.

The position is clearly unsatisfactory from the client's perspective and ought to be seen as unsatisfactory by the cloud service providers as well. To persuade customers to adopt the convinced benefits of migrating to the cloud, cloud service providers need to overcome their client's fears and doubts. Moreover, given the high value placed on information ownership, as seen earlier, vague and open license terms are highly unlikely to be persuasive. However, moving forward from the current control situation where cloud service providers necessarily draft clauses and are not open to negotiation is clearly difficult.

12.6. Cloud Accountability

[49] HON, W.K., MILLARD, C. and WALDEN, I. (2012b) *Negotiating cloud contracts, looking at clouds from both sides now*. Stanford Technology Law Review. https://journals.law.stanford.edu/ [Accessed 16 February 2016].
[50] DROPBOX. (2014) *Dropbox terms of service posted*. Dropbox. https://www.dropbox.com/ [Accessed 12 April 2016].
[51] GOOGLE Inc. (2014) *Terms of service. Your, content in our services*. Google Inc. https://www.google.com/ [Accessed 12 March 2016].

Numerous scholars have alluded to the fact that applying the concept of accountability to the cloud could assist in mitigating the risks of information exploitation, particularly in respect of IPRs, privacy and confidentiality.[52] There are numerous definitions of accountability, but all have two elements in common, transparency about how the information is intended to be stored and processed and the verification of what has happened to the information in question. Some add a third element, remediation on 'errors or fault correction.'[53]

To achieve greater control over the information use, a cloud customer needs first to know or be able to discover what practice of each element or relevant piece of information is utilised. Because cloud services are often layered, with different elements of services provided by various cloud service providers, the customer will want to know 'who' is storing and processing the information. There may be a need to know 'where' it is being stored and processed, for instance, for data protection compliance purposes. Customers will certainly want to discover any disclosures or other uses of the information which go beyond what is necessary for the provision of the service. They will want to know the likelihood of these things in advance so that they can decide whether to enter into that particular cloud relationship which requires transparency. They will also want to know whether, what was supposed to happen did happen, and if anything which was not meant to happen occurred, which is achieved through verification.

Remediation of 'errors or fault correction' can either be built into the accountability system itself or effected through external organisations such as the Courts or regulators.

Much of the academic texts on answerability (or responsibility) relates to the governance of transnational institutions. In this context, accountability requires a decision maker to explain how he arrived at his decision, which in turn permits those affected by the decision to question the justification or challenge the outcome. All are in agreement that a fundamental prerequisite for accountability is transparency.[54] Hale, translates accountability as:

[52] PEARSON, S. (2011) *Towards accountability in the cloud.* HP. http://www.hpl.hp.com/ [Accessed 27 March 2016]. See also WEITZNER, D.J. et al. (2008) *Information accountability*. MIT Computer Science and Artificial Intelligence Laboratory. http://dig.csail.mit.edu/ [Accessed 22 March 2016].
[53] SCHEDLER, A. et al. (eds.) (1999) *Conceptualizing accountability the self-restraining state: Power and accountability in new democracies*. London: Lynne Reiner Publishers.
[54] IBANEZ, J. (2005) *Who governs the internet? The emerging regime of e-commerce*. Pompeu Fabra. University Barcelona. https://ecpr.eu/Filestore/ [Accessed 12 May 2016].

> Transparency has become the international community's standard retort to liability concerns at international institutions, appearing in the assertions of government and international officials, corporate executives and activists alike.[55]

Transparency requires an organisation to disclose all the information which is necessary for outsiders to determine if it is performing correctly. Such transparency bestows on the communities, or at least in theory, 'the ability to know what a performer is doing and the capability to make that performer do something else.'[56]

Authors argue that transparency on its own goes a substantial distance towards holding a transnational player to account.[57] The three mechanisms of market pressure, public criticism and core standards act as a powerful enforcement mechanism in many cases. Market pressure works through the decisions of suppliers and customers. In the cloud context, customers will be more likely to choose a cloud service provider whose proposed and actual uses of their information are acceptable. Cloud service providers will tend to modify their information uses to attract customers. Public criticism acts imperceptibly, but there is evidence that it too works to change behaviours.[58]

A useful study in the context of how transparency may lead to variations in information utilisation in the cloud is Facebook, who in 2007 set about the launch of a new advertising campaign, termed Beacon. The advertising system targeted transactions of Facebook users. When a user performed any operation with a Facebook partner company, the advertising system would immediately post the details of the operation onto that user's Facebook newsfeed. Consequently, the particular advertising data was forwarded to all Facebook users that subscribed to the particular newsfeed.[59]

User opposition grew rapidly and within a month Beacon was changed to an opt-in system, rather than an opt-out system.[60] All this was a consequence of transparency. Subsequent remediation as a result of the settlement in a class action brought by Facebook users led to

---

[55] HALE, T.N. (2008) *Transparency, accountability, and global governance*. Questa, trusted online research. https://www.questia.com/ [Accessed 12 May 2016]. p. 73

[56] Idem. p. 75.

[57] *Ibid.*

[58] REED, C. (2012) *Making laws for cyberspace*. Oxford: Oxford University Press. pp. 213–214.

[59] KRAVETS, D. (2012) *Facebook's $9.5 Million 'Beacon' settlement approved*. Wired. https://www.wired.com/ [Accessed 3 April 2016]. See also *Fraley et al. v. Facebook, Inc., et al.*, Case No. CV-11-01726 RS. Fraley. http://www.fraleyfacebooksettlement.com/ [Accessed 25 February 2016].

[60] ZUCKERBERG, M. (2007) *Thoughts on Beacon*. Facebook. https://www.facebook.com/ [Accessed 5 April 2016].

Beacon's final discontinuance in 2009 and the establishment of a Privacy Foundation for Facebook.[61] A mere eighteen months later in February 2009, Facebook generated more controversy when it unilaterally deleted a section from its terms which read as follows:

> You may remove your User Content from the Site at any time. If you choose to remove your User Content, the licence granted above shall automatically expire. However, you acknowledge that the Company may retain archived copies of your User Content.[62]

The effect of this was that Facebook would have unlimited rights to use the content indefinitely under the license granted when users signed up. As we have seen, this license permits use by Facebook for any purposes whatsoever. Once a journalist discovered the change and alerted users, over thirty-eight thousand users joined a Facebook group to protest at the change,[63] and there was substantial adverse publicity in the media. Within a few days, Facebook was forced to announce that it was reinstating the term,[64] as a consequence of transparency.

Since then Facebook has made further attempts to share the data of its users as widely as possible, nonetheless to a significant part, these changes have been opposed successfully by users as being contrary to the social norms which they expect to govern their use of the service. Remedies, applied through law, have played a significant part by way of the denigrations made by the EU's Article 29 Working Party,[65] in conjunction with a decision made by the Canadian Privacy Commissioner.[66] Customer antagonism and opposition proved

---

[61] LIGITEC. (2012) *Lane v. Facebook: Privacy class action settlement requires Facebook to pay $9.5 million, but provides no direct benefits to most plaintiffs*. Leon Jacobson ESQ. http://www.nylitigationfirm.com/ [Accessed 21 April 2016].

[62] ASAY, M. (2009) *Facebook changes terms of service to control more user data*. CNET. http://www.cnet.com/news/ [Accessed 21 April 2016].

[63] ANDERSON, G.N. (2010) *Are individuals waking up to the privacy implications of social-networking sites?* European Intellectual Property Review, 32 (3), p. 99.

[64] STONE, B. and STELTER, B. (2009) *Facebook withdraws changes in data use*. New York Times. http://www.nytimes.com/ [Accessed 22 April 2016].

[65] *Article 29 Data Protection Working Party, 2009, Opinion 5/2009 on online social networking.* EC Europa. http://ec.europa.eu/justice/ [Accessed 22 April 2016]. See also Digital civil rights in Europe (n.d.) *Article 29 Working Party on online social networking*. EDRI. http://history.edri.org/ [Accessed 22 April 2016].

[66] DENHAM, E. (2009) *Findings under the Personal Information Protection and Electronic Documents Act (PIPEDA).* Office of the Privacy Commission of Canada. https://www.priv.gc.ca/ [Accessed 22 April 2016].

equally as efficient and a faster method of counteracting the changes to the data use which customers found offensive.[67]

Transparency is inevitable on Facebook. It provides a uniform set of services to all its customers and because it has such a high-profile any changes to the ways it uses customer information are likely to be detected very quickly. However, how is transparency and verification to be achieved for those cloud relationships which are more diverse and subject to far less external scrutiny?

The answer proposed by the EU A4 Cloud Project[68] is the development of technical tools which enable customers to interrogate and obtain automated reports from cloud service providers about the uses made of customer information. These tools are still under development, but as currently proposed they will aim to assist in meeting the A4 Cloud Accountability Project objectives:[69]

> The A4 Cloud Project has four interconnecting objectives. The goals have been set to get the cloud users, cloud providers and regulating authorities aligned regarding accountability for data in the cloud. To spell out the liability and ensuring greater overall transparency and
>
> a) enable cloud service providers to give their users appropriate control and transparency over their data utilisation.
> b) empower users to make choices about how cloud service providers may use and will protect data in the cloud.
> c) monitor and check compliance with users' expectations, business policies, and regulations.
> d) implement accountability ethically and effectively.[70]

The scope of the A4 Cloud Project is limited to data protection and confidential information, but it is clear that the tools could be extended to cover potentially all uses of customer information. If the tools are successful and are adopted by cloud service providers, they will facilitate a high level of transparency and verification for customers.

An important point to note is that these tools will be individually configured by customers so that each client can set his limitations on use and monitor the requirements. This level of

---

[67] TRICHKOVSKAX, C. (2011) *Legal and privacy challenges of social networking sites*. Duo UIO. https://www.duo.uio.no/ [Accessed 24 January 2016].
[68] A4CLOUD. (n.d.) Cloud accountability project. A4CLOUD. http://www.a4cloud.eu/ [Accessed 22 April 2016].
[69] RASHDI, Z.A., DICK, M. and STONY, I (2015) *A conceptual framework for accountability in cloud computing service provision*. Australasian Conference on Information Systems (ACIS). https://acis2015.unisa.edu.au/ [Accessed 25 April 2016].
[70] A4CLOUD. (n.d.) *Cloud accountability project*. A4CLOUD. http://www.a4cloud.eu/ [Accessed 22 April 2016].

individualisation is not achievable through legal drafting, (even in high worth contracts where negotiation of terms is possible) because of the complex milieu of information and its potential uses and the difficulties of coping with frequent changes to contract terms.

Tools of this sort are what Lessig terms as computing code having the effects of the law.[71] Subsequently, cyberspace demands a fresh understanding of how regulation functions. It requires a look outside the law sphere of the legal practitioner's traditional views; it requires vision beyond common law or norms. It requires a wider interpretation of 'regulation' and more importantly, the acknowledgement of a new noticeable regulator.

That regulator is the anonymity of Code. In the conventional sense, the law stands recognised through various edicts, statutes and other Coded rules. However, in cyberspace there is a different understanding of Code regulation and how software and hardware (i.e. cyberspace Code) makes cyberspace what it is today, as well as regulates cyberspace, or put plainly by Mitchell as cited by Lessig 'cyberspace's law',[72] and Reidenberg as cited by Lessig, had initially put it as 'Lex Informatica', or more precisely 'code is law'. This catchphrase concerns legal practitioners and theorists. These groups insist that there are differences between the regulatory effects produced by 'Code' and the regulatory effects created by law, notwithstanding the differences in the *'internal perspective*' which runs each type of regulation.

Potentially such 'Code' control even surpasses law in some cases. If such tools were available to deal with information ownership issues, all that the contract would need to state is that the Cloud service provider undertakes to comply with the information policies set by the customer using these tools. The tools would provide transparency and verification while the role of the contract clause would be limited to remediation activities.

Of course, accountability cannot solve all the problems of information use on its own. It assists customers to make a more fully conversant choice when entering into a cloud service agreement. Moreover, if information is used or disclosed in an inappropriate way, accountability provides the evidence which the customer needs to seek a legal remedy or more likely negotiate a solution with the cloud service provider.

12.7. Cloud Communal Customs

[71] LESSIG, L. (2006) *CODE version 2*. New York: Perseus Books. http://codev2.cc/ [Accessed 29 April 2016]. See also LESSIG, L. (2000) *Code is law, on liberty in cyberspace*. Harvard Magazine. http://harvardmagazine.com/ [Accessed 18 February 2016].
[72] *Ibid.*

The discussion on accountability explained how it might be used to enable the customer to control the use of information uploaded or produced in the cloud. Accountability requires the cloud service provider to agree to notify the client about these uses and the principle is uncontested, though putting it into effect is a technical challenge since all the cloud players agree that the customer owns the information.

Dealing with usages of derived information, uploaded by the cloud service provider from its metadata and via data mining is more difficult. The cloud service provider will effectively be the owner of the metadata information and so shall utilise the data as they deem fit for. As the data remains derived from information which customers own, those customers will feel protective about it and will want some element of control over its use. Accountability is not a solution on its own because in most cases derived information will be aggregate customer's information and metadata. Therefore, it will not always be possible to identify which individual elements of the derived information engage a particular client's interests. Even if it were possible to make this link, transparency about usages of the acquired information would disclose the cloud service provider's business partners and working methods, both of which are commercially confidential.

Consequently, there remains a requirement to develop a set of external rules and guidelines which regulate the usages of derived information by cloud service providers. This raises the question: 'where are these to originate?

In another place[73] it is clear that national laws are incapable of producing appropriate regulation for cyberspace activities. The legislation process is too slow and unwieldy for the fast-moving technologies, particularly in coping with the rapid change which is inevitable. Moreover, since the cloud technologies operate with little or no reference to regional geography, they can only be properly regulated by an internationally consistent set of rules. National law does not produce uniformity in law.

As Murry has shown, the process of achieving a regulatory settlement is an inescapable dialectic. He identifies four modes of regulation in cyberspace: Hierarchical control; Competition-based control; Community-based control and Design-based control. He also contends that regulatory settlements stand only over temporary symmetries, frequently disturbed by technology changes, the entry of powerful new and the 'flow-on' effects of

[73] REED, C. (2012) *Making laws for cyberspace*. Oxford: Oxford University Press. pp. 213–214.

changes to other, vaguely-connected regulatory settlements.[74] There is a continuous process of communication between lawmakers and individuals and also with the other modalities of regulation, norms, markets and code in terminology[75] through which each modifies the position of the other to produce changes in the regulatory settlement. This dialogue identifies the collective and competing norms of the community, which have to be reflected and balanced in the regulatory agreement if that settlement is to be accepted by members of the community.[76]

[74] MURRAY, A. (2007) *The regulation of cyberspace: Control in the online environment.* Abingdon: Routledge-Cavendish. See also MURRAY, A. (2008) *Symbiotic regulation*. The John Marshall Journal of Information Technology & Privacy Law. http://repository.jmls.edu/ [Accessed 29 April 2016].
[75] LESSIG, L. (2006) *CODE version 2.* New York: Perseus Books. http://codev2.cc/ [Accessed 29 April 2016].
[75] LESSIG, L. (2000) *Code is law, on liberty in cyberspace*. Harvard Magazine. http://harvardmagazine.com/ [Accessed 18 February 2016].
[76] REED, C. (2012) *Making laws for cyberspace*. Oxford: Oxford University Press. pp. 213–214.

13. Copyright in the Cloud

13.1. Introduction

As seen in the earlier discussions, the cloud has significantly altered the way in which information is gathered, processed, stored and distributed by companies, government agencies and individuals. Recently, Gartner identified the top ten technology trends of which three are directly associated with cloud technology namely Mesh App and Service Architecture, Adaptive Security Architecture and Advanced System Architecture.[1] Building on these and the associated risk questions of the cloud environment about information handling of content and personal information alerts to one of the key IP areas affected, namely copyright. New challenges are being experienced against existing copyright regulation content and traditional models of commercialising and protecting copyright works.

To interpret these problems and understand how to overcome each issue, an inspection of national cloud strategies, regulations and policy features would need to be performed on the most recent developments in copyright in the cloud. An assessment has to be made to ascertain if the existing rules deliver adequate legal protection for 'content and business information' or whether an improvement would be required for the cloud environment.

A review of the copyright regulation of South Africa and other major jurisdictions, such as the EU, UK and the USA together with the related copyright liability of the cloud users and cloud service providers respectively is needed. The 'safe harbour' law and the new EU-US Privacy Shield Framework[2] also need to be assessed.

13.2. Advantages of Cloud

Unlike traditional modes of information technology usage, cloud technology provides several overlapping advantages and flexibilities. In the first instance, computer resources are adaptable, can be shared by numerous remote users simultaneously and can be scaled either up or down depending on the demand of the resource. This arguably leads to significant operational cost reductions for the cloud service providers. In the second instance, cloud services are offered as a 'pay-as-you-go' model providing further economic efficiencies, which

[1] GARTNER Inc. (2015) *Gartner identifies the top 10 strategic technology trends for 2016*. Gartner. http://www.gartner.com/ [Accessed 6 February 2016].
[2] *EU-US Privacy Shield Framework* (2016) https://www.privacyshield.gov/ [Accessed 15 April 2016].

is similar to other forms of utility service offerings such as electricity supply. This also leads to cost reductions for service users. In the third instance, other services related to operational and administration expertise such as information technology management and maintenance can be outsourced to the cloud service providers,[3] leading to the creation of more new work opportunities. It can be seen in business models where cloud specialists are required for cloud product support, management and service consultants, through to network experts and engineers, to assist businesses to transfer and maintain new cloud environs. A study conducted by the International Data Corporation (IDC) found that public and private cloud services would produce close to fourteen (14) million new jobs across the globe and over half of these new jobs will be created by small to medium enterprise growth in the market.[4]

In addition to the IDC white paper, KPMG International conducted a study on the standing and influence of cloud adoption around the world and found cloud technology was accepted by an increasing number of businesses.[5] The study produced numbers indicating an increasing number of enterprises anticipating to migrate their business processes to the cloud over the next few years, receiving budget advantages through cloud implementation as well as spending less time building and defending the cloud business models and cases to senior management. The study survey found that 'the majority of organisations around the world have already begun to adopt some form of cloud or "as-a-service" technology within their enterprises.'[6] From the study it is evident that '… business is becoming more comfortable with the related benefits and accompanying risks that cloud services present.'[7]

Observers perceive that the benefits of cloud services, which include the 'ease of use' and cost savings initiatives, are simply too great to ignore and that cloud services have become a mainstream technology choice for many organisations. Corporate hesitation to migrate applications to the cloud has given way to cumulative approval of the cloud, specifically among business users.[8]

---

[3] GASSER, U., FARIS, R. and JONES, R.H. (2013) *Internet monitor 2013: Reflections on the digital world.* The Berkman Center for Internet and Society Research Publication Series. https://papers.ssrn.com/ [Accessed 19 April 2016].

[4] GANTZ, J.F., MINTON, S. and TONCHEVA, A. (2012) *Cloud computing's role in job creation*. IDC White Paper sponsored by Microsoft. https://news.microsoft.com/ [Accessed 16 April 2016].

[5] THE ADVISORY INSTITUTE. (2013) *The cloud takes shape: Global cloud survey|the implementation challenge*. KPMG. http://www.kpmg-institutes.com/ [Accessed 18 April 2016].

[6] *Ibid.*

[7] *Ibid.*

[8] SKYHIGH. (2015) *Cloud adoption and risk report Q2 2015.* SKYHIGH. https://uploads.skyhighnetworks.com/ [Accessed 7 May 2016].

13.3. Cloud Approach and Policy in Key Countries

The potential benefits of cloud technology have also been well-recognised by the RSA government, together with other governments around the world.[9] Major economies in the world have all developed their national IT policies or strategies and have in some instances been included in detailed regulation, to cultivate and guide the development of the emerging cloud industry and to balance the benefits of different stakeholders in the new cloud environment.[10]

As an example, some such policy and strategy moves by governments towards the cloud are detailed below. The RSA government's high-level strategy and policy are mapped out by the Department of Telecommunications and Postal Services. Their objectives are to formulate a so-called 'citizen, business and government focused e-strategy.' The initial focus of internet-based applications will be in areas such as agriculture, environment, villages, rural development, health, emergency services, safety and security with other e-service areas to follow.[11] The reference indicates the importance of the government's cloud policy and strategy which provides the basis for the executive branches and various government departments to adopt cloud services, particularly internal Private Government cloud and Government community cloud.

Other governments like the USA have a more comprehensive cloud strategy. The federal government's, 'Federal Cloud Computing Strategy' provides an approach that involves multiple levels of government.[12] A critical component of the strategy is the 'cloud first' policy. It sets up a 'top-down' requirement for all executive branches or agencies to transition heritage information technology resources to the cloud. The requirement had laid down an eighteen (18) month period for the conversion to be achieved.[13]

Similarly to that of the USA, the UK government introduced the Government Cloud Strategy, which announced a high-level vision of aims and an implementation strategy for the UK's 'G-

[9] JACKSON, K. (2013) *A framework for cloud computing adoption in South African Government*. Cloud Credential Council. http://www.cloudcredential.org/ [Accessed 7 May 2016].
[10] SCHOFIELD, A. and ABRAHAMS, L. (2015) *Research study on the use of cloud services in the South African Government. Joburg Centre for Software Engineering*. Wits University. https://www.jcse.org.za/ [Accessed 15 May 2016].
[11] Department of Communications. (2013). *South Africa Connect: Creating opportunities, ensuring inclusion, South Africa's broadband policy*. Department of Communications. http://www.gov.za/ [Accessed 11 May 2016].
[12] GASSER, U. and O'Brien, D. (2014) *Governments and cloud computing: Roles, approaches, and policy considerations*. Berkman Center for internet and Society Research Publication. https://dash.harvard.edu/ [Accessed 17 May 2016].
[13] *Ibid.*

Cloud'. By implementing a large scale upgrading effort, the UK government's objective is to solve the information technology issues such as uneconomical duplication of resources and systems, over-capacity, inadequate integration and central control.[14]

The EU has also announced their commitment to cloud services and set out a long-term plan for the establishment of a 'standard set of rules to develop a cohesive market structure among the European member states as well as for cloud service providers'.[15] In particular, it says that the EU policies will concentrate on 'enabling and facilitating faster adoption of cloud-based services across all sectors of the economy which can reduce information technology costs, and combined with new digital business practice, can boost productivity, growth and employment.'[16]

Although some major economies have developed their national strategies or policies to promote widespread implementation of cloud technology models and rapid growth of the cloud industry, a significant question remains as to whether these new technology choices are lawful under copyright law in the various countries.[17] It also appears that most of the governments have not yet set up comprehensive policies/regulatory guidelines for protecting copyright content in the new cloud environment.

13.4. Cloud User's Copyright Liabilities

From the onset, copyright challenges that cloud-service providers and cloud users mutually have to consider, in particular, are the potential risks to cloud service providers for copyright infringement activities conducted by their customers and whether the existing internet service providers' so-called 'safe harbour' legislation are sufficient to strike a healthy balance between different stakeholders.

As some scholars have pointed out, copyright laws are a significant contemplation for companies looking at the cloud as the companies have serious concerns about copyright and

[14] CABINET OFFICE. (2011) *Government ICT Strategy.* Cabinet Office London. https://www.gov.uk/ [Accessed 21 May 2016].
[15] GASSER, U. and O'Brien, D. (2014) *Governments and cloud computing: Roles, approaches, and policy considerations*. Berkman Center for internet and Society Research Publication. https://dash.harvard.edu/ [Accessed 17 May 2016].
[16] *European Commission. (2012) Unleashing the potential of cloud computing in Europe. Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and the Committee of Regions*. Eur-Lex. http://eur-lex.europa.eu/ [Accessed 11 May 2016].
[17] DONOVAN, K., NORTH, J. and FONSEKA, R. (2014) *Fair use exception to copyright infringement: The cloud is the limit*. Modaq. http://www.mondaq.com/australia/ [Accessed 10 April 2016].

confidentiality once uploading data into a cloud environment.[18] Indeed, a substantial amount of data or content stored in the cloud is subject to copyright protection, including films, texts, photographs, games, programs and software.

Generally, under copyright law in most countries, vests automatically when a work is created. However it should be noted that there are certain distinctions between the author of a work and the owner (holder) of the copyright in the work. Section 2(1) of the Copyright Act provides for some exceptions to the general rule that the first author is the owner.[19] These include works which have been commissioned or works produced in the course of employment. Copyright in these works vest in either the person who commissioned the works or the employer, as the case may be.

Copyright registration is unnecessary. A copyright owner has exclusive rights in using and exploiting their 'work',[20] including storing and distributing through the cloud. For any other users, reproduction or exploitation of such work is usually prohibited, even in the cloud. In other words, if a user exercises the exclusive rights of the copyright holder, infringement is likely to occur. The Electronic Communications and Transaction Act 25 of 2002 (referred to as ECTA 2002),[21] provides certain liability limitation. The limitation applies to cloud service providers, online service providers and information systems as 'a system for producing, transmitting, receiving, storing, displaying or otherwise processing data messages' [which system] includes the internet. The compound definition encompasses the essential functions and services required by users of the cloud and the internet. There are several areas covered involving service provider limitations, such as mere conduit limitation, system caching limitation, hosting limitation and linking limitations, as well as general provisions.

A. Cloud Terms of Use and Copyright Liability

Based on the nature of services previously discussed in Chapter 2, cloud services are divided into three broad categories, SaaS, PaaS and IaaS. Taking the limitation of liability conditions

[18] SCOTT, R.J. (2012) *Understanding the legal risks of cloud computing navigating the network security and data privacy issues associated with cloud services*. Thomas Reuters Aspatore. .http://www.scottandscottllp.com/ [Accessed 15 May 2015].
[19] *Copyright Act, 1978 (Act No. 98 of 1978 as amended up to Copyright Amendment Act 2002) 2002*. National Legislator. http://www.nlsa.ac.za/downloads/Copyright%20Act.pdf [Accessed 3 May 2015]
[20] KLOPPER, H.B. et al. (2011) *Law of Intellectual Property in South Africa*. Cape Town: LexisNexis. p. 145.
[21] *Electronic Communications and Transaction Act 25 of 2002 (SA) (ECTA)* Government of South Africa. Southern African Legal Information Institute. http://www.saflii.org/za/ [Accessed 26 March 2016].

of the ECTA (2002) into account, the services of SaaS and IaaS present more copyright problems than PaaS.[22] PaaS may be less of an issue as a developer or a user of PaaS is the creator of 'a work' and therefore automatically the copyright owner. There should be no copyright issue in this area since the created work is not used by an end-user, but by the developer.

When using SaaS, the cloud software is stored temporarily on the user's computer random access memory. If the terms of use for SaaS applications contain a license that authorises its users to make copies of the software, its users will not be at risk of copyright infringement. However, occasionally a cloud service provider may fail to comment as to reproduction rights in its terms of use.[23] In IBM's case, the terms of use for IBM SmartCloud for Social Business[24] does not clearly reference anything about whether its users can make temporary copies of cloud software.[25] The failure to mention reproduction rights in the terms then raise questions such as whether a SaaS user commits a copyright infringement and whether this may give the cloud service providers 'a right to demand the cessation of use and compensation.'[26]

The terms of use of an IaaS service provider are also an initial point to identify potential copyright infringement. The terms of use normally contain specific clauses as to whether the users may download software or content to their computers or devices and whether such content may be communal with others. For instance, on the downloading and use of IaaS software, Dropbox Terms of Service explicitly state:[27]

> Your Responsibilities:
>
> You are responsible for your conduct, Your Material, and you must comply with our 'Acceptable Use Policy'. Content in the Services may stand protected, by someone else's intellectual

[22] SOLOMECKE, C. (2013) *The legal aspects of cloud computing under Copyright law.* WBS Law. https://www.wbs-law.de/eng/ [Accessed 12 April 2016].
[23] STRANEX, M. (n.d.) *Judgements on Copyright 18, Case, Technical Information systems Pty Ltd v. Marconi Pty Ltd.* The Law Publisher CC. http://library.sun.ac.za/ [Accessed 2 March 2016]. Adaptation of a computer programme for use by an end-user by the removal of the licence agreement by the party given the right to copy and distribute the programme for end-users constitutes an adaptation of the programme.
[24] IBM. (2013) *IBM SaaS terms of service, smart cloud for business*. IBM. https://www-03.ibm.com/ [Accessed 9 April 2016].
[25] *Ibid.*
[26] SOLOMECKE, C. (2013) *The legal aspects of cloud computing under Copyright law*. WBS Law. https://www.wbs-law.de/eng/ [Accessed 12 April 2016]. See also termination conditions in Oracle agreement. ORACLE. (n.d.) *Oracle software as a service agreement V 121509*.Oracle. http://www.oracle.com/ [Accessed 14 April 2016].
[27] DROPBOX. (2014) *Dropbox terms of service posted*. Dropbox. https://www.dropbox.com/ [Accessed 12 April 2016].

property rights. Please do not copy, upload, download or share content unless you have the rights there to. We may assess your behaviour and content or compliance with these Terms and our 'Acceptable Use Policy'. Therefore, we have no obligation to do so. We are not responsible for the content people post and share via the Services.

Copyright.

We respect, the intellectual property rights of owners, and ask the same from you. We respond to notices of alleged copyright infringement if they comply with the law, and such notifications should be reported using our DMCA[28] Process. We reserve the right to delete or disable content alleged to be infringing and terminate accounts of repeat infringers.

If a user breaches the rules, they may receive a warning letter or even face Court action for copyright infringement.[29] Before storing copyright content to the cloud or accessing materials provided by a cloud service provider, it is important to carefully read the terms of use of cloud service providers.

13.5. Traditional Copyright Law and Statutory Exemption of Private Reproductions

While protecting the rights of copyright owners and creators, the copyright regulations in RSA provide for guaranteed measures of exception as with most countries' copyright laws. This means some limitations apply under various conditions. For example a user either uploading or downloading copyright works or materials while not having the consent of the copyright holder.[30]

The Copyright Act in South Africa provides for the 'fair dealing' principle, which allows for certain use of copyright protected works without infringement. Sections 12 to 19 of the Act provides for general exceptions on the utilisation of copyright protected works, as well as when a user may reproduce a copyrighted work, provided that such copied work be for personal and private purposes and limited in numbers and that the reproductions of work do not conflict with the normal exploitation of such works. Recently, the DTI proposed a new Copyright

[28] *The Digital Millennium Copyright Act 1998 (DCMA) (USA).* Copyright Gov. http://www.copyright.gov/ [Accessed 12 April 2016].

[29] SOLOMECKE, C. (2013) *The legal aspects of cloud computing under Copyright law*. WBS Law. https://www.wbs-law.de/eng/ [Accessed 12 April 2016]. See also WHITTAKER, Z. (2014) *Dropbox under fire for 'DMCA takedown' of personal folders, but fears are vastly overblown*. ZDnet. http://www.zdnet.com/ [Accessed 14 April 2016].

[30] *Ibid.*

Amendment Bill[31] with the aim of updating the Copyright Act to be more aligned with the new digital era. The proposed amendment bill included the introduction of the USA law principle of 'fair use' to South African copyright law. With proposed amendments to section 12 (1)(a) and (b) of the Act to incorporate the application of the 'fair use' principle.[32]. However the proposed new bill has been rejected in parliament on several issues of which the USA adopted 'fair use' principle was one of the primary items shot down by the parliamentary trade and industry portfolio committee. Citing that the 'fair use' principle should be left to the second phase of amendment proposals, as intellectual property rights are one of the most complex issues in global trade debates, especially with new disruptive technologies.[33] Furthermore, the committee requested that the DTI expanded on the 'fair dealing' principle to address the needs of academic, research and educational institutions as well as to take into account any international treaties which may impact on the proposed amendments.

There are also general copyright exceptions in the EU and particularly under German copyright Law. For example, an individual may reproduce a copyright work without the consent of the copyright holder, provided that it is the for personal and private purposes and in limited quantity and then upload the copyright works or content to the cloud, such as with the sharing of copyright protected MP3 music files with close friends and family. This is also referred to as the 'personal use' principle. The 'personal use' principle is closely related to the USA copyright law of 'fair use' principle. However, the USA 'fair use' policy coverage is slightly broader than the so-called 'personal use' policy.

Taking into account the RSA parliamentary pushback on the proposed new Copyright Amendment Bill, the adoption of the 'fair use' principle is unlikely to take place in the near future. However, the parliamentary committee has left the door open for the 'fair use' principle to be considered in the second phase of copyright amendments.[34] For now the copyright laws remain intact and part of the 'fair dealing' group of countries.

13.6. Exceptions under Digital Copyright Law

[31] Department of Trade and Industry. (2017) *Copyright Amendment Bill b3, 2017.* DOTI. http://www.gov.za/ [Accessed 22 July 2017].
[32] *Copyright Act, 1978 (Act No. 98 of 1978 as amended up to Copyright Amendment Act 2002) 2002.* National Legislator. http://www.nlsa.ac.za [Accessed 3 May 2015]
[33] ENSOR, L. (2017) *Revision plans for Copyright Bill raise MP's ire*, Business day, https://www.businesslive.co.za/ [Accessed 28 August 2017]
[34] *Ibid.*

Most countries have amended their copyright law in response to the rapid development of digital technology, particularly the internet. For instance, the USA enacted the Digital Millennium Copyright Act (DMCA) in 1998.[35] Some new amended provisions in copyright laws, such as internet service provider safe harbour provisions and the provisions on anti-circumvention of technical measures, may have a direct impact on the effects of implementing the existing copyright exemptions. For instance, most other countries, provide that the right to reproduce a private copy is excluded when the 'work' copied is protected by technological protection measures. The law in RSA have been expanded to include such technical measures. For example a work protected by ECTA[36] and digital rights management technologies to prevent a work from being copied.[37] Therefore, if a cloud service provider applied any anti-circumvention technology to prevent the copyrighted work from being transferred to other users, including close friends, any conduct circumventing such measures would then be treated as illegal.

Moreover, many cloud service providers may use technical measures to restrict user access to purchased content within a particular time frame. For instance, users can only watch a video for a certain number of days and after that access to that material is denied. If any users circumvent such a technical measure and view the video after their license has expired, the user will breach the copyright provisions.

13.7. Conclusion

Achieving effective dialogue is difficult as has already been seen in the case of Facebook. The regulatory settlement had been accomplished through adversarial confrontation, with Facebook pushing for the changes it wanted and its customers pushing back hard. It is clear that a stable solution still has to be accomplished.

Given this, an effectual consensus on the cloud community's norms for information use is likely to be achieved without establishing formal structures for dialogue. Those structures will need to be properly representative of all elements of the cloud community, which extends beyond customers and cloud service providers to include those individuals whose information remains processed in the cloud and national governments and other regulators who have a

[35] *The Digital Millennium Copyright Act 1998 (DCMA) (USA).* Copyright Gov. http://www.copyright.gov/ [Accessed 12 April 2016].
[36] *Electronic Communications and Transaction Act 25 of 2002 (SA) (ECTA)* Government of South Africa. Southern African Legal Information Institute. http://www.saflii.org/za/ [Accessed 26 March 2016].
[37] *Ibid.*

duty to protect citizens and ensure the proper functioning of commerce and society.[38] Building a global representative structure is one of the key challenges for the cloud in the coming years.

[38] *Ibid.*

14. Cloud Service Providers Copyright Liability

14.1. Introduction

For cloud service providers, potential liability for copyright infringement might include two aspects, primary direct responsibility and secondary indirect liability. Direct responsibility would entail that cloud service providers use their facilities to participate in the copyright infringement, such as uploading and distributing copyrighted content. They are then clearly breaching copyright law.[1] In considering secondary liability, whether contributory or vicarious, a core question is whether or not, or in what circumstance, a cloud service provider should be liable for the copyright infringement activities of their customers.[2]

In Chapter XI of ECTA deals with the limitation of liability of service providers and section 70 provides the description of a service provider, as 'any person providing information systems services'.[3] For instance, a question may arise on whether a cloud service provider breaches copyright through offering copyright-protected files for downloading, rather than uploading, or through simply providing a platform to facilitate the exchange of the copyrighted content. Clearly, secondary liability is the primary concern of most cloud service providers.

As mentioned above, internet service providers' safe harbour provisions in new digital copyright laws are mainly designed to address the internet service providers' secondary liability issues. It should, however, be noted that the anti-circumvention provisions impinge on the 'fair use' of copyright work.

14.2. What Is Safe Harbour Legislation?

The history of the internet service provider safe harbour is traced back to the World Intellectual Property Organization (WIPO) Copyright Treaty and Performances and Phonogram Treaty ,

[1] KOELMAN, K. and HUGENHOLTZ, B. (1999) *Online service provider liability for copyright infringement*. University of Amsterdam. http://dare.uva.nl/ [Accessed 27 March 2016].
[2] KLOPPER, H.B. et al. (2011) *Law of Intellectual Property in South Africa*. Cape Town: LexisNexis. p. 205.
[3] *Electronic Communications and Transaction Act 25 of 2002 (SA) (ECTA) Government of South Africa*. Southern African Legal Information Institute. http://www.saflii.org/za/ [Accessed 26 March 2016].

also known as the 'Internet Treaties' adopted in 1996.[4] The Copyright Treaty clearly required member countries to provide 'immunity' or 'safe harbour'. This was intended to limit internet service providers' liability for their customers' online infringement actions and further, provided that copyright liability ought not to be applicable to organisations or individuals who act as a pipeline for delivery, which provides regional facilities for enabling or making a communication.

> WIPO Copyright Treaty Article 8.
> Right of Communication to the Public
> Without prejudice to the provisions of Articles 11(1)(ii), 11*bis*(1)(i) and (ii), 11*ter*(1)(ii), 14(1)(ii) and 14*bis*(1) of the Berne Convention. Authors of literary and artistic works shall enjoy the exclusive right of authorising any communication to the public of their works, by wire or wireless means, including, the making available to the public of their works in such a way, that members of the public may access these works from a place and at a time individually chosen by them.[5]
>
> Concerning Article 8
> It is, understood that the mere provision of geographical facilities for enabling or the making of communication in itself does not amount to communication within the meaning of this Treaty or the Berne Convention. It is, further understood that nothing in Article 8 precludes a Contracting Party from applying Article 11*bis* (2).[6]

The safe harbour provision is particularly important for online service providers such as Google and Facebook, to avoid any potential legal liability for infringement of copyright by their customers. For instance, their customers may upload unauthorised copyright content through their website or network without notifying them.

14.3. The United States Free Trade Agreement and Safe Harbour Laws

Following the WIPO Internet Treaties, many countries have amended their copyright laws and included their service provider provisions.

For instance, Australia announced its service provider safe harbour legislation in 2000. The Copyright Amendment Act 2000 (Digital Agenda or DAA) included a service provider safe

---

[4] World Intellectual Property Organization. (n.d.) *WIPO Internet Treaties*. WIPO. http://www.wipo.int/ [Accessed 14 April 2016].
[5] *WIPO Copyright Treaty. (Adopted in Geneva on December 20, 1996).* WIPO Int. http://www.wipo.int/ [Accessed 17 January 2016].
[6] WIPO. (1996) *Agreed statements concerning the WIPO Copyright Treaty*. WIPI Int. http://www.wipo.int [Accessed 26 February 2016].

harbour provision for defining and limiting the liability of both 'direct' responsibility of their infringement and 'authorisation' liability, vicarious or contributory responsibility for their customer contravention, for copyright infringement on the internet. The landscape has changed as a result of the conclusion of the Free Trade Agreement (referred to as FTA) between Australia and the USA back in 2004.[7]

The FTA unambiguously obliges the Australian authorities to set up rules to ensure the replication and balance achieved in the USA's DMCA (1998). Moreover, assurances are required to ensure that the rules for liability of service providers for copyright infringement are adjacent to the rules reflected in the DMCA, in particular to service provider operations and copyright violations.[8] It also requires the Australian authorities to ensure the service providers comply with rights holders' requests if such a service provider would like to attain safeguards against the infringing actions of the users (the USA Notice and Takedown rule).

It further necessitates Australian authorities to make available 'procedures for material owners to summons the service providers for data around the service providers' users who may be suspected of utilising the service to store unauthorised material' (the USA Subpoena Procedures).[9] After the ratification of the FTA, in 2005, Australia amended the Copyright Act 1968 and included limitation provisions aimed at transporter service providers. Numerous academics and commentators consider the USA-Style 'Safe Harbour' system as more beneficial to the copyright holder and exercises a greater duty on the service providers.[10] In fact, Australia is not the only country affected by the FTA. In almost all FTA agreements post-2000, in which the USA was a party, a particular provision exists requiring the FTA parties to introduce the USA's DMCA-style service providers' safe harbour regulation. As an example, the USA and Chile signed the USA-CHILE FTA (USCFTA) in June of 2003 and included a separate IPR chapter (Chapter 17).[11]

The USCFTA attempted to coerce the Chilean authorities to comply with the Chilean responsibilities regarding the TRIPS agreement, as well as to meet the requirements under

---

[7] *Free Trade Agreements Australia.* (2009) Office of the United States Trade Representative. https://ustr.gov/ [Accessed 12 October 2016].
[8] *Ibid.*
[9] TIAN, Y. (2009) *Rethinking intellectual property: The political economy of copyright*. London: Routledge-Cavendish.
[10] ALLENS. (2004) *Australia-United States Free Trade Agreement: impacts on IP, communications and technology*. ALLENS. http://www.allens.com.au/ [Accessed 27 September 2016].
[11] *Chapter Seventeen Intellectual Property Rights*. (2003) Office of the United States Trade Representative. https://ustr.gov/ [Accessed 29 September 2016].

the WIPO Internet Treaties, such as prohibiting 'consumers from tampering with anti-pirating codes placed on audio-visual and software products' and setting up, safe harbour for service providers' liabilities for online infringement acts conducted by their customers.

In the Asian and Pacific markets, Singapore became the first nation to ratify a free trade agreement with the USA. The two countries concluded the United States–Singapore Free Trade Agreement (USSFTA) in May of 2003. Like its counterpart, the USCFTA, the USSFTA also contained a particular IPR chapter (Chapter 16).[12] This chapter requested Singapore to harmonise its IP laws with those of the USA, and to import the USA's DCMA model to 'strengthen and modernise' its copyright protection in the digital age, including service provider safe harbour legislation.

14.4. Recent Case Law on Safe Harbour in the USA

Recent cases adjudicated in the USA have highlighted a reasonable outlook for online intermediaries, including cloud service providers. The condition is that the cloud service providers function responsibly and within the DMCA safe harbour guidelines and circumvent actions which would induce any infringement. The role of intermediary ought not to place emphasis on the liability aimed at copyright infringement.[13] In numerous cases in the USA, the Courts have granted online service providers safe harbour immunity. The following cases are examples. *Io Group, Inc. v. Veoh Networks, Inc.N.D. Cal,*[14] copyrighted videos section 512 of the DMCA. The Court qualified Veoh Networks for safe harbour protection in *UMG Recordings, Inc. v. Veoh Networks Inc.*[15] UMG Recordings sought copyright infringement against Veoh. After examination of the technical process, the Courts again found in Veoh Networks' favour. In *Viacom Int'l Inc. v. YouTube, Inc.*[16] Viacom sued YouTube for copyright infringement and the Court granted summary judgement to YouTube on all of the Viacom's

[12] *Free Trade Agreements Singapore* 2003, Office of the United States Trade Representative. https://ustr.gov/ [Accessed 29 September 2016].
[13] MELZER, M.A. (2011) *Copyright Enforcement in the Cloud*. Fordham Intellectual Property, Media and Entertainment Law Journal, 21 (2), 2011, Art. 9. VOLUME XXI, BOOK 2. http://ir.lawnet.fordham.edu/ [Accessed 27 September 2016].
[14] *Io Group, Inc. v. Veoh Networks, Inc.N.D. Cal., August 27, 2008, No. C06-03926 HRL*. JOLT Law Harvard. http://jolt.law.harvard.edu/ [Accessed 15 April 2016].
[15] *IP IN BRIEF. (2010) UMG Recordings, Inc. v. Veoh Networks Inc., 665 F. Supp. 2d 1099 (C.D. Cal.2009)*. IP in Brief. http://www.ipinbrief.com/ [Accessed 15 April 2016].
[16] *Viacom Int'l Inc. v. YouTube, Inc., 07 Civ. 2103 (S.D.N.Y. April 18, 2013).* JOLT Law Harvard. http://jolt.law.harvard.edu/ [Accessed 15 April 2016].

claims for direct and secondary infringement and found that they qualified for safe harbour provision 17 U.S.C.s. 512 (c).

14.5. Safe Harbour in South Africa

The RSA, by way of the USA 'Safe Harbour' regulations, the new EU-USA Privacy Shield Framework, and the WIPO Internet Treaties, have promulogated the electronic communications regulations[17] to include digital measures and limitation of liability provisions which are comparable to those of the USA safe harbour requirements. ECTA focuses on the limitation of liability for service providers by way of the provisions in Chapter XI section 70 to 79 of ECTA.[18] These provisions include, the recognition of a service provider by the regulator, together with conditions for eligibility as a service provider. Furthermore the provisions provide an extensive list of operational criteria outlining what, where and when a service provider may be either, liable or not liable for infringements for providing access to or for operating information systems facilities. The criteria also takes into account main services such as acting as a mere conduit, caching, hosting and information location data or tools. All the criteria are typical functions or services of a cloud service provider. A few exceptions in the provisions relate to take-down notifications and no obligation by the service provider to monitor the data which is either transmitted or stored in the system. [19]

The regulator observed the global importance of privacy and the protection of personal data, with the development of legislation by introducing the POPI Act.[20] Similarly the POPI Act, in Chapters 8 and 9, includes the same system of safe harbour regulations dealing with the various categories of personal information and the manner in which the data is handled or used, provided the data subject has consented to such procedures. The act also addresses the duties of the service providers for cross-border data flow of the personal data.

It could remain argued that the scope of safe harbour regulations is sufficiently broad to safeguard online intermediaries, as well as for the development of cloud services and the enhancement of business models. Moreover, if this form of interpretation was to be followed,

---

[17] *Electronic Communications and Transaction Act 25 of 2002 (SA) (ECTA).* Government of South Africa. Southern African Legal Information Institute. http://www.saflii.org/za/legis/consol_act/ecata2002427.pdf [Accessed 26 March 2016]

[18] *Ibid.*

[19] *Ibid.*

[20] *The Protection of Personal Information Act No. 4 of 2013 of South Africa, Policy, Law, Economics and Politics*. http://www.polity.org.za/ [Accessed 6 December 2015].

legislators may find that there is no urgency to amend or upgrade the safe harbour protection for online intermediaries.

14.6. Conclusion

Since many countries have introduced the USA-style ‘safe harbour’ legislation, the jurisdictional experiences of the USA courts in implementing ‘safe harbour’ law to cloud service providers are arguably very influential for other countries in dealing with similar matters. Some key questions the courts have to answer may include whether the service providers’ safe harbour or limitation of liability provisions can adapt to new cloud environments; whether the existing immunity is broad enough to cover all cloud services, as well as understanding the relationship between service provider safe harbour or limitation of liability protection and traditional copyright exception provisions, such as the ‘fair use’ or ‘fair dealing’ principles.

15. Copyright Gap

15.1. Introduction

Many cases and studies have shown that the legal certainty for the USA cloud providers cannot just be credited to its safe harbour law. It seems that the USA's 'safe harbour' law and the fair use principle, broad copyright exceptions, have worked together to strike a sound balance for different stakeholders in the new cloud environment. However, when importing the USA-style of safe harbour law, many countries have not imported the same broad style of exceptions of fair use. The exception differences may place cloud service providers in those countries in a position of legal uncertainty for copyright infringement.

15.2. Industry Concerns and the Gaps in Copyright Law

One example of a jurisdiction with significant legal uncertainty for cloud service providers is Australia. Many online intermediaries and cloud service providers are keen to have expanded safe harbour immunity for service providers. An illustration of this would be, search giant Google who in recent times made a submission to the Australian federal communications ministers about media regulation reforms,[1] recognising two critical areas for enhancement.[2]

The first crucial area deals with Google requesting an extension to the copyright safe harbour rules for intermediaries, for instance 'search engine' intermediaries and other forums of that nature. They are seeking more sound clarity and definition of the operations of online intermediaries such as themselves. In the second crucial area, Google was extremely vocal in support of a recommendation made by the Australian authorities to repeal complicated and technology detailed copyright exceptions and substitute them with a 'fair use' provision. Google mentioned that the introduction of a 'fair use' provision would ensure that Australian

[1] Australian Government. (2014) *Deregulation. The Australian Government is reducing the regulatory burden for business and the community*. Department of Communications. https://www.communications.gov.au/ [Accessed 21 September 2016].
[2] TIAN, G. (2014) *Don't sue us for search: Google's unnecessary safe harbour appeal*. University of Hertfordshire. http://www.herts.ac.uk/ [Accessed 15 February 2016].

copyright laws could keep astride with the digital world in a manner that continues to incentivise creation and protect Australian copyright owners.[3]

As with many other countries, due to the lack of a broad 'fair use' exception provision, the existing copyright law does have many potential problems. As Google observed, the present Australian Copyright Act comprises 'various, comprehensive requirements which are not suitable for a digital age.'[4] For instance, a primary internet function such as caching is apportioned within three separate places in the Act, with three different legal treatments. Moreover, simple web services such as search indexing and crawling have not been explicitly covered by a particular exception. Arguably this creates significant legal uncertainties for the cloud service provider to operate a cache or provide search indexing services in Australia.

The provision of a cloud service, such as that of Dropbox or online backup data service often consists of caching, indexing, data transfer and other technical functions that require moving or copying data. As such, both the cloud users and cloud service providers may be at risk of infringing copyright in the course of using and providing such services. For instance, a cloud user that stores personal files in the cloud may not benefit from the formatting shift exception provision because the data files are stored on remote servers, which the user does not own. Similarly, when a cloud service provider moves a customer's saved and stored data files from place to place or from server to server, making copies each time, he may be at the risk of infringing copyright as well.

The Australian Law Reform Commission (ALRC) examined these issues, to which they recommended the revoking of technology-specific copyright exception provisions and replacing them with a 'fair use' provision. This would ensure that Australian copyright laws could keep astride with the digital world in a manner that continues to incentivise creation and protect Australian copyright owners.[5]

15.3. The Fair Use Solution

[3] Australian Government. (2014) *Deregulation. The Australian Government is reducing the regulatory burden for business and the community*. Department of Communications. https://www.communications.gov.au/ [Accessed 21 September 2016].
[4] *Copyright Act 1968, Commonwealth Consolidated Acts*. http://www.austlii.edu.au/ [Accessed 22 September 2016].
[5] TIAN, G. (2014) *Don't sue us for search: Google's unnecessary safe harbour appeal.* University of Hertfordshire. http://www.herts.ac.uk/ [Accessed 15 February 2016].

The principle of 'fair use' or 'personal use principle' allows for the particular limited use of copyrighted works. What is viewed as 'fair use' and is 'fair use' a solution in the cloud environment?

'Fair use' in the copyright sphere is discussed as any reproduction or copying of a work protected by copyright with limitations and alteration purposes, for example, criticism, reviews and reporting on current events or emulating a copyrighted work.[6] Section 12 of the Copyright Amendment Bill[7] now included the aspects of 'fair use' similar to Section 107 of the US copyright law,[8] which contains a number of identified determinations of use, in which way a reproduction of a copyrighted work may be reflected as 'fair use'. For example, research works for private studies in its strict interpretation and not for any commercial value[9] as well as teaching and personal use. Such use can run without the permission from the copyright owner or holder. However, put differently, 'fair use' is a protection against an assertion of copyright infringement. Once a reproduction or utilisation qualifies as a 'fair use' copy or reproduction, it would not be considered as an infringement.

'Fair use' may then questionably be seen as a substantial justification for online customers and service providers as a defence against copyright infringement, especially in circumstances where the copyright holders are unable to establish a copyright infringement by online service clients in the first place. An example would be Facebook users. In cases such as the Facebook users, it would be highly unlikely that the copyright holder would be able to institute proceedings against the online service providers for contributory liability.[10]

15.4. 'Fair Use' and Why?

As many commentators observe, 'fair use' can encourage innovation and can be flexibly applied to changing technologies, like cloud services that store and move customer data

[6] KLOPPER, H.B. et al. (2011) *Law of Intellectual Property in South Africa*. Cape Town: LexisNexis. p. 213.
[7] Department of Trade and Industry. (2017) *Copyright Amendment Bill b3, 2017*. DOTI. http://www.gov.za/ [Accessed 22 July 2017].
[8] *Copyright Law of the United States and Related Laws Contained in Title 17 of the United States Code*. Copyright Gov. https://www.copyright.gov/ [Accessed 17 September 2016].
[9] PRIVATE STUDY. (n.d.) *Hawkes & Sons (London) Limited v. Paramount Film Service, Limited [1934] 1 Ch. 593 (C.A.)* Stated that 'private study' should be strictly construed.
[10] TIAN, G. (2014) *Don't sue us for search: Google's unnecessary safe harbour appeal.* University of Hertfordshire. http://www.herts.ac.uk/ [Accessed 15 February 2016].

regularly.[11] When the USA courts decide on the liabilities of online service providers, in addition to safe harbour legislation, they often refer to the 'fair use' provision as well, for instance as in the *Viacom Int'l Inc. v. YouTube* case previously mentioned. It therefore seems that the internet service providers' safe harbour legislation and 'fair use' exception work well together to deliver safeguard confidence for public cloud users and online intermediaries in the RSA as well as the USA.[12]

Over the past decades, the 'fair use' administration of the USA copyright law has proven that it is flexible towards the advancements in technologies such as cloud services and the internet and encouraging innovation.[13] As the Australian authorities had noted, "If 'fair use' occurred in Australia, the Copyright Act would not need to be modernised merely because consumers now want to store purchased copies of copyright materials in the cloud instead of on a hard drive."[14]

Moreover, a study of late has shown that 'the court's' willingness to accept that innovative cloud services can be captured by the 'fair use' principle would have a profound impact on the rapid growth of the cloud industry as a whole.

As an example, in the case of *Cartoon Network et al. v. Cablevision,*[15] the USA Court of Appeals accepted that a cloud-based digital video recording service fell within the 'fair use' principle. Furthermore, a study directed by the Harvard School of Business, using the *Cartoon Network et al. v. Cablevision* case decision, found that the decision led to 'additional incremental investment in the USA cloud computing companies that ranged from $728 million to approximately $1.3 billion, based on the two and a half years after the decision of the *Viacom Int'l Inc. v. YouTube* case.[16] By contrast, the study revealed that more restrictive rulings on cloud services in France and Germany during the same period resulted in a total

---

[11] *Cartoon Network et al. v. Cablevision et al. 536 F.3d 121 (2d Cir. 2008)*. Berkman Center for Internet & Society. http://cyber.law.harvard.edu/ [Accessed 15 February 2016]. The United States Court of appeal found it acceptable that a 'Remote Storage-Digital Video Recorder system (RS-DVR) fell within the 'fair use' principle of copyright, Such remote storage is a Cloud based system.

[12] MELZER, M.A. (2011) *Copyright Enforcement in the Cloud. Fordham Intellectual Property*, Media and Entertainment Law Journal, 21 (2), 2011, Art. 9, VOLUME XXI, BOOK 2. http://ir.lawnet.fordham.edu/ [Accessed 27 September 2016].

[13] DONOVAN, K., NORTH, J. and FONSEKA, R. (2014) *Fair use exception to copyright infringement: The cloud is the limit*. Modaq. http://www.mondaq.com/australia/ [Accessed 10 April 2016].

[14] *Ibid.*

[15] *Viacom Int'l Inc. v. YouTube, Inc., 07 Civ. 2103 (S.D.N.Y. April 18, 2013)*. JOLT Law Harvard. http://jolt.law.harvard.edu/ [Accessed 15 April 2016].

[16] BOREK, C. et al. (2013) *Lost in the clouds: The impact of copyright scope on investment in cloud computing ventures.* IDEI. http://idei.fr/ [Accessed 21 April 2016].

decrease in French and German cloud project capital investment of approximately $87 million, reflecting a loss of almost $270 million in traditional research and development investment for the two countries in the same period.[17]

The result provides further evidence that the introduction of a flexible copyright administration, such as through the introduction of the 'fair use' principle utilised in the USA, may create enormous economic benefits for countries like Australia and others. It would seem that ALRC's recommendation on the revocation of existing technology-specific exceptions and replacing them with copyright restrictions with broader rules, as those used in the USA's 'fair use' principle, would serve as the optimal long-term solution.

15.5. Conclusion

In addition to the earlier discussion and having viewed some of the history of the safe harbour regulation together with USA case law involving service provider infringements, a clearer image comes into view. This is especially true about the interpretation of safe harbour where the legislators may find that there is no urgency to amend or upgrade the safe harbour protection for online intermediaries. For jurisdictions outside the USA, the establishment of the 'fair use' exception alone, as recommended by the Australian authorities, may serve as the most flexible/feasible approach for providing legal certainty for cloud service providers and users.

As seen in Australia, many other countries only introduced the safe harbour law rather than the 'fair use' principle. Therefore the optimum long-term solution for Australia is arguably applicable to other nations as well. It is imperative to make service provider safe harbour law and 'fair use' exceptions work together to promote innovative cloud business models, to enhance the development of the content industry in conjunction with solid legal practices and strike a sound balance of different stakeholders in the cloud environment.

[17] DONOVAN, K., NORTH, J. and FONSEKA, R. (2014) *Fair use exception to copyright infringement: The cloud is the limit*. Modaq. http://www.mondaq.com/australia/ [Accessed 10 April 2016].

16. License Agreements and Distribution

16.1. Introduction

People today utilise the internet for various things. However, one of the principal uses of the internet is maintaining contact with friends and family through social media, as well as keeping abreast with the latest news and information. The people access shared files and information anytime from anywhere in the world. Businesses and organisations utilise the internet for an ever increasing variety of functions which include professional commercial applications and advanced technological platforms. Such services are exceedingly simple to start up and use and very frequently with minimal data entry requirements. Services of this nature would also accommodate the use of credit cards and associated information. A limited number of keyboard entries to commence with the service, ensures full access to the operations of the internet and other applications. It is understandable that the cloud environment is just as easily reached, which in turn offers multiple business solutions and facilities.[1] Linked to these activities, is a significant misperception as to the rights, responsibilities and legal implications of what appears to be an open, free and relaxed environment. Fundamentally these activities carry extensive consequences for the users, consequences that may come as a complete shock together with unforeseen implications on businesses and individual consumers.

An example of such misperception of the cloud arrives in the form of the broad public perception that everything available on the internet is possessed by the community as a whole and therefore can be liberally and limitlessly utilised. Understandably, this indulgence is flawed as there is the small detail of IPRs, which in this context and most other cases is predominantly copyright based as it is present in almost every aspect of data loaded on the internet or in the cloud, whether shared, posted or transmitted. Immediately when a user uploads data onto the internet, that upload is invariably subject to terms that define the access and use rights of other cloud users, as well as the ownership retained or relinquished by the uploading user of such data. These rights constitute an actual or constructive contract or license, provided it is granted to the service or platform provider and potentially other internet users as well. Although

[1] KNAPP, K. (2015) *Top considerations for choosing a cloud provider.* Search Cloud Computing. http://searchcloudcomputing.techtarget.com/ [Accessed 12 October 2016].

sometimes difficult to discern, the terms of this type of contract define rights of use to the data for particular purposes or within certain limitations.

Regardless of the cloud services involved, there are license rights that define the various parties' rights in and to data in the cloud environment as well as other essential rights and obligations, whether the cloud service client is a licensor or licensee or, as is frequently the case, both.

The following are typical scenarios reflecting licensing of the cloud services:

a) *Client owned data.* This is where the customer uploads and stores data using cloud storage, whether that data is a photo, a word document, a soundtrack, logo or other software, they do so with a 'use features' of rights, whether express or implied, to the storage service provider. This 'use features' extends, at a minimum, to the right to make such copies as may be required to enable the provider to perform the storage, processing, backup and retrieval functions for the servers providing the storage facility. Often these servers are situated in different locations or even different jurisdictions, which may also vary at times based on aggregate demand and the provider's platform and arrangements for data balancing. The 'use features' of these rights is called content licensing. Further, when a client engages a service provider in making available IaaS or PaaS, the client similarly licenses or sub-licenses in the case of third party software uploaded by the customer to the service provider system for integration.[2]

The exact contractual terms of a license 'use features' may be plainly communicated and agreed to by the parties, but often they are at least partly implied through the actions and conduct concerning services agreed to by the client at service initiation and the scope of the licenses may be broad. In fact, such terms may extend well beyond the immediate requirements of the services to be provided. For instance, a relatively common right included under these licenses is 'use features' to the provider itself, the right to use the client data for the benefit of the service provider itself, including for the further development of the facilities for all customers of that vendor.[3]

b) *Service provider owned/licensed software.* Whenever a client engages a cloud service, the cloud service provider must also make available a 'use features' license for the customer

[2] SILALASHI, J.M. (2011) *Drafting a cloud computing contract*. Academia. http://www.academia.edu/ [Accessed 12 March 2016].
[3] *Ibid.*

for at least the necessary rights to use the service provider's software interface and functionality or other components essential to the delivery and use of the relevant services.

Cloud clients, especially in the public cloud, may be unaware that they are provided with content licenses to the service provider's software at all, much less the actual nature, scope and duration of the licenses granted. Even though the clients may retain ultimate ownership of their data, there is a very real risk that they may have lost control over it.[4] Often equally important other rights or obligations are contained, or not contained, in the contract terms governing the use of the cloud service and these may also be unappreciated by the client.

An overview of the essential cloud license terms, the complexities of the cloud services contracting process and details of some of the key issues and challenges in cloud licensing practice will now be discussed.[5]

16.2. The Frequent Challenges of Determining Terms

Ideally, the conditions under which any cloud solution is delivered should be explicitly and comprehensively stated in a written, static, readily accessible and understandable agreement. Again ideally, these terms and conditions should be known and understood by both the client and the provider, which is often not the case.

The growth of the cloud services' delivery model has been rapid and has challenged consumers' ability and perhaps willingness to adequately assess and manage the legal implications and risks presented in contracting for and utilising cloud solutions. In fact, the sheer ease of initiation and use of cloud services belie the legal significance of the undertaking. From the initial set-up, from the contracting to the operational use of the services and through to termination agreements, cloud services present new but familiar variations on the risk and opportunity trade-offs presented in traditional technology service agreements. Specifically, virtually all the major issues long recognised as involved in IT outsourcing, appear in cloud services.[6]

Cloud solutions, by their very nature, are more susceptible, when compared to prior bespoke technology solutions, to the client proceeding with adoption and use without a clear

[4] Loss of control over data, see discussion Chapter 12.
[5] HUBERT GROUP. (2016) *Cloud computing and contracts.* Hubert Group. http://journal.iaccm.com/contracting-excellence-journal/cloud-computing-and-contracts [Accessed 3 September 2016].
[6] MARSH. (2012) *The cloud risk framework, informing decisions about moving to the cloud*. Marsh and McLennan. http://f.datasrvr.com/ [Accessed 8 August 2016].

understanding of the full contractual dimensions of the agreement undertaken. Additionally, this might be the result of 'commando-style' keyboard click through practices, where the client effectively just 'clicks acceptance' to online terms without even making an effort to review and understand the contract undertaken. Of course, there have always been those clients who do not read contracts, but with the proliferation of 'click-through' contracts over the internet, the practical ease of elective ignorance has never been greater and this has often contributed to reduced vigilance around contracting.[7] In fact, one of the biggest strengths of the cloud is its sheer ease of use and access and has no doubt contributed to this, sometimes reducing the contracting process to seemingly nothing more than navigating the internet.

The cloud service providers often prepare the terms and conditions of service delivery for cloud solutions and frequently only cover limited issues. Determining actual contract terms applicable to the services is more difficult where items are missing. In such cases, those missing contractual terms may be implied, where required under the agreement to make commercial sense. Terms may be implied in law, such as the rights of the provider or a third party under copyright or patent law or may be implied in fact where necessary to give efficacy to the cloud agreement. Terms may also be drawn from what is seen as the reasonable expectations of the parties, including as reflected in their actions or conduct. The result is that frequently with cloud solutions, especially public cloud solutions, any comprehensive understanding of terms only starts with those expressly required by the service provider in the 'accept-before-entering' gateway and therefore must be supplemented with implied terms. Once established, implied terms can be enforced, but the burden of establishing implied terms can be difficult and raises risks for either or both of the parties.[8]

The frequent lack of certainty over precise terms may be acceptable and even appropriate for a cloud solution, subject to purely casual use. Think of a purely personal email service used for non-critical communications. However, to the extent that a cloud service begins to involve critical functions or sensitive data, it becomes increasingly important for the client to have a clear understanding of the terms and rights so that suitability for its use can be evaluated. Again, one of the core strengths of the cloud, the practical ease of initiation of use, has led to the situation where the adoption of cloud services has frequently outpaced careful evaluation and management of risk.

---

[7] BRADSHAW, S. et al. (2011) *The terms they are a –changin'. Watching cloud contracts take shape. The Center for Technology Innovation*. The Brookings Institution. https://www.brookings.edu/ [Accessed 12 August 2016].

[8] *Ibid.*

The need for the client to evaluate the suitability of available contract terms against their requirements is unambiguous in the case of cloud solutions, especially the public cloud, where there may be a slight opportunity or even no possibility for the client to have an input on the terms available. Often the choice facing the customer is acceptance of the service provider's standard terms or preceding the adoption of the cloud solution entirely. Such a stark set of alternatives is complicated further by both the speed and the ease of acceptance and approval. The result is that clients may unwittingly make bad trade-offs between cost savings and flexibility versus risk.

A further consideration in cloud contracting is that the party seeking to enforce a right or obligation affirmatively inevitably has some greater threshold burden than the opposing party, especially if the right or duty to be imposed is not expressly part of their agreement and must be established as an implied term. Again, cloud solutions present a dilemma: their ease of contracting, while a core strength, also presents significant oversight challenges. Opportunities promising quick-fix cost savings and flexibility may drive hasty decisions that have substantial business and risk consequences. Wanting or needing a particular right of assurance in a contract is far from establishing it.[9]

The 'take it' or 'leave it' understanding is a reality of many public cloud solution contracts and is another important consideration. Service providers are often resistant to any modifications to their contract terms. Some of this resistance may be the traditional opposition of any party in any transaction to changes in their established and most preferred conditions. However, many cloud solutions involve engineering practices or agreements that place very practical limits on the ability of the service provider to accommodate designated consumers' preferred contracts, much less give contractual assurance of doing so. Additionally, one of the core characteristics of the cloud is the ease of provisioning, including contracting, where service providers are often not set up to spend effort and resources on contracts or accommodating variations in terms or services for individual customers. Even where a vendor may be able and willing to make available a client's costs, such costs should pass on to the client and so adversely impact the financial benefits of the cloud solution. For the customer, achieving full value from a cloud solution inevitably demands a careful and responsible balancing of the cost savings and functionality benefits, with risk and strategy.[10]

[9] FOLEY. (n.d.) *Cloud computing: A practical framework for managing cloud computing risk*. Foley. https://www.foley.com/ [Accessed 10 March 2016].
[10] SILALASHI, J.M. (2011) *Drafting a cloud computing contract*. Academia. http://www.academia.edu/ [Accessed 12 March 2016].

16.3. Cloud Contract Terms

Going beyond the drawbacks and challenges often faced in cloud services contracting, due consideration should be given to the substantive terms of a real cloud services contract as well as what it should contain. In doing so, significant leverage may remain derived from the prior experience of technology delivery, namely traditional outsourcing. Outsourcing has been through a critical evolution in contracting over the past decade. The cloud merely represents the latest means of delivery of technology solutions, following on from initial modern outsourcing or offshoring.[11] Each of these delivery models involved stabilisation and growth phases intensely driven by contracting models and in each the contracting pressures were the same, developing a model to support a practice that gave sufficient assurances to clients to permit the adoption of the service.

Thus, evaluation of the present issues in cloud contracting for cloud solutions through contrasting cloud licenses, contract challenges and terms with traditional outsourcing contract problems and conditions can be performed. Such an exercise provides a means to critically analyse relevant client protection provisions, many of which remained developed through outsourcing contracts. The practical challenge is how to combine this contracting experience and learning from outsourcing with the flexibility and standardisation essential to cloud computing solutions.

The business environment in which the cloud operates presents many challenges, as business users face new and changing legislation and regulations (such as data protection) impacting on the provision and use of cloud database and computing services. Further, capability and competition within the cloud and outsourcing market are growing as cloud service contract agreements and terms are evolving.

To enhance the discussion on cloud contracts, particular attention is given to the following essential contractual issues: license 'use features', services commitments and services quality protections, client control rights, compliance obligations, data and security protections, IP protections, services continuity protections and end of term assistance.

Most of the discussion will compare and contrast representative approaches to the issues taken in the traditional outsourcing model as a primary point of reference. This traditional approach to services will be compared with the method frequently found in the pure public or utility cloud model, which represents the spectrum extreme in cloud services contracting, more

[11] CRANE, J. (2012) *The death of outsourcing and other IT management trends.* Forbes. http://www.forbes.com/ [Accessed 20 August 2016].

towards the real cloud services approach. Then the middle ground approach will be reflected and a discussion on the issues in the context of private or hybrid cloud solution models follow, where the cloud service provider may be in a better position to be responsive to particular or individual client requirements.[12]

In the discussion, the terms 'contract' and 'license' will be used interchangeably. While acknowledging that all licenses are indeed contracts, but not all contracts are licenses, the interchangeable use of the terms is a method of ease for the discussion and to illustrate the various considerations raised in association with the placement and use of data in the cloud. Nonetheless, because of the significant role that licensing concepts play in many cloud service solutions, the natural tendency is often to refer to the cloud service contract as a license. Hence the reference in the title to two practical aspects of licensing in the cloud.

16.4. Cloud License Utilisation Features

The first, and in many respects pivotal, set of contract issues associated with any cloud solution contract is the actual license 'use features'. This set of problems encompasses the subject of the permissible users and the use of the license. Most cloud service agreements involve at least two sets of license 'use features':

A cloud service provider 'use feature' granted to the client, and
A client 'user feature' accorded to the cloud service provider.

The discussion will focus primarily on the cloud service provider to client 'use features', which is the 'use feature' establishing the scope and nature of the cloud services. In the majority of cases, the client to cloud service provider 'use features' is mostly ancillary to the services and focus on addressing the use to which the client's data, including software, must be put by the cloud service provider in performing the cloud services.[13]

a) The subject of license. The first consideration in any right of use or license 'use feature' is the purpose of the 'use feature'. In cloud services or cloud computing, the topic matter or service may be software, as in the case of SaaS, or it may be a technology platform as in the case of PaaS. It may also be a combination of a software and technology platform as in the occasion of IaaS. In identifying the subject, it is important to consider how the

[12] Note: For the purpose of the discussion and as a point of reference, a representative private or hybrid cloud solution could be cloud provision of an enterprise application, as seen in business-focused SaaS offerings, Chapter 2.
[13] The client-to-cloud service provider grant is especially important and is filled with critical issues such as potential loss of data or control and regulatory compliance.

topic is defined. For instance, whether the use of software includes the use of its source code, which may be substantial if the client needs to make modifications or enhancements, including for purposes of interfacing or integrating with other software or processes. Similarly, it is important whether the software provided includes updates and new versions and whether the client has the discretion to move to such updates or new releases.

In addition, this is an area where the nature of cloud services or cloud computing often drives limits in the client's discretion regarding the implementation of software updates or new versions. Often the SaaS model is built as a 'one-size-fits-all' solution, where software updates are uniformly rolled out for all of the services, or with limited flexibility for clients to select different releases or version levels for their use. While this uniformity can be one of the core strengths of the cloud for software services, enabling clients to keep current with versions and releases without undertaking the upgrade implementation themselves, may be a limitation itself of the cloud solution, as clients are taken to updates, whether they are ready or not.

b) Permissible users. The next issue to be addressed in analysing a cloud solution is determining who has the right to use the solution. Client requirements, here are often driven by the customer's identity. For instance, whether they are an individual or a business enterprise, and the purpose or purposes for which the cloud solution is implemented as may be noted in casual personal use or business use. Other significant matters include the number of users permitted, (depending on the number of staff of the firm requiring access) and whether the client may allow third parties (such as their customers or contractors) to access the cloud services.[14]

c) Permissible use. License 'use features' frequently also address the allowable uses for which the cloud solution may be set by the user(s). User rights can be expressed as general or specific, and particular 'use features' may explicitly provide that only expressly permitted uses are allowed. Such an exclusivity provision makes defining the scope of the permissible 'use features' critical. Use limitations may be based on aspects of the solution such as access, use, execution, reproduction, display, performance, distribution, modification and creation of derivative works of the software/platform; or based on the activities of the client, such as use in operations of a defined business or geography. It is critical that the customer has a clear understanding of the scope of use for which they

[14] JAEGER, P., LIN, J. and GRIMES, M. (2008) *Cloud computing and information policy: Computing in a policy cloud?* Journal of Information Technology and Politics. http://www.tandfonline.com/ [Accessed 24 April 2016].

require the cloud solution and ensure that the user rights provided under the contract terms are sufficient to meet those requirements.[15]

The pricing agreements of a cloud solution may be closely parallel to, or adequately define the license 'use features' terms. For instance, changes may be based on the particular use of the solution, such as access to and use of different software modules, or numbers of users (named or concurrent) or size of cloud storage. Through such agreements, the client uses the service on a 'pay-as-you-go' system,[16] where no particular level or volume of the grade of service delivery is provided. However, the client may increase and decrease usage of the service as needed (and available).

d) Terms and termination. Contract provisions relating to the contract period and circumstances of termination vary dramatically among cloud solutions and drive crucial considerations for the client. These types of requirements broadly define the extent to which the provider is making a threshold commitment to deliver or provision the solution and correspondingly, the level of assurance the client may have that the solution will continue to be available for their use. The core issues are how long the solution is committed as accessible and if there is a dedicated period of provision and further under what circumstances may such provision nonetheless be terminated by the provider. A closely related issue is the right to partial termination, including suspension of the service for a limited time.

If there is no, or a limited committed term of provision of a cloud solution, there is a correspondingly limited reason for termination rights. In many cloud services and computing solutions, the committed contract period is short with little or no notice of termination required (by either party). If the client has a particular business need, longer committed period contracts and termination periods may be necessary to enable the customer to incorporate the solution into their operations prudently. When cloud service providers seek to offer cloud solutions targeting innovative and energetic business operations, it becomes increasingly important to provide specifically committed contract periods. With a move to fixed service provision determined terms, the issues around early termination become significant.[17]

---

[15] *Ibid.*

[16] HON, W.K. et al. (2012b) *Negotiating cloud contracts, looking at clouds from both sides now.* Stanford Technology Law Review. https://journals.law.stanford.edu/ [Accessed 10 January 2016].

[17] FOLEY. (n.d.) *Cloud computing: A practical framework for managing cloud computing risk*. Foley. https://www.foley.com/ [Accessed 10 March 2016].

The first problem with any committed condition in a cloud solution is the length of the active period, including any renewal rights and whether such renewal rights are automatic or subject to an election to renew the contract or not, by either or both parties. In service agreements, committed periods may range from short notice periods, typically thirty days, to multi-year terms. In evaluating the certainty of continued availability of a cloud solution, it is important for the client to consider the minimum duration that may, in fact, stand applicable to the contractual agreement.[18]

Where a cloud contract contains a committed period, the conditions or circumstances under which either party might terminate the arrangement before the expiration of its term, become relevant. Classically, service contracts provide that termination rights be available to a party in circumstances of a material breach by the other party, recognising that what constitutes a material breach may vary between the parties. Although some termination rights are parallel to both clients and service providers, the traditional service agreements often provide broader termination rights to the customer for breaches by service providers, than to the service provider for violations by the client. Reflecting on the most general scope of (performance) responsibilities of service providers (and thus a wider range of potential material breaches) in traditional outsourcing agreements, it is common that the scope of possible material default by the client giving rise to a termination right by the provider is limited to non-payment. Another traditional default circumstance giving rise to termination rights (typically also a termination right for the client) is multiple non-material breaches that constitute material default to frequency. A terminating party should have regard for the overall circumstances and its position would be strengthened if it could lead to a breakdown in relations and the prospect of continuing a substandard performance.[19] Additionally, rights of termination for convenience and circumstances of *force majeure* remain frequently included in licenses with fixed terms.[20]

16.5. Service Commitments

a) *Contract obligations and terms.* The issue concerns the extent to which the service provider retains the ability to make changes in the services unilaterally.

---

[18] *Ibid.*

[19] WALKER, S. and GREENE C. (2007) *'What constitutes a material breach'.* The Lawyer. [https://www.thelawyer.com/ [Accessed 12 August 2016].

[20] FOLEY. (n.d.) *Cloud computing: A practical framework for managing cloud computing risk.* Foley. https://www.foley.com/ [Accessed 10 March 2016].

In the traditional outsourcing contracting model, terms of service can only be modified by agreement. Provisions such as *force majeure* may provide relief from performance obligation in certain circumstances,[21] but the service provider generally has no unilateral rights to alter or modify their performance obligation during the term of the agreement.

The commitment to contract terms is not always present in the standard public cloud contract. Rather, service providers of pure public or utility cloud solutions, such as Facebook (cloud-based online social media) and Dropbox (cloud-based online file storage), have terms of service that often reserve for the service provider the ability to change those terms at any time at their discretion. Sometimes this right is expressly stated as a unilateral right to make changes and other times the right is more indirectly preserved through the incorporation of external documents (often linked) such as policies and procedures that can be varied by the provider from time to time. In some cases, the provider commits to provide some level of notice of changes, but in most cases, clients have to monitor the service provider's website for changes to the contract terms. Enforceability of such changes may be limited to a degree of reasonableness under applicable law, but the existence of such a unilateral service provider right in any cloud solution is a significant and defining consideration for the client, inevitably sowing uncertainty for them. Cloud solutions marketed for business adoption, such as a SaaS model for enterprise applications utilising a private or hybrid deployment model, tend to address this issue in a manner closer to traditional outsourcing. It provides the client with the assurance that contract terms can be changed only by agreement between the provider and the client.[22]

b) *The obligation to services.* This issue involves the extent to which the cloud service contract commits the service provider to deliver specified and expressly defined services or gives the service provider latitude in the services that may be performed.

The traditional outsourcing contract is created on the premise of a detailed; customised service definition often contained in all-encompassing, descriptive statements of work. These service descriptions may contain common elements between a service provider's clients, but they are frequently tailored to the customer's specific operational and practice

[21] Force majeure in cloud services context typically covers power cuts, strikes, failure to telecom services, third-party failures, natural disasters and any other event beyond the control of the service provider. See also FOLEY. (n.d.) *Cloud computing: A practical framework for managing cloud computing risk.* Foley. https://www.foley.com/ [Accessed 10 March 2016].

[22] SILALASHI, J.M. (2011) *Drafting a cloud computing contr*act. Academia. http://www.academia.edu/ [Accessed 12 March 2016].

requirements and therefore the outsourcing contract and delivery models are entirely oriented towards this.

The standard public cloud solution, classically provides high-level, general definitions of standard services, that are common to all clients and that are often provided on an 'as is' system. Here the service provider makes no explicit commitment that the services will, in fact, conform to the high-level, general services definition. The middle-ground approach, frequently seen in SaaS private or hybrid cloud solutions, involves contracts that may contain relatively detailed service definitions in definitive statements of functionality or work, but not customised service definitions tailored to a client's specific operational or practice requirements. This cloud model takes a 'one-size-fits-all' approach to current standard facilities for the representative clients, to preserve that efficiency which marks cloud solutions.

c) *Minimum term obligation*. This issue involves the extent to which the cloud service contract commits the service provider and the client to maintain the contract for a particular period, subject to defined termination rights, such as in the case of uncured default by one of the parties.

On this issue, the outsourcing model has traditionally remained founded on a commitment period of years applicable for the service provider. Although, the regular term in outsourcing agreements has shortened over the past decade, outsourcing contracts routinely provide for an initial term of three to seven years. They normally include elective extension terms of one to two years exercisable by the client to terminate early (for convenience) with a notice period and the payment of pre-established termination charges. The standard utility cloud contract classically provides little or no minimum term, reflecting (as will be discussed below) the frequent absence of performance commitments generally by the cloud service provider. In such circumstances, the cloud service provider is not obligated to make the services available. The middle-ground private or hybrid cloud contract often carries a relatively short minimum term, but in some cases may require a notice period before termination by either party.[23]

16.6. Quality Protection of Services

[23] FOLEY. (n.d.) *Cloud computing: A practical framework for managing cloud computing risk.* Foley. https://www.foley.com/ [Accessed 10 March 2016].

a) *Testing and acceptance.* This issue involves the extent to which the cloud service contract makes provision for the client to test and accept the services (or other deliverables) as part of the initial performance or delivery.

The traditional outsourcing contract model often builds a level of user testing and acceptance into the main implementation of the services. Trial and approval are also commonly constructed into the project methodology around all deliverables following the initial deployment, including transformations of service delivery. These procedures are designed to afford assurance to the client that the services meet the client's pre-defined operational and practice requirements and, to some degree, pledge to the provider that the customer will accept (often a prerequisite to payment) if the conditions are achieved.

The standard utility cloud solution contract classically does not provide for testing and acceptance, either at service initiation or subsequent delivery level (such as software upgrades). In some cases, a trial period may be allowed to permit the client to make a determination of whether they want to proceed with the actual adoption and production use, but often this is adequately accommodated by allowing the customer to terminate the services whenever they decide the solution does not meet their operational or practice requirements.[24]

The middle-ground private or hybrid model contract often provides testing of the major transition milestones during initial implementation and subsequent deliverables during the term. These tend to be generic and aimed at permitting the client to make a 'go-no-go' decision rather than confronting a delivery commitment on the part of the service provider.

b) *The obligation to service levels*. Service levels and their related provisions constitute one of the key contractual devices in establishing, measuring and reporting service performance. This issue involves the extent to which the service provider provides contract commitments that the services will conform to certain pre-defined performance requirements.

Service levels typically play a crucial role in the traditional outsourcing contract model. Outsourcing agreements often provide detailed and client specific service levels which serve as both a contractual commitment of service performance (for instance, establishing service availability, response time, transaction rate, processing speed, accuracy and the

[24] *Ibid.*

like) and the basis of credits (penalties) for failed performance.[25] Typically, these provide the ability to the client to modify service levels and credits to address both problem areas and evolving areas of the customer's concern, together with detailed reporting of the service provider against the service level requirements. In many cases, certain pre-defined levels of service level failures may be the basis of termination rights, which may be exercisable by the client.[26] Recognising that in no event can service levels adequately address the full range of performance, outsourcing contracts classically also provide more general performance requirements, such as the commitment to perform the services with reasonable skill, care and diligence.

Standard utility cloud solution contracts classically do not include significant provider commitments to service levels and, where service levels may be included, they are often a component of the general service description which either does not provide for service level credits or establishes unrealistic hurdles to obtaining such service level credits. Understandably, for the standardised and low-cost solutions, the standard utility cloud service providers are reluctant to guarantee (with a penalty for non-compliance) the quality and reliability of duty. As providers seek to broaden the acceptability of public cloud solutions in business environments, many are reconsidering offering some service level commitments as a way to accommodate their client's needs and attract new business. Even in such cases, the service level provisions often function in a defensive manner by being structured so as to restrict the service provider's responsibility to limited credits which operate as exclusive remedies, or their equivalent, for failure to attain the defined service level.[27]

The middle-ground private or hybrid solution contracts more commonly contain service level provisions, although these service levels tend to be focused more on supplier technology rather than reflecting the particular client's needs associated with the solution. Nonetheless, these service levels may carry meaningful service credits for failure to attain

[25] JAEGER, P., LIN, J. and GRIMES, M. (2008) *Cloud computing and information policy: Computing in a policy cloud?* Journal of Information Technology and Politics. http://www.tandfonline.com/ [Accessed 24 April 2016].

[26] Such provisions are based on service levels entitling the client to terminate the service contract which may include such a right when: (i) the service performance level drops below a defined point in any measurement period; or (ii) a certain value of service credit becomes payable within a prescribed period (for example, in one year); or (iii) a service level is not met for a certain number of consecutive measurement periods.

[27] BRADSHAW, S., MILLARD, C. and WALDEN, I. (2011) *The terms they are a -changin'. Watching cloud contracts take shape. The Center for Technology Innovation*. The Brookings Institution. https://www.brookings.edu/ [Accessed 28 March 2016].

the service provider's defined service levels. In general, only those clients with high subscription and upfront payments of significant fees have the power to negotiate for service level commitment.[28] In larger cloud service projects, service providers and customers may agree on a substantial list of the key performance metrics to express the degree of performance with which both parties are comfortable. Cloud service projects on a smaller scale will typically cover far fewer performance metrics.[29] It is, therefore, important to select which performance metrics are most crucial in achieving the client's business needs and objectives and to select metrics that are measurable and auditable, with the metric standards, measurement mechanisms and reporting requirements documented clearly and concisely.

16.7. Control Rights of the Client

a) Rights to determine architecture. This issue involves the extent to which the cloud service contract gives the customers rights on the technical design that the service provider utilises in performance and delivery of the service.

The traditional outsourcing model contract classically gives the customer the right to approve the design used by the service provider. This approval may be part of the initial contractual agreement, with assurances provided to the client that changes will not be made in the technical design via modification control protections. The client typically has the right to dictate enhanced technological design, although implementation may involve additional services and carry new changes.

The standard utility cloud solution contract invariably gives the client no right to approve technical architecture. Similarly, the middle-ground private or hybrid cloud model also gives the customer no right to support the technological design. In fact, it is one of the core distinctions of the cloud (over traditional bespoke outsourcing) that it primarily offers clients 'one-size-fits-all' solutions.[30]

---

[28] For example: City of Los Angeles. (2009) *Professional Services Contract between the City of Los Angeles and Computer Science Corp. for the SaaS E-mail and Collaboration Solution.* SECS. https://sites.google.com/ [Accessed 24 February 2016].

[29] An example of some of the key service quality metrics such as: (i) availability metrics; (ii) outage duration metric; (iii) mean-time between failures metric; (iv) reliability rate metric; (v) network capacity metric; (vi) storage device capacity metric; (vii) server capacity metric; (viii) web application capacity metric. See also Mc KENDRICK, J. (2013) *16 key service quality metrics to boost cloud engagements*. ZDNET. http://www.zdnet.com/ [Accessed 22 August 2016].

[30] SILALASHI, J.M. (2011) *Drafting a cloud computing contract.* Academia. http://www.academia.edu/ [Accessed 12 March 2016].

b) Modification, or change control rights. This issue involves the extent to which the service contract provides consumer protection from modifications or changes made by the service provider in the services; modifications or changes which impact those services or the customer's use of them.

The traditional outsourcing contract model requires that any amendment or change in services, which has a direct or indirect impact on the services or the client's use of the services, must be contested by the customer. This client protection provides assurance that the services will not be altered in a way that results in additional costs for the client or diminishes required functionality.

The standard utility cloud contracting model, with solutions that are driven by a common, 'one-size-fits-all'[31] service, typically allows the provider to make changes in the services without notice to or consent by the client. The middle-ground private or hybrid cloud contract frequently requires that the service provider gives notice to the customer of changes and allows the client to terminate the contract if the changes have an adverse impact on the services or the client. The service provider has no obligation to obtain the customer's consent to the changes.

16.8. Obligations Towards Legal Compliance

a) Assistance in complying with laws. This issue involves the extent to which the services contract obligates the service provider to assist or accommodate the client in meeting the client's legal compliance requirements, particularly in the activities and operations of the customer involving the use of the services.

Compliance with laws is an essential element in the traditional outsourcing contract model. Typically provisions oblige the service provider to comply with all the laws applicable to the services and their delivery and performance and that they assist with the client's compliance related to the services. These provisions are based on the recognition that a customer cannot transfer their compliance responsibilities to a third party and therefore necessarily needs to build assurances promoting legal compliance.[32]

[31] STONEBRAKER, M. (n.d.) "One Size Fits All": An idea whose time has come and gone. Computer Science and Artificial Intelligence Laboratory. MIT. https://cs.brown.edu/~ugur/fits_all.pdf [Accessed 12 February 2016].
[32] FOLEY. (n.d.) Cloud computing: A practical framework for managing cloud computing risk. Foley. https://www.foley.com/ [Accessed 10 March 2016].

The standard public cloud solution's offering affords limited flexibility to adjust the services to a particular client's legal requirements. Some of this inflexibility arises from the frequent heavy reliance on third-party contractors in public clouds.[33] In reality, it may be almost impossible for the service provider to assist the client in complying with local laws given the cross-border nature of the cloud offering. Although service providers may endeavour to perform the services in compliance with applicable laws, the contract invariably will not include commitments respecting particular legal acquiescence. This is shared with the service provider's reserved ability to make unilateral changes in the services (often without notice). The result is that a client facing legal compliance considerations must continually monitor the services and their use to ensure valid compliance. In some cases, the customer's ability to accurately observe the services is not feasible within a cloud solution, rendering some solutions inappropriate for certain uses.

The middle-ground private cloud or hybrid cloud model often provides a certain level of flexibility to configure the service to meet diverse client compliance requirements. These more tailored solutions are also frequently designed and operated in a manner allowing the client more assurances on legal compliance.

b) Audit review rights. The issue involves the rights provided to the customer to inspect and assess the service provider and their provision of the services.

In the traditional outsourcing model contract, clients are typically provided with well-defined rights to undertake operational and financial audits of the service provider and the services (including third-party contractors).

The standard utility cloud solution contract commonly provides no audit rights for the client, particularly in respect to secondary contractors. In fact, the service provider in standard utility cloud solutions frequently does not even disclose whether secondary contractors have been used.

In this area, middle-ground and private or hybrid cloud solutions often provide some audit rights. Typically, however, these rights do not include any right of territorial access to the service provider's facilities for audit or review purposes.[34]

[33] CLARKE, G. (2011) 'Apple's iCloud runs on Microsoft and Amazon services: Who says Azure isn't cool and trendy now'. The Register. http://www.theregister.co.uk/ [Accessed 2 August 2016].
[34] FOLEY. (n.d.) Cloud computing: A practical framework for managing cloud computing risk. Foley. https://www.foley.com/ [Accessed 10 March 2016].

c) Liability. Contractually, one of the core compliance assurance mechanisms is the potential exposure to liability for failure to perform according to the terms.[35] Thus, one of the threshold issues in any services contract is the extent to which the service provider may be exposed to liability for non-performance of contractual obligations.

Industry practice for the traditional outsourcing model is for liability to be limited to direct damages and further restricted to a pre-defined (or calculable) limitation of compensation, subject to certain exclusions for breaches or defaults under the contract.[36] Typically indirect and punitive damages are expressly disclaimed, except in cases of significant misconduct, such as gross negligence, fraud or willful abandonment.

The standard public cloud solution provides extremely limited liability for breaches or failures of any type. It is common practice that the service providers' standard service contracts will exclude liability as much as possible. In some cases, the cloud service provider will assume that the functions will be executed (if at all) with equitable ability and care,[37] but will commonly not provide monetary compensation in the event the service provider fails to comply with the given undertaking. In such circumstances, the public cloud contract may state that the service provider will use commercial endeavours to rectify problems of non-performance. Often, this commitment is the client's 'sole and exclusive' remedy for non-performance.

The middle-ground private or hybrid cloud model often has a narrowly defined scope of potential damages: direct costs only, subject to a limited maximum usually determined either by reference to the contract price or changes or a fixed sum and subject to certain exclusions from such limitations. All losses that are special, indirect or consequential are most frequently excluded entirely under the contract. Additionally, to limit their potential

[35] CATTEDDU, D. and HOGBEN, G. (2009) *Cloud computing, benefits, risks and recommendations for information security. The European Network and Information Security Agency.* (ENISA). https://resilience.enisa.europa.eu/ [Accessed 22 August 2016]. See also *Basic guidelines for contracts and contract risk management*, Harvard University. http://rmas.fad.harvard.edu/ [Accessed 22 August 2016].

[36] DE SILVA, S. (2014) *5th Meeting of European Commission Expert Group on Cloud Computing Contracts Liability Discussion Paper*. EC Europa. http://ec.europa.eu/ [Accessed 23 August 2016].

[37] For example: We undertake that the Services will be performed with reasonable skill and care. This undertaking shall not apply to the extent of any non-conformance which is caused by your use of the Services contrary to our instructions or these Terms of Service, or any alternation or modification made to the Services or the software used in the provision of the Services by a third party who is not authorised by us. We do not warrant that use of the Services will be error-free, and you agree that it is not our obligation to maintain, support or update the Services (except where necessary to carry out our other obligations under these Terms of Service), HITCH Software Platform. (2016) *Provider terms of service*. Hitch HQ. https://www.hitchhq.com/ [Accessed 23 August 2016].

liability exposure, the service provider will seek to disclaim liabilities for certain events or incidents, including service outages and data loss, delays, delivery failures or other damage or loss resulting from the transfer of data over communication networks and facilities. It is important for the client to understand the details of the protection offered under the service contract and to evaluate in advance whether the risks are acceptable in the context of their intended use of the services before entering into the contract.

16.9. Security and Data Protection

a) Location of data. This issue concerns provisions restricting or identifying where the client's data, used in conjunction with the cloud service, may be stored or processed. The location of the client's data can have significant implications for both security and legal compliance.

In traditional outsourcing contracts, permissible locations for the service provider's storage and processing of the client's data are defined and approved. Changes to these sites (at least involving material changes, including any transfer to a different country) require the approval of the client or, at a minimum, compliance with the change control processes (which itself likely requires the customer's approval).

In the standard public cloud contracts, there are typically no restrictions on where the client's data may be processed or stored. In fact, in many cases, the technical infrastructure used by the service providers may itself even limit the service provider's ability to control, or know, the location of data processing and storage: for instance, where networks of third parties are utilised to provide storage and processing.

Private or hybrid cloud solutions are more likely to provide assurances about the location of data, frequently fixing data location by country. Nonetheless, even with such safeguards, broader consideration must be given to the localities from which the service provider may access the client's data, resulting in the potential for deemed exports or transfers as a result of access from a foreign jurisdiction.

b) Information security. Information security is a primary consideration in any service contract. Focusing on the extent of the security assurance that the client's data is provided or created by the service provider in creation with the services, that the data will be protected from access, use or alteration by unauthorised third parties. (See section 3.7 on risk assessment)

Outsourcing contracts classically contain detailed information security provisions, focused on the safety to meet the client's specific requirements. Additionally, the client under an outsourcing contract usually has the right to require changes in the service provider's security practices, subject to the possibility of the additional work constituting new services for which there may be other charges.[38]

In the case of standard public cloud solutions, information security provisions are typically included in the contract. These solutions, however, tend to be standardised offerings and based on the use of the service provider's standard controls, with little or no ability to make modifications to any specific requirements of the client.

Middle-ground private and hybrid cloud solutions tend to treat security as a service and may provide elective or optional arrangements from a pre-established suite of security offerings.

c) Return, disposal or destruction of client data. This issue involves the extent to which the service contract provides assurances that the service provider will return or destroy the client's data and the timing of that return or destruction.

With traditional outsourcing, the contract gives the client clear and direct commitments from the service provider that client data will be returned or destroyed at the client's option, not only at the termination of the agreement, but also when the data has no further use or requirement for the performance of the services. Similarly, outsourcing contracts classically commit the service provider to returning the client's data at any time upon the client's request.

Standard public cloud contracts classically contain little or no assurance that all of the client's data will be found and erased or returned. As with limitations on some service provider's control of the location of their clients' data, the technical structure of many standard public cloud solutions places boundaries on the service providers' ability to provide assurances about return or destruction.

Middle-ground private or hybrid cloud solutions classically provide that data will be returned or destroyed, although the alternative selected is sometimes at the determination of the service provider.

[38] FOLEY. (n.d.) *Cloud computing: A practical framework for managing cloud computing risk*. Foley. https://www.foley.com/ [Accessed 10 March 2016].

16.10. Intellectual Property Protection

a) IP rights of clients' data. The data in the cloud can be any data, in any form. Each and any data enjoys some level of IP protection (most frequently copyright in this context, but this does not necessarily exclude any of the other IPRs from the discussion, in particular, personal data protection in the cloud as a primary concern).

It is well established that copyright subsists in original works (including electronic data) unless: (i) it is *de minimus* and hence fails to meet the minimum threshold for copyright protection; (ii) it is copied from others; or (iii) the copyright has already lapsed. In some cases, data for instance a drug formula may also be protected as a trade secret or a potentially patentable subject matter. This issue involves the IP ownership of the data which clients may provide or produce through the utilisation of the services and the extent to which the service provider is allowed to use such data.[39]

The traditional outsourcing model stringently protects the client's ownership of their data and specifies clearly the service provider's right to access, store process, make necessary copies and use the client's data (and its associated IP rights) for the purpose of providing the service. Similarly, the outsourcing contract will detail ownership of any IP developed by the service provider (including jointly with the client) and will allocate these rights through ownership and license rights. Essentially, it is a content license provided by the client to the service provider and it is commonly seen that such license covers use by the service provider and their third-party contractors and strictly limits use for such purposes.

The standard utility cloud model provides that the client retains his ownership of data he provides and 'use features' of a use license to the service provider. The big players in the

[39] HON, W.K. et al. (2012b) *Negotiating cloud contracts, looking at clouds from both sides now*. Stanford Technology Law Review. https://journals.law.stanford.edu/ [Accessed 10 January 2016].

market, such as Hitch[40] and Apple (iCloud[41]), make it clear in their terms of service that, by utilising their services the clients 'use features', which is a worldwide, perpetual and royalty-free license allows the service provider to use the client's data. Some service providers specify that the license 'use features' is for the use of data for the purpose of providing, promoting or improving the services, but some are silent on the scope of such content license. More likely than not, the license is a permanent one which does not end upon termination or expiration of the service. Such broad licenses raise risks for IP owners putting data on a public cloud. These risks include the risk that trade secrets may lose the necessary element of confidence. As for patent rights, risks arise as the novelty required for registration of a patent may be compromised by placing patentable subject matter on a public cloud under such broad license. The maintenance of novelty may be lost when the data is accessible to a large number of people within an enterprise without proper access controls. It remains to be seen how courts will approach such a situation, leaving this a considerable business risk. Another issue is the more precarious position of data loss, loss of control of the client's IP. This may result in the absence of a clear commitment by the service provider to safeguard access to the data. Additionally, permanent and complete erasure or prompt return of data when such data is no longer used or of value

[40] For example: Your Material and Proprietary Rights You Give Us. You shall own all right, title and interest in and to your API, API documentation and any material, information or data you provide or otherwise transmit to us or to others using the Platform or the Services ("Your Material"). We claim no intellectual property rights in and to Your Material; however, we require, and you hereby grant us, a worldwide, non-exclusive, royalty-free license to store, use, reproduce, display and transmit Your Material to the extent necessary to enable your use of the Platform and the Services. This license shall remain in effect until and unless these Terms of Service are terminated by you or us. You shall have sole responsibility for the legality, reliability, integrity, accuracy and quality of Your Material. Hitch Software Platform. (2016) *Provider terms of service.* Hitch HQ. https://www.hitchhq.com/ [Accessed 23 August 2016].

[41] For example: License from You. Except for material we may license to you, Apple does not claim ownership of the materials and/or content you submit or make available on the Service. However, by submitting or posting such Content on areas of the Service that are accessible by the public or other users with whom you consent to share such Content, you grant Apple a worldwide, royalty-free, non-exclusive license to use, distribute, reproduce, modify, adapt, publish, translate, publicly perform and publicly display such Content on the Service solely for the purpose for which such Content was submitted or made available, without any compensation or obligation to you. You agree that any Content submitted or posted by you shall be your sole responsibility, shall not infringe or violate the rights of any other party or violate any laws, contribute to or encourage infringing or otherwise unlawful conduct, or otherwise be obscene, objectionable, or in poor taste. By submitting or posting such Content on areas of the Service that are accessible by the public or other users, you are representing that you are the owner of such material and/or have all necessary rights, licenses, and authorization to distribute it. Apple Inc. (n.d.) *iCloud terms and conditions*. Apple Legal. http://www.apple.com/ [Accessed 22 August 2016].

or needed for the services (as discussed further below in connection with the end of term assistance).

The middle-ground private or hybrid model typically provides that the client retains ownership of data (and its associated IP) provided or processed through the cloud services and 'use features' a content license to the service provider. It is particularly important for business clients with high-value IP,[42] business data and trade secrets to have an express provision in the contract covering IP ownership, the scope of the content license, termination right of the content license and return and removal of data upon conclusion. Unlike the standard public cloud model, such rights may be protected in middle-ground private or hybrid model contracts.

IP considerations also drive some other issues previously seen in cloud agreements. For instance, preservation of confidentiality and novelty critical to IP protection highlights the importance of contracts clearly defining access rights. Use of end-to-end encryption to prevent unauthorised access and preserve privacy and originality of the data can also be utilised to mitigate risk. Further, because IP protection is primarily territorial (local law determined), the location of cloud data storage or processing has a significant impact on the IP rights. If the service provider's servers storing client data are located in a country where the customer data are unprotected under local IP laws or where IP rights are difficult to enforce, risks will increase if the client's IP is stolen locally or misappropriated. Hence, the location of data storage by the service provider is a major risk factor for IP-rich clients, making countries with strong IP regimes preferred and assurances that the client's data will remain there significant.

b) Developed materials and ownership. This involves the extent to which the service contract provides that the client retains possession and ownership of the IPRs of the data (including metadata) and materials that may be developed through the provision of the services.

The traditional outsourcing model clearly defines and allocates the client's and the service provider's respective rights in the IP developed through the performance of the services. Once ownership is established and set in the developed materials, either restrictive license provisions may be provided for such IP or the contact's general provisions respecting licenses to the parties' IP may apply.

[42] HILLELSON, L. (n.d.) *Making the business case for the media industry transition to IP.* Broadcasting and Cable. https://www.cisco.com/ [Accessed 23 April 2016].

Standard public cloud solutions classically allow clients to retain ownership of their data, but frequently do not define ownership of data created (even derivative) or IP developed in the course of the provision of the services. Such arrangements raise risks of unauthorised use and potential loss of ownership and control.[43]

Typically the middle-ground private or hybrid cloud contract provides that the client retains possession and proprietorship of any data provided or processed or created through the cloud services. These provisions frequently also provide limited rights to ownership of customisations of the services (such as customised software interface), with license-back (to the service provider) rights.

c) Non-infringement warranty and indemnity. This issue involves the extent to which the cloud contract requires the service provider to warrant that the cloud services do not violate the IPRs of the third party and to guarantee the client against costs and damages associated with third party claims of such infringement. This issue encompasses the implied warranty and indemnity by the client to the service provider against claims by a third party that the data or other material provided by the client, or the use to which the client puts the cloud services, oversteps the third party's IPRs.

The traditional outsourcing contract contains a service provider's warranty of non-infringement and indemnities against third party claim(s) that the cloud services (at least when used as contemplated under the contract) infringe the third party's IPRs. Less frequently, the contract may provide for a warranty and indemnities from the client that data they provide (and make available for use by the service provider), or uses to which they put the services, infringe third party IPRs. Some significant ancillary issues associated with any indemnity arise from outsourcing. An example is the extent to which the protection is subjected to or excluded from some or all of the limitations of liability contained in the contract and the scope of remedies available to the indemnitee in the event of an actual or alleged infringement, as discussed further below. Indemnities are frequently the subject of meaningful negotiation in any outsourcing transaction.[44]

The public cloud solution regularly entirely omits warranties and indemnities by the service provider and broadly bends such issues within the general 'as is' condition under the

[43] FOLEY. (n.d.) *Cloud computing: A practical framework for managing cloud computing risk.* Foley. https://www.foley.com/ [Accessed 10 March 2016].
[44] BRADSHAW, S., MILLARD, C. and WALDEN, I. (2011) *The terms they are a –changin'. Watching cloud contracts take shape. The Center for Technology Innovation*. The Brookings Institution. https://www.brookings.edu/ [Accessed 28 March 2016].

services which are provided.[45] Nonetheless, it is more common that standard public cloud solutions include indemnities and even warranties from the client, particularly in respect of data or materials provided or used by the client in connection with the cloud services. These aspects come in addition to their appropriate infringement notice and take-down procedures imposed in compliance with the safe harbour provisions of the USA's DMCA 1998, Electronic Commerce Directive 2000/31/EC[46] or other similar legislations.

The middle-ground private or hybrid cloud often includes some level of provider infringement indemnification, but less frequently includes warranties of non-infringement. Typically this compensation is limited to transgression associated with the deployment of the cloud services, but it is often narrowly scoped and subject to far-reaching exceptions. As with the standard public cloud solutions, middle-ground private or hybrid cloud solutions frequently impose a greater level of client non-infringement warranties and indemnities, including an arrangement to the service provider's notice and take-down policy.

d) Remedies for infringement. The issue involves the scope and nature of the solutions provided should there be a claim of infringement against the client (or service provider in the case of a non-infringement warranty or indemnity by the client) arising from the provision or use of the cloud services. The remedies provided under such an indemnity are a critical component of the compensation itself, as they define the scope of potential liability and responsibility of the indemnitor.

The traditional outsourcing contract typically provides express protection remedies if the services infringe third party rights. These solutions consist of the obligation to indemnify for costs of defence and any judgement or settlement. In addition it is to either obtain any necessary rights in order to continue the provision and use of the services, or to replace or modify the services so that they do not infringe a party's rights, without a material decrease in functionality. Frequently, the actual choice of these remedies is the election of the service provider. With its primary focus on services, the outsourcing model typically does not allow the service provider the right to cease performance (withdraw the service).

---

[45] Anonymous. (2016) *Terms of service,* Dropbox. https://www.dropbox.com/ [Accessed 12 December 2016]. Section 'Services "AS IS".

[46] *The Digital Millennium Copyright Act of 1998. U.S. Copyright Office Summary.* Copyright Government. https://www.copyright.gov/ [Accessed 17 November 2015]. Also see *Directive 2000/31/EC 2000 Art. 3 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce').* Eur-Lex. http://eur-lex.europa.eu/ [Accessed 12 May 2016].

This situation leaves the provider obligated to either obtain the necessary rights or modify or replace the infringing portion of the services, at the risk of breaching the contract for its failure to do one or the other. A related issue of significance is whether such defined remedies are the exclusive remedies of the indemnitee for any infringement or if others are available, such as the ability to terminate the agreement or make a claim for other damages. A warranty of non-infringement may be its self-serve as the basis of the exercise of rights under the contract in the event it is breached, including a claim of material default that may give rise to a termination right.[47]

The standard utility cloud terms of service typically offer little or no committed remedy in case of infringement, which is consistent with the service provider's natural right to unilaterally terminate the provision of the services.[48]

The middle-ground private or hybrid cloud contract, more likely than not, includes some remedies in the case of infringement. These solutions typically include the modification or replacement alternatives found in the traditional outsourcing agreement. However, frequently there is also a right for the service provider to terminate the services if they determine neither of these options to be commercially viable. Usually with a refund to the client of amounts paid, sometimes reduced based upon use up to the time of termination.

16.11. Protection of Service Continuousness

a) Personnel continuity. This issue involves the extent to which the service contract gives the client assurances that the service provider will seek to maintain key personnel to provide support for the services. Such continuity can be an essential element in assuring the client that the services will be appropriately performed.

The traditional outsourcing model provides for the identification of a group of service provider personnel or positions that the service provider is obliged to seek to maintain for service delivery to the client over a defined period and often offers protection on a service provider's normal personnel turnover.[49]

---

[47] BRADSHAW, S., MILLARD, C. and WALDEN, I. (2011) *The terms they are a –changin'. Watching cloud contracts take shape. The Center for Technology Innovation.* The Brookings Institution. https://www.brookings.edu/ [Accessed 28 March 2016].

[48] SILALASHI, J.M. (2011) *Drafting a cloud computing contract.* Academia. http://www.academia.edu/ [Accessed 12 March 2016].

[49] FOLEY. (n.d.) *Cloud computing: A practical framework for managing cloud computing risk*. Foley. https://www.foley.com/ [Accessed 10 March 2016].

The middle-ground private or hybrid model may provide some commitment to continuity for a limited number of key personnel for particularly crucial functions or activities.

b) Non-suspension/interruption. This issue involves the extent to which the contract expressly prohibits the service provider from interrupting or suspending the services.

The traditional outsourcing contract prohibits any suspension of services (subject to defined termination rights by the service provider) and requires detailed business continuity planning. Outsourcing contracts typically also state that under no circumstances can the service provider withhold the client's data, including specifically for the purpose of gaining an advantage in the event of a dispute.[50]

Consistent with the lack of overall commitment in respecting the provision of service, the standard public cloud terms of service frequently expressly acknowledge potential interruptions of services and make no commitment regarding business continuity.

The middle-ground private or hybrid cloud contract regularly provides special rights to limit users to protect the integrity of the services and may contain provisions regarding business continuity procedures and practices.

16.12. Term-end Protection

a) *Termination assistance.* Exit or termination agreements represent a critical set of considerations associated with any adoption of services, especially in business operations. It is important that, as part of a client's adoption of a cloud solution, they carefully evaluate and provide for a viable exit strategy, taking into account the support they can expect from the service provider and the demands they expect to face at that time. The provisions in service contracts concerning the parties' respective obligations when the service or contract is terminated are crucial. The client must evaluate such responsibilities in the light or their anticipated options at the time the services end. It is particularly important in the cloud context where the client may have transferred, shared or stored data in the cloud or developed a degree of reliance on the cloud services as part of their business operations. This issue involves the extent to which the contract commits the service provider to assist

[50] *Ibid.* See also CLOUD STANDARDS CUSTOMER COUNCIL. (2016). *Public cloud service agreements: What to expect and what to negotiate, Version 2.0.1.* CSCC. http://www.cloud-council.org/deliverables/CSCC-Public-Cloud-Service-Agreements-What-to-Expect-and-What-to-Negotiate.pdf [Accessed 22 September 2016].

the client at the termination of the services in association with the client's changeover to the facilities in-house or successor service provider.[51]

The traditional outsourcing contract contains detailed provisions addressing the obligations of the service provider to support the client in transitioning to successor provision at the termination of all or part of the services (including the extension of services to the extent that additional time is required for the successor agreements). These provisions are aimed at assuring the client has access to appropriate support to avoid the disruption of its operations. Such comprehensive requirements address most of the elements of service delivery from return of the client's data to the infrastructure (equipment, software and personnel) used in the service delivery.

The standard public cloud terms of service typically provide a right for the client to access its data in cases of termination, except in some cases where the termination is by the service provider for the customer's default. Consistent with the overall absence of service assurances in the standard public cloud model, contracts do not provide for further assistance to avoid disruption of the client's operations.

The middle-ground private or hybrid cloud model may provide the client with some ability to extend services and some reasonable assistance in the transition to a successor agreement.

b) *Data transmission format for data return.* One of the most critical components of an end of service changeover is the service provider's hand back, retention and deletion of client data. It is important that client data is handed back in a format that is reasonably accessible and compatible with the systems which they will be using or at least have access to for conversion purposes during the cloud services termination phase.[52]

c) *Data security for data return.* Data security must be considered at all stages of engaging cloud services, including the dissolution step. At the conclusion, clients should understand the level of information protection applied in the transmission of such data and be prepared for appropriate remedial action in the event of data leakage. Addressing these issues at the time of termination is probably already too late for practical arrangements. It

[51] FOLEY. (n.d.) *Cloud computing: A practical framework for managing cloud computing risk*. Foley. https://www.foley.com/ [Accessed 10 March 2016]. See also CLOUD STANDARDS CUSTOMER COUNCIL. (2016). *Public cloud service agreements: What to expect and what to negotiate, Version 2.0.1.* CSCC. http://www.cloud-council.org/deliverables/CSCC-Public-Cloud-Service-Agreements-What-to-Expect-and-What-to-Negotiate.pdf [Accessed 22 September 2016].
[52] *Ibid.*

is critical that the client assesses the full life-cycle risks associated with any cloud solution from the time of initial adoption.

d) *Data retention (by service providers).* Even where service providers have committed to deleting client data upon termination and in reality permanently, this process may involve an extended period, often up to three months before such data is in fact removed. Additionally, service providers may retain backup copies, logs and other information which may have been shared with other users (such as a photo on Facebook) for a longer period. However, it is worth noting that data privacy laws in many jurisdictions prohibit retention of personal data for long periods.[53]

e) *Data deletion and information removal*. The removal of information and data in the cloud is a much more complicated process than a mere click of a button. The existing standard terms offered by cloud service providers (particularly public cloud) commonly do not specify in any detail the arrangements for data deletion or information removal upon termination of the service contract. Even where the provider has offered to delete the client's data at the client's request, it is exceptionally difficult to achieve complete and permanent erasure.[54] Complete deletion of data is even more challenging in a cloud environment where multiple locations for data storage and data processing are involved.[55] The challenges associated with securely deleting data and information in the cloud are as yet another particular consideration that clients must carefully evaluate as part of their decision to adopt cloud services.

f) *Other termination support issues.* On termination cloud service providers will offer limited dissolution or termination support. Under existing market practice, enterprise solution clients should develop and through the lifecycle of the cloud services maintain a

[53] EURO CLOUD. (2015) *Major mistakes in data privacy – data protection in the cloud*. Euro Cloud. https://www.eurocloud.org/ [Accessed 10 August 2016]. Notes from paper. Right to deletion of data and obligation to notify of data breaches. The right to deletion of data is problematic as a result of organisational deficits and the supply chain. 63% of cloud providers maintain data indefinitely or have no provisions for data retention in their terms and conditions. Another 23% of cloud providers maintain the right in their terms and conditions to share data with another third party, making it even more difficult to ensure all copies are deleted, because of the numerous parties with whom a cloud provider shares data.

[54] Anonymous. (2016) *Terms of service, security*. Dropbox. https://www.dropbox.com/. [Accessed 12 December 2016]. Section 'File recovery and version history'. Dropbox saves a history of all deleted and previous versions of files, and allows you to restore them for up to 30 days. Extended version history is available as a Dropbox Plus subscription add-on. Dropbox Business users have 120 days to recover deleted files.

[55] *Ibid.*

transformation separation plan. That plan should be based on the assistance available from the service provider giving them adequate assurance that they will be able to successfully transition the services back in-house or to a successor provider.

16.13. Conclusion

It is important to recognise that characterisation of a particular cloud offering such as that of the public cloud versus private cloud or hybrid cloud is undoubtedly a significant over-simplification that does not tell the whole story when it comes to license or other contract rights. There is a considerable variability among cloud offerings within each category. The result is that the client's due diligence is essential. It is vital that the client reads the service descriptions for such important aspects of the service as processing locations, data backups, redundancy, encryption, security, transition process and options for client control. Even beyond explicit contractual assurances, the service provider's form of contract often provides significant insight into the way the service is structured and in cloud solutions, this structure often defines the ability of the service provider to meet clients' requirements.

Any service agreement carries certain risks for the parties that may be influenced or driven by practical realities in the technological structure of the solution and the operations of the parties. These risks can be significantly exacerbated for the client by the lack of certainty (or understanding) of the contract or license terms, leading to poor decision-making in connection with the adoption of cloud solutions. One of the greatest risks associated with the acceptance of any cloud solution by a client is a failure to understand the full range of their rights, responsibilities and requirements associated with the solution and its operations. In this sense, cloud computing and cloud services present certain nuanced differences from traditional services and licensing which are driven by technological structure and operation of cloud computing. Previous experience, based on prior service and licensing arrangements offers valuable signposts for charting responsible approaches to the adoption of any cloud solution.

17. Unified Global Distribution of Cloud

17.1. Introduction

Since the arrival of cloud systems and the associated services they have presented enormous challenges to IPRs, in particular, copyright holders. So far, many of the cloud-related discussions have focused on unauthorised content distribution through the cloud storerooms, the most notorious being Megaupload and Rapidshare. The arguments resemble the earlier debates on peer-to-peer file-sharing technology and internet intermediary liability. A few critics have raised queries concerning the ownership of IP in works stored in the cloud together with privacy-related matters. Notwithstanding the myriad of challenges cloud has posed to copyright holders, it cannot be overlooked that the unlimited prospects which innovative technology has delivered to rights holders enables them to distribute the copyrighted material globally.

The increase in the world propagation of cloud material and information has revitalised a long-standing debate about the precise reaction towards disruptive technology and copyright productions, repetitive and perhaps ill-advised exertions to safeguard obsolete business models[1].

Furthermore, adding to the complex problems of Cloud systems and service facilities, other queries have been raised which had previously not been broadly debated in law and technology circles, since the cloud systems and services concurrently enable multi-jurisdictional portals to copyrighted material. These are predictably running on a conflict path with IP law and the principles of territoriality. The cloud systems have also presented queries about the applicable legislation and whether such rules cater for the distribution of protected material or data.

17.2. Cloud Services and Territorial Rights

[1] MANIVAKA, J. et al. (2013) *Disruptive technologies: Advances that will transform life, business, and the global economy*. McKinsey. http://www.mckinsey.com/ [Accessed 7 August 2016].

More recently legal practitioners have been discussing the copyright challenges raised by the cloud. The ECJ recently issued the opinion of the *ITV Broadcasting Ltd v. TVCatchup Ltd*,[2] considering questions referred for a preliminary ruling by the High Court of Justice 'England and Wales'.[3] In the case, British television broadcaster ITV, Channel 4 and Channel 5, challenged the legality of a service enabling paying subscribers to view live streaming of unlicensed content provided through a '*free-to-air*' television broadcast. Although the case involved many complicated factors concerning the changing technology environment, the ECJ eventually held that[4]

> [The right of communication to the public] handles a retransmission of works included in a terrestrial television broadcast
>
> a) Where the transmission is, made by an organisation other than the original broadcaster,
> b) Using an internet access point provided to the member subscribers of that other organisation, who may obtain that transmission by logging on to its server,
> c) Even though, those member subscribers are within the area of reception of that terrestrial television transmission and may lawfully receive the transmission on television receivers.[5]

On the other side of the Atlantic, the USA Supreme Court has also handed down a decision in *American Broadcasting Companies v. Aereo, Inc*.,[6] which has raised similar questions concerning the right to public performance. The case concerned a major USA television broadcaster challenging the legality of service allowing paying subscribers to receive online streaming of unlicensed content provided through '*over-the-air*' television broadcasts. In the oral argument, several of the justices expressed concerns that the wide-ranging decision against Aereo could stifle the future development of cloud based computing and other yet to be developed communications technologies. It was Justice Beyer's (2014) who wrote a narrow

---

[2] *ITV Broadcasting Ltd and Others v. TV Catch Up Ltd. Reference for a preliminary ruling: High Court of Justice (England & Wales) (Chancery Division) - United Kingdom. Directive 2001/29/EC - Article 3(1) - Broadcasting by a third party over the internet of signals of commercial television broadcasters - 'Live streaming' - Communication to the public. Case C-607/11*. Curia Europa. http://curia.europa.eu/ [Accessed 7 August 2016].

[3] *Ibid.*

[4] *ITV Broadcasting Ltd and Others v. TV Catch Up Ltd*. Curia Europa. http://curia.europa.eu/. [Accessed 7 August 2016].

[5] *Ibid.*

[6] *American Broadcasting Cos., Inc., et al. v. Aereo, Inc., FKA Bamboom Labs, Inc. Certiorari to the United State Court of Appeals for the Second Circuit. No. 13–461. Argued April 22, 2014—Decided June 25, 2014*. Supreme Court of United States. https://www.supremecourt.gov/ [Accessed 7 August 2016].

majority decision, holding that Aereo made public performances within the meaning of the 1976 Copyright Act.[7] He declared: 'An entity that transmits a performance to individuals in their capacities as owners or possessors does not perform to the "public," whereas an entity like Aero that sends to significant numbers of paying member subscribers who lack any prior relationship to the works does so perform.'[8]

To be sure, the issues which the ECJ and the USA Supreme Court recently explored are highly important to copyright law reform at the domestic level, including change related to cloud or digital works. Nevertheless, the new technology has raised additional challenges when content is distributed via remote servers located outside the user's territorial location. For instance, the problems will occur when copyright content is uploaded to an external overseas server of such services as Amazon Cloud Drive, Dropbox, iCloud and even Megaupload, all of which will also arise when larger transnational company work compiles many smaller components 'works' authorised by individuals located in different territories of the globe.[9]

In either situation, cloud platforms are likely to create what Ginsberg (1997)[10] referred to as '[t]he disjunction between the territorial treatment of copyright claims and the ubiquity of cyberspace.'[11] The disjunction has raised two sets of territoriality questions.

17.3. Independence Rights

The first set of questions covers what is commonly described as the impartiality of 'The Right Principle'.[12] Under this principle, rights holders do not have a unified form of protection around the world. As an alternative they gain nation-based rights in countries like China and Brazil. What type of right they gain, how robust will the right be and whether the rights are to be efficiently enforced relies deeply on each of the various countries' IP protection systems. While the territoriality principle has been used to justify national discretion, such discretion is also

[7] *Ibid.*
[8] *Ibid.*
[9] GORDON, W.J. et al. (1994) *Virtual reality, appropriation, and property rights in art: A roundtable discussion*. Cardozo Arts and Entertainment Law Journal. http://heinonline.org/ [Accessed 4 April 2016].
[10] GINSBURG, J.C. (1997) *Copyright without borders? Choice of forum and choice of law for copyright infringement in cyberspace.* Cardozo Arts and Entertainment Law Journal. https://cyber.harvard.edu/ [Accessed 5 August 2016].
[11] *Ibid.*
[12] ABBOT, F.M. (2009) *Seizure of generic pharmaceuticals in transit based on allegations of patent infringement: A threat to international trade, development and public welfare. World Intellectual Property Organization Journal (WIPO), 1. p. 43. 2009*. SSRN. https://papers.ssrn.com/ [Accessed 5 April 2016].

strongly supported by the principle of state sovereignty and concerns about the international harmonisation policy.

Thus far, the continued national divergences in laws, policies and institutions have created a 'territorial untidiness' that significantly hinders the global distribution of copyright content.[13] The challenges are further aggravated by varying market dimensions and customer anticipations. Moreover, in addressing the territorial untidiness of countries, countries have worked hard to harmonise their laws.

Continental Europe, together with various other countries, has begun working together to tackle the 'cross-border' data flow problems by creating international IP accords. These accords are based on the initial IP agreements, from the Berne Convention[14] to the TRIPS Agreement[15] of the WTO and the Internet Treaties (1996)[16] of the WIPO.

The Berne Convention, the predominant international copyright treaty, expressly states in Article 5 (2)

> That, the gratification and application of such rights shall be independent of the presence of protection afforded in the country of origin of the works. Accordingly, apart from the requirements of this Convention, the degree of safeguard, in addition to the means of recompense afforded to the author to preserve his rights, shall be administered solely by the regulations of the Republic where protection is, demanded.[17]

Even though scholars suggested that the lack of registration, substantive examination or other administrative procedure may make the independence of right principle less relevant to copyright law than to trademark or patent law,[18] there is no denying that global exploitation rights do not yet exist under the current nation-based copyright laws. Instead, countries

---

[13] YU, P.K. (2012) *Region codes and the territorial mess*. Cardozo Arts & Entertainment Law Journal. https://papers.ssrn.com/ [Accessed 4 April 2016]. p. 187.
[14] *Berne Convention for the Protection of Literary and Artistic Works Paris 1971 (Act of July 24, 1971, as amended on September 28, 1979)*. World Intellectual Property Organization. http://www.wipo.int/ [Access 12 January 2015].
[15] *Agreement on Trade-related Aspects of Intellectual Property Rights (TRIPS) agreement 1995*, World Trade Organization. https://www.wto.org/ [Accessed 12 January 2015].
[16] World Intellectual Property Organization. (n.d.) *Internet Treaties,* WIPO. http://www.wipo.int/ [Accessed 12 January 2015].
[17] *Berne Convention for the Protection of Literary and Artistic Works Paris 1971 (Act of July 24, 1971, as amended on September 28, 1979)*. World Intellectual Property Organization. http://www.wipo.int/ [Access 12 January 2015]. Article 5(2).
[18] PATRY, W. (2000) *Choice of law and international copyright.* The American Journal of Comparative Law. https://litigation-essentials.lexisnexis.com/ [Accessed 15 January 2015].

introduced the national treatment concept and minimum international standards to foster certainty, predictability and harmony. While countrywide treatment prohibits discrimination against overseas creators, minimum international standards seek to offer authors an adequate level of protection.

17.4. Scope Protection and Jurisdiction

The second set of territoriality questions concerns the national reach of agreed jurisdictional geography and the extent of the relevant copyright law.[19] Both issues are usually resolved at the discretion of nation-based institutions such as the legislature or the judiciary. USA case law for instance indicates that federal statutes should not be interpreted as to apply to behaviour out of the country which is lacking Congressional intent to achieve the same outcome.[20] Consequently, courts are commonly unwilling to apply copyright laws for violations outside of the USA, unless there is a direct violation within the country.

The important case in the area is '*Subafilms, Ltd v. MGM-Pathe Communications Co.*'[21] Subafilms and Hearst Corporation sued Metro-Goldwyn-Meyer/United Artists (MGM/UA) for the unauthorised foreign dissemination of the Beatles' *Yellow Submarine,* construing, that the USA Copyright Act[22] confers rights no further than the national border. The USA Court of Appeals for the Ninth Circuit held that authorising inside the USA, acts that occur wholly overseas, did not infringe domestic copyright law.

[19] TRIMBLE, M. (2014) *Advancing national intellectual property policies in a transnational context*. University of Nevada. School of Law. https://papers.ssrn.com/ [Accessed 3 April 2016].
[20] *Equal Employment Opportunity Commission v. Arabian American Oil Company Nos. 89-1838, 89-1845 Argued Jan. 16, 1991, Decided March 26, 1991 499 U.S. 244 Certiorari to the United States Court of Appeals for the Fifth Circuit*. Supreme Justia. https://supreme.justia.com/ [Accessed 5 April 2016].
[21] *SUBAFILMS, LTD; The Hearst Corp., Plaintiffs-counter-defendants-Appellees, v. MGM-PATHE COMMUNICATIONS CO., FKA MGM/UA Communications Co. and as United Artists Corporation; MGM/UA Home Video, Inc.; Warner Home Video, Inc.; Warner Bros. Inc., Defendants-counter-claimants-Appellants. And SUBAFILMS, LTD; The Hearst Corp., Plaintiffs-Appellants, v. MGM-PATHE COMMUNICATIONS CO., FKA MGM/UA Communications Co. and as United Artists Corporation; MGM/UA Home Video, Inc.; Warner Home Video, Inc.; Warner Bros. Inc.; United Artists Corporation, Defendants-Appellees. Nos. 91-56248, 91-56379 and 91-56289. United States Court of Appeals, Ninth Circuit. Argued and Submitted February 24, 1994. Decided May 13, 1994*. H2O Harvard Law School. https://h2o.law.harvard.edu/ [Accessed 5 April 2016].
[22] *Circular 92. Copyright Law of the United States and Related Laws Contained in Title 17 of the United States Code, December 2016*. Copyright Government. https://www.copyright.gov/ [Accessed 22 December 2016]. Read together with T*he Digital Millennium Copyright Act of 1998. U.S. Copyright Office Summary*. Copyright Government. https://www.copyright.gov/ [Accessed 17 November 2015].

Post the Subafilms case, numerous courts have abstained from ruling in respect of the Ninth Circuit Courts judgement, maintaining that the Ninth Circuit Court had overlooked the fluctuating economic reality, technological environments as well as consumer anticipation. In its place they sought to justify the application of USA law by recognising a causal link concerning the violating act and the USA itself. In doing so they not only strengthen the protection of USA copyright works abroad, but also remove the territoriality-based loophole from the USA copyright law.

17.5. Conclusion

The distribution of copyright content via cloud platforms has raised many difficult but important questions. If the platform is located entirely within the country, these queries will concern whether existing copyright regulation meets the tasks posed by this new and disruptive technology. For instance, will the right of public performance cover the cloud-based dissemination of copyright content? Will the replication within the cloud for reasons of performance, availability, back-up and redundancy and parallel processing infringe on the right of reproduction?[23] Should the answer to either question be affirmative, will the potential infringement be exempted by an applicable limitation or exception, for instance an exception for 'temporary reproduction' regarding cloud-based or cloud-driven replication?

If the cloud platform involves remote servers located outside the country, such distribution will raise two additional sets of territoriality questions, namely what is the applicable law? and will such law be applied extraterritorially? As an illustration, consider the unauthorised distribution of USA copyright content via remote cloud servers in the RSA. Such distribution will implicate both the USA and RSA copyright laws. It may also involve the laws of other jurisdictions, especially if it has substantial adverse effects in third countries.

The first question focuses on what law(s) should apply, USA law or RSA law, the laws of other jurisdictions, or all or none of them. Because cloud platforms often involve storing multiple copies of protected work on servers in different countries, the multijurisdictional nature of acts involving these platforms makes it very likely that the laws of more than one jurisdiction will apply. The second set of questions concerns whether infringement has taken place under the applicable law if the infringing act occurred outside the national border. For instance, if the Court finds USA law applicable, it will still have to explore whether a deed committed in the RSA will constitute infringement under RSA law.

[23] MILLARD, C. (ed.) (2014) *Cloud computing law. Oxford: Oxford Scholarship Online*. Part IV Cloud Regulation and Governance.

18. Introduction of Territorial Restrictions and Justification

18.1. Introduction

The question of territoriality could be tackled head-on. Content providers have thus far avoided these complicated queries by introducing geographic constraints. By controlling the location in which their copyright content is being accessed or used, these providers transform the borderless digital environment back into territorially based distribution platforms. If past distribution strategies used by the music, movie and television industries provide any guide, similar restrictions will increasingly be positioned on authorised cloud-based distribution platforms.

To understand why content providers have resorted to territorial constraints, a look at four sets of validations that copyright holders, industry groups and scholars have advanced so far is required. Although cloud may not yet provide sufficient concrete examples to illustrate the validations entirely, it is possible to deduce from similar technology research on other forms of regional restrictions, such as DVD regional coding,[1] used commonly to protect movies, television programmes, computer software and online games. These technological limitations have been around since their introduction in the 1990s. To limit content access to only authorised geographic regions, for instance, the regional codification of DVDs, Region 1 protection is assigned for the USA, Region 2 protection assigned for the UK and the coding continues with other location number settings for the rest of the world.

While this form of regional codification provides a classic image of the utilisation of territorial restriction to safeguard copyrighted material, these constraints and limitations are found in numerous other consumer merchandise, as well as merchandise established before the digital era, for instance, electrical sockets and receptacle plugs used on appliances.

Present day regional codification has been broadly utilised to safeguard the film and television industry, although it also extends to include safeguards for online gaming, computer software, music and other similar industries.[2] Safeguards are also deployed in other controlled situations

[1] Anonymous. (n.d.) *Extra protection for digital media: Digital Millennium Copyright Act*, Region Coding. University of Florida. http://www.clas.ufl.edu/. [Accessed 5 April 2016].
[2] *Ibid.*

such as local mobile service providers via blocking codification, which has effectively been established in mobile devices, hand-phones, tablets and smartphones to provide regional restrictions. Technically, the mobile codification design is not the same as that of the DVD codification, nonetheless they are both performing similar control and safeguard functions.[3]

The codification systems are growing and being utilised more frequently, for instance, YouTube recently implemented territorial codification restrictions on accounts, limiting access to media in various regions. In so doing YouTube has removed what was seen as its main market strength of a 'region-free' podium for broadcasting and watching material. Furthermore, numerous content providers are establishing alternative pricing schemes for different regions. The Digital Rights Management (DRM) safeguards the content provider from consumer arbitrage. Together with the pricing scheme, content provider servers ensure that users that attempt to access such controlled services in the user's region, for example in the UK offered on a non-restricted website hosted in the USA, are automatically rerouted back to the UK restricted site.[4]

Similarly, to satisfy the users' desires as well as to guarantee the material constraints in a limited contract location, cloud service providers have started introducing local limitation cloud services or local district cloud services.[5] Such geographical confines are not limited to cloud services alone; they are also found in a variety of consumer merchandise across the globe.

18.2. Five Areas of Adjustment to Cloud

To assist with realising the cloud's full potential and to facilitate the global distribution of copyright content, five areas of potential modification can be identified. These can be considered when addressing the challenges posed by the territoriality principle of IP law and the continued national divergence in laws, policies and institutions, in particular the copyright field. While some of the identified areas of adjustment may be easier to introduce than others, the harder-to-introduce adjustments can also be more operative. Besides, many changes are introduced at the same time or *ad seriatim*. Therefore, it is more important to identify the

[3] VINELLI, R. (2009) *Bringing down the walls: How technology is being used to thwart parallel importers amid the international confusion concerning exhaustion of rights. Cardozo Journal of International and Comparative Law*. SSRN. https://papers.ssrn.com/ [Accessed 5 April 2016].
[4] *Ibid.*
[5] MILLARD, C. (ed.) (2014) *Cloud computing law.* Oxford: Oxford Scholarship Online. Part II Cloud Computing Transactions. See also, BRADSHAW, S. MILLARD, C. and WALDEN, I. (2010) *Contracts for clouds: Comparison and analysis of the terms and conditions of cloud computing services.* SSRN. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1662374 [Accessed 11 March 2016].

potential modifications than assessing their strengths and weaknesses and their ease of introduction and implementation.

18.2.1. Treaties

The first modifications relate to international accords. This set of changes is arguably the hardest to introduce, but is likely to be the most operative in the long term. Even though international treaties tend to trail behind technology development, leading to a cat-'n-mouse chase between the two,[6] introducing treaty-based adjustments to the existing international IP regime is important if nation-based rights are to collapse into a single global unitary right.

Although no such right presently exists in the global IP system, a close parallel is found in the community trade market (CTM) and community design systems in the EU. As a region-wide, unitary trademark, CTM came into existence following the adoption of the Council Regulation on the Community Trade Mark in December 1993[7] and the establishment of the Office for Harmonisation in the Internal Market. Instead of having national trademarks in the initial 12 and current 28 members of the EU, rights holders can enjoy the protection of a single unitary CTM throughout the EU.

As of 2013, the EU has implemented a unitary patent system[8] and unified patent Court known as the 'patent package.'

The EC's Copyright Division had previously been investigating the necessity for a European single unitary copyright title,[9] which has permitted the Commission to announce that they will be pushing forward with a transformation package of the EU copyright scheme. A primary focal point of the Commission's consultation was to increase the cross-border accessibility of material provided by content services within the single market. Together with appropriate assurances of satisfactory tiers of safeguards for rights holders,[10] the consultation has also

---

[6] MERCURIO, B. and JUNG NI, K. (ed.) (2014) *Science and technology in international economic law: Balancing competing interests*. Abingdon: Routledge. Section on trade agreement cats and the digital technology mouse.

[7] *Council Regulation (EC) No. 40/94 of 20 December 1993 on the Community trade mark*. Eur-Lex. http://eur-lex.europa.eu/ [Accessed 6 April 2016].

[8] *Unitary patent: Uniform protection across 26 EU countries*. EC Europa. https://ec.europa.eu/ [Accessed 12 February 2016].

[9] *EU copyright reform: Revisiting the principle of territoriality Briefing September 2015.* Euro Parliament. http://www.europarl.europa.eu/ [Accessed 6 April 2016].

[10] European Commission. (2013) *Public Consultation on the review of the EU copyright rules*. EC Europa. http://ec.europa.eu/internal_market/ [Accessed 8 April 2016].

provided further building blocks for the 'practical industry-based' standards investigated in the earlier settled 'Licences for Europe' stakeholder's discussions of 2013.[11]

Without a doubt, countries, including members of the EU, are still very unlikely to agree to an international accord that facilitates the development of a global, unitary copyright. The reasons are twofold. Firstly, copyright subsists in the original work upon its creation or, in some jurisdictions, fixation as in a work which is expressed in a tangible medium. Because no registration or examination is required, it is sometimes hard to know when copyright protection is secured. Even more complicated, Article 5(2) of the Berne Convention specifically references 'the gratification and application of these rights shall not be subject to any formality'.[12] Registration and other formalities affecting the enjoyment and exercise of copyright are therefore prohibited.

Secondly and more importantly, it took the EU some decades to establish both the CTM and then the unitary patent system. Given the considerable diversity within the international community it is highly unlikely that a global copyright system will emerge shortly. If it took the EU some decades to create just their CTM, it becomes hard to envisage how long it would take to get more than 180 WIPO members across the globe to establish a unitary copyright system.

It is thus highly unlikely that countries will agree to develop a global system. Nevertheless, the unlikelihood of developing such a system does not mean that countries could not agree on the establishment of a unitary right in unique situations, such as those involving internet and cloud platforms. As scholars have widely discussed over the last two decades, territorially based IPRs do not sit well with the internet, even though copyright holders, industry groups and policymakers continue to retrofit national boundaries back into the digital environment.[13] Even if there is a reluctance to introduce a unitary right, such as internet or cloud-based global exploitation right, treaties can be used at the international level to facilitate the exhaustion of rights in situations involving both the internet and the cloud. Such reduction prevents rights

[11] Licences for Europe. (2013) *Structured stakeholder dialogue*. EC Europa. https://ec.europa.eu/ [Accessed 8 April 2016].
[12] *Berne Convention for the Protection of Literary and Artistic Works Paris 1971 (Act of July 24, 1971, as amended on September 28, 1979)*. World Intellectual Property Organization. http://www.wipo.int/treaties/ [Accessed 12 January 2015]. Article 5(2).
[13] Department of Trade and Industry. (2017) *Copyright Amendment Bill b3, 2017*. DOTI. http://www.gov.za/ [Accessed 22 July 2017].

holders from retaining any rights of distribution or commercial exploitation after the copyrighted work has been marketed with their consent in any part of the globe.

So far, negotiations on the exhaustion of rights and, by extension, parallel importation, have been highly contentious in the WTO. As some scholars have recounted, during the negotiation of the TRIPS Agreement, countries had to 'agree or disagree'[14] over the exhaustion issue. While the EU communities and the USA favoured national or regional exhaustion, other nations like those in Asia, (Hong Kong, Singapore, New Zealand and Australia) preferred international exhaustion.[15] Even though Article 6 neither mandates nor forbids international exhaustion, it states that the mandatory WTO dispute settlement process will not be 'used to address the issue of depletion of intellectual property rights.'

Notwithstanding the compromise reached in Article 6 by developed and developing countries during the TRIPS negotiations, the exhaustion debate has been slowly changing, especially in light of digital technology advances, the increasingly globalised marketplace and the multi-jurisdictional nature of acts involving the internet and now in the cloud. While the EU has embraced regional exhaustion, the recent USA Court decision in *Kirtsaeng v. John Wiley & Sons, Inc.*[16] confirmed that the first sale principle in the USA copyright laws applies to copies of copyright works lawfully made within the USA and abroad.[17]

Indeed, after Kirstsaeng and earlier comparable cases such as *Quality King Distributors, Inc. v. L' Anza Research International, Inc*.[18], an increasing number of academics have suggested that the USA has in effect a global exhaustion governance in the copyright field. Many practitioners have also considered the national exhaustion approach as Patry (2011)[19] wrote:

> There should be a world-wide reduction of digital rights once a work has been licensed in one country. Countrywide or regional exhaustion is a relic of the analogue world. Societies should

[14] GINSBURG, J.C. and TREPPOZ, E. (2015) *International copyright law: U.S. and E.U. perspectives: Text and cases*. Cheltenham: Edward Elgar. p. 413, Sec IV.
[15] WATAL, J. (2011) *From Punta Del Este to Doha and Beyond: Lessons from the TRIPs negotiating processes, analysis of intellectual property issues*. World Intellectual Property Organization Journal (WIPO), 3 (1). http://www.wipo.int/ [Accessed 8 April 2016].
[16] *Kirtsaeng, DBA Bluechristne99 v. John Wiley and Sons, Inc. Certiorari to the United State Court of Appeals for the second Circuit*, *No. 11–697. Argued October 29, 2012—Decided March 19, 2013*. Supreme Court. https://www.supremecourt.gov/ [Accessed 11 April 2016].
[17] *Ibid.*
[18] MERGES, R.P., MENELL, P.S. and LEMLEY, M.A. (2012) *Intellectual Property in the New Technological Age. 6th ed*. New York: Aspen Casebook Series, Wolters Kluwer Law and Business. p. 587.
[19] PATRY, W. (2011) *How to fix copyright. New York*: Oxford University Press Inc. Chapter7.

> be required to maintain free, publicly accessible online databases of which works they claim the right to administer, as well as contact information for the rights holders sufficient to permit users to communicate with the rights holders directly. There should be legally required fixed time periods to distribute monies, especially for foreign rights holders. If foreign money is not distributed within the specified period, the overseas rights holder or the home society of the rights holder may bring suit and are entitled to attorney fees and penalties.[20]

Certainly, treaty-based adjustments are difficult to introduce. Nevertheless, the past few decades have not seen a higher momentum to push for treaty-based reforms at WIPO. Ever since the adoption of the WIPO Copyright Treaty[21] and the WIPO Performances and Phonograms Treaty in December 1996,[22] no new substantive international IP agreement has been established at WIPO. However, in June 2012, close to 50 WIPO members signed the Beijing Treaty on Audiovisual Performances, which offers protection to audio-visual performers under the existing international copyright system. Shortly after that WIPO adopted and added the 'Marrakesh treaty to facilitate access to published works for persons, who are blind, visually impaired, or otherwise print disabled.'[23]

The Marrakesh Treaty is interesting because it includes a provision that explicitly covers the 'cross-border exchange of accessible format copies.' Article 5(1) clearly states that

> Contracting Parties shall provide that if an accessible format copy is made under a limitation or exception or operation of law, that accessible format copy may be distributed or readily available by an authorised entity to a beneficiary person or an authorised entity in another Contracting Party.'[24]

Accordingly, even though Article 5(5) states that 'nothing in this Treaty shall be used to address the issue of exhaustion of rights','[25] the Marrakesh Treaty allows an accessible format copy made under the permitted conditions in one country to be distributed or made available under similar circumstances in another country.

---

[20] *Ibid.*
[21] *WIPO Copyright Treaty. (WCT) (Adopted in Geneva on December 20, 1996).* WIPO Int. http://www.wipo.int/ [Accessed 17 January 2016].
[22] *WIPO Performances and Phonograms Treaty (WPPT) (adopted in Geneva on December 20, 1996).* WIPO. http://www.wipo.int/ [Accessed 12 April 2016].
[23] WIPO. (2013) *Main Provisions and Benefits of the Marrakesh Treaty*. WIPO. http://www.wipo.int/ [Accessed 12 April 2016]. See also *'Marrakesh treaty to facilitate access to published works for persons who are blind, visually impaired or otherwise print disabled'*. http://www.wipo.int/ [Accessed 12 April 2016].
[24] Idem. Article 5(1).
[25] Idem. Article 5(5).

Moreover, since the 2013 General Assembly, the WIPO Director General has taken note of the significance of producing 'a unified global digital marketplace,'[26] which the Director General more recently clarified in an interview with the IP Watch.

> For as long as it is easier to get content illegally than it is to get it legally, there is an encouragement to privacy. We have to make the conditions to obtain it legally better than illegally, and that is the global digital marketplace.
>
> I present this example, if one of the HBO series comes out in a new season in, for instance, the US and is however not available for the new season in various territories. What do people do? Do the people wait around patiently until it is released? Or not, since they are hooked on the series! Therefore I think our objective should be towards a seamless global digital marketplace, and I think everyone has to agree on this.[27]

While the Director General's belief in the formation of a so-called 'new market' through a legislative process is not presently being promoted, he noted that there is a requirement to initiate a 'multi-stakeholder' exchange of ideas to enable the formation of the 'new market'. Such exchange of ideas still needs to ascertain whether or not the discussion will ignite the commencement of the development of a new international instrument or even a soft law recommendation from WIPO.

18.2.2. Choice of Law

The second set of adjustments, which is less difficult to introduce than the first, pertains to the development of choice-of-law principles that are particularly useful for cloud platforms and related services. Because the Berne Convention focuses on national treatment, it arguably does not provide any choice-of-law principles for determining copyright ownership and infringement. Instead, Courts have developed their doctrines to address these issues.

For instance, in *Itar-Tass Russian News Agency v. Russian Kurier, Inc.*[28] , a major USA copyright law case, some journalists from Russia pursued legal action against a New York

---

[26] GURRY, F. (2013) *Address by the Director General WIPO Assemblies – September 23 to October 2, 2013.* WIPO. http://www.wipo.int/ [Accessed 23 April 2016].
[27] WIPO. (2014) Director Gurry Speaks on Naming New Cabinet, Future of WIPO. IP watch. http://www.ip-watch.org/ [Accessed 21 April 2016].
[28] *Itar-Tass Russian News Agency et al., Plaintiff, v. Russian Kurier, INC. et al., Defendant. Al J. DANIEL, Jr. and Michael New city, Appellants, v. Itar-Tass Russian New Agency, et al. and Julian H. Lowenfeld and Moskovsky Komsomolets and AR Publishing Co. Inc., Appellees. Docket No. 97-7444. Decided: April 03, 1998*. United States Court of Appeals, Second Circuit. Case Law. http://caselaw.findlaw.com/ [Accessed 11 April 2016].

established Russian tabloid for allegedly violating the copyrighted articles of the writers, which were initially published in Russia. Post examination of the various interpretations of the national treatment, the USA Court of Appeal held that nationwide treatment in this case, is not the correct choice-of-law. As an alternative, the Court advanced federal common law to bridge the deficiency of the USA Copyright Act.[29]

The advancement made by the Court in this case concerned the extent of ownership of the copyright. The Court found that the law most applicable would be the law of the State which had the 'most significant relationship' between the copyrighted work and the persons involved, which in the present case was the law of Russia. Regarding the violation issue, the Court applied the law of the country in which the damage had taken place, which in the present case was the USA.

In the 1990s and early 2000s, the Hague Conference on Private International Law sought to draw up a new Convention on Jurisdiction and Foreign Judgements in Civil and Commercial Matters. Although the drafting exercise was ultimately unsuccessful due to a large extent to the emerging challenges posed by the internet,[30] the draft Convention paved the way for the development of two related projects, the American Law Institute Project on Principles on Jurisdiction and Recognition of Judgments in IP Matters and the Max Planck Group on Conflict of Laws in IP (CLIP) Principles.[31]

Similarly to the Hague Convention, both projects started with a focus on jurisdiction and enforcement. Unlike the Convention, however, both projects go beyond the original focus to cover choice-of-law issues. Although it is too early to tell how influential these two projects will eventually become, or whether later efforts to redraft the Hague Convention will be fruitful, it is not difficult to note the importance of developing coherent choice-of-law principles in the light of the territoriality challenges posed by the internet and cloud technology.

In addition to the two projects mentioned, as well as other similar projects conducted by the RSA Law Reform Commission and under the auspices of the International Law Association,[32] scholars have suggested new choice-of-law approaches that may be useful in the context of

---

[29] *Ibid.*

[30] HAINES, D. (2002) *The impact of the internet on the Judgements Project: Thoughts for the future*. Hague Conference on Private International Law. https://assets.hcch.net/ [Accessed 28 April 2016].

[31] Max Planck Group. (2011) *Principles on conflict of laws in intellectual property prepared by the European Max Planck Group on conflict of laws in intellectual property (CLIP)*. Munich Max Planck. http://www.cl-ip.eu/ [Accessed 18 April 2016].

[32] TRIMBLE, M. (2014) *Advancing national intellectual property policies in a transnational context*. University of Nevada. School of Law. https://papers.ssrn.com/ [Accessed 3 April 2016].

cloud platforms and related services. For instance, Dinwoodie (2000),[33] called for Courts to 'decide international copyright cases, not by choosing an applicable law, but by devising and applying an appropriate solution.'[34] He reasoned as follows;

> International copyright disputes implicate interests beyond those at stake in purely domestic copyright cases. Nationwide Courts should thus be permitted to resolve an issue in an international case using different applicable copyright rules that reflect not only a single national law but rather the values of all affected systems, be they domestic or international, that may have a prescriptive claim on the outcome. This approach to choice-of-law may unleash the generative power of common law adjudication as a means of developing international copyright norms. Moreover, it would accommodate the concerns of dynamic flexibility without compromising the values of regional diversity or pluralistic perspective in a way that public law-based copyright law making does not.[35]

Berman (2005) also advocated '[a] cosmopolitan approach to an international adjudication that allows Courts to participate in a dialogue with each other concerning the appropriate definition of community affiliation and the proper scope of perspective jurisdiction.'[36]

18.2.3. Business

The third set of adjustments involves private ordering. Of all the five areas discussed in this section, contract-based adjustments are the easiest to implement. They are also the most practical. Nevertheless, these changes vary considerably according to the parties involved and the power disparity between them. In the light of the drastic changes to technology environments and consumer expectations brought about by the internet and cloud technology, it is high time content providers rethink their territorially based distribution strategies.

Over the last few years, content providers invested substantial resources developing responses to copyright problems posed by online services and technology advances, in particular, cloud. As difficult as these problems may be, content providers unfortunately have not spent sufficient time reassessing transmission strategies for world distribution. For instance, content providers ought to have considered distribution models using a global stage,

---

[33] DINWOODIE, G. B. (2000) *A new copyright order: Why national courts should create global norms.* University of Pennsylvania Scholarship Law. http://scholarship.law.upenn.edu/ [Accessed 21 April 2016]. Rev 469, p. 476.
[34] *Ibid*.
[35] *Ibid.*
[36] BERMAN, P.S. (2005) *Towards a cosmopolitan vision of conflict of laws: Redefining governmental interests in a global era.* George Washington University Law School. http://scholarship.law.gwu.edu/ [Accessed 3 May 2016].

instead of utilising a limited random region selection strategy. Also, the content providers could have explored options giving copyright holders from various districts a share in the returns produced by the use of a worldwide distribution system, assisted by gathering social communities.[37]

Furthermore, there is the reluctance from distributors to making programmes accessible online even with the present high demand. As an example, the British Broadcasting Corporation's (BBC's), iPlayers include region-based codification restrictions.[38] This is understandable when taking into consideration that the limitation set by the British public broadcaster is based on the fact that such programmes may already be under license to other foreign broadcasters. This is in contrast to programmes such as '*Downton Abbey'*, which is transmitted by Public Broadcast Services in the USA, together with other programmes such as the *'Doctor Who'* series also distributed in the USA.

The BBC would also have to consider the issue that such programmes are required to produce sufficient advertising interest in the UK and other markets within the Commonwealth, such as Australia, Singapore and the RSA before they could become prevalent in the USA or receive worldwide distribution.

Moreover, the BBC may not have attained all the license or distribution rights of the material in respect of the programmes which might be transmitted in the USA or other regions of the world. The present situation will not change unless content providers alter the way in which they consider the distribution of the materials, such as adopting a global strategy as opposed to the limited region-based models. The reluctance to acquiring a global distribution model may be driven by two concerns, high costs and appropriate safeguards of the material as well as the time to achieve these goals.

The content providers must further consider the continuous changing way of life of the consumers. Together, with variations in the consumer behaviour and the growing call for borderless entertainment, the combined impact of these issues no longer makes any sound business rationale, in particular when the consumers are unable to acquire the materials they seek, notwithstanding the fact that the user is prepared to pay a reasonable price for the materials.[39] The more pressing issue is in the knowledge that the potential users'

[37] PATRY, W. (2011) *How to fix copyright. New York:* Oxford University Press, Inc. Chapter 7.
[38] BORAN, M. (2011) *Stream of online TV shows and movies starts flowing*. Irish Times. http://www.irishtimes.com/ [Accessed 23 April 2016].
[39] PATRY, W. (2011) *How to fix copyright*. New York: Oxford University, Press Inc. Chapter 7.

disappointment of not gaining access to the material sought, has driven the call for unlawfully disseminated materials.

A major part of the illegally dispersed materials is powered by the content providers themselves, who in part have 'shot themselves in the foot' by not having elected to distribute the materials to meet the consumer demands. The manager of the music group *'Pink Floyd'* coined the phrase:

> The flagrant spread of 'Piracy' in advanced countries is a reflection of the failure of the industry as a whole to develop an appropriate copyright response to the distribution and remuneration options made possible by the new technologies.[40]

Likewise, Patry (2011),[41] observed:

> Successful Internet business models stand based on satisfying consumer preferences, honed and targeted through information provided by users. Such business models offer more choices, more user satisfaction, since they stand based on users' preferences, and therefore ultimately lead to greater revenue.[42]

Indeed, the arrival and growing popularity of cloud platforms and related services have made it particularly urgent for content providers to reconsider their use of regional restrictions to ensure that consumers who are willing to pay for materials they seek can do so. As Patry (2011) goes further to say, 'the best way to prevent the sale of unauthorised goods is to flood the market with authorised products.'[43] The highly influential Hargreaves Review of IP and Growth also declared:

> Where enforcement and education alone have struggled so far to make an influence on levels of copyright breach, there has been more indication of accomplishment where inventive businesses have reacted to unlawful facilities by making accessible lower priced legal products in a form consumers want.'[44]

[40] KNOT, G. (2009) *Ripped: How the wired generation revolutionized music paperback*. New York: Simon and Schuster, Inc.
[41] PATRY, W. (2011) *How to fix copyright.* New York: Oxford University Press, Inc. Chapter 7.
[42] PATRY, W. (2009) *Moral panics and the copyright wars*. New York: Oxford University Press, Inc.
[43] PATRY, W. (2011) *How to fix copyright*. New York: Oxford University Press, Inc. Chapter 7.
[44] HARGREAVES, I. (2011) *Digital opportunity: A review of intellectual property and growth*. Gov. UK Publications. https://www.gov.uk/ [Accessed 5 May 2016].

18.2.4. Government

The fourth set of adjustments is similar to the third, except that it concerns content produced by governments or other public entities, for instance, works created by government employees or funded by taxpayers, such as content created by or for public broadcasters. While the type of territoriality challenges confronting this kind of material is similar to those confronting content owned by private content providers, the resistance towards global content distribution may be lower when compared with the private sector.

Assuredly, governments may be wary about the global distribution of content produced by their employees or funded by taxpayers. They may also believe that their focus and priority should be on promoting the interests of their nationals. Indeed, it is not uncommon to find existing laws on parliamentary or government works copyright. For instance, Chapter 1 section 5 of the Copyright Act 98 of 1978 provides 'Copyright qualified to the State and certain international organisations,'[45] whereas, many jurisdictions now have laws removing copyright protection from government works. For instance, section 105 of the USA Copyright Act[46] stipulates that 'copyright protection is unavailable for any works of the United States Government'. Works created by employees of the USA federal government are therefore ineligible for copyright protection. Even for jurisdictions with parliamentary or state copyright, a growing number of these parliaments or governments have introduced easy-to-use licensing to enable 'greater right of entry' to and utilisation of the protected content. This practice also extends to regional areas under Crown affiliation such as Commonwealth countries. In June 2010, the Australian Parliament announced its plan to port its central website across to Creative Commons License.[47] Australia presently only has two such licenses:

a) The version 3.0 CC Australia licences (the Australian 'ported licences'), which stood launched in June 2010;
b) The version 4.0 International licences (the unported licences), which stood initiated in November 2013. [48]

[45] *Copyright Act, 1978 (Act No. 98 of 1978 as amended up to Copyright Amendment Act 2002) 2002*. National Legislator. http://www.nlsa.ac.za/ [Accessed 23 October 2015]. Ch. 1, s 5.
[46] *Circular 92. Copyright Law of the United States and Related Laws Contained in Title 17 of the United States Code. December 2016*. Copyright Government. https://www.copyright.gov/ [Accessed 22 December 2016].
[47] COATES, J. (2010) *The Australian Parliament goes CC – with v3.0,* Creative Commons. http://creativecommons.org.au/ [Accessed 10 May 2016].
[48] CREATIVE COMMONS. (n.d.) *About the Licences*. Creative Commons. http://creativecommons.org.au/ [Accessed 10 May 2016].

Such licensing agreement has opened up the national website, which contains bills, committee and regulatory reports and other key public documents. The RSA parliament has also opened up its website[49] which is complementary to those items addressed by the Australian parliament.

Moreover, the global distribution of government-produced content could induce other governments to do the same. Reciprocity and international comity are key factors for determining whether copyright law should be extraterritorially applied. By facilitating the promotion of the country or the governed territory to foreign tourists, investors and workers, exceptional global distribution can also provide indirect benefits to taxpayers. As such benefits may not essentially be sufficient. The global distribution of government-produced content can create 'soft power,' which is widely discussed by observers who wrote:

> Soft power is harder, because many of its crucial resources are outside the control of governments, and their effects depend heavily on acceptance by the receiving audiences. Moreover, soft power resources often work indirectly by shaping the environment for policy, and sometimes take years to produce the desired outcomes.[50]

Soft power is initiated on the internet which has provided individuals with an unprecedented opportunity to obtain information about the way of life in the RSA and other countries; such distribution can benefit the international community by enabling nationals in other countries to make information judgments about possibilities of life. Such enablement is especially valuable to residents in countries having robust data control environments, where proxy servers are used to hide the user's identity and regional location.

Finally, the action that governments take in this area could encourage greater voluntary action on the part of the private sector. Hurley, former Director of the Harvard Information Infrastructure Project, reminds us that:

> Governments, by placing their hefty thumbs firmly on the side of the scale, which stands tipped toward more access to information would re-energise the debate and send a strong signal to other content providers.'[51]

---

[49] *Parliament of the Republic of South Africa* http://www.parliament.gov.za/ [Accessed 11 May 2016].
[50] NYE, J.S. (2004) *Soft power: The means to success in world politics*. Harvard Belfer Center. http://www.belfercenter.org/ [Accessed 12 May 2016]. Ch. 4 - Wielding Soft Power.
[51] HURLEY, D. (2003) *Pole Star: Human rights in the information society, rights and democracy.* https://www.brown.edu/ [Accessed 12 May 2016].

Therefore, by distributing content globally using cloud platforms, governments would help kick-start adjustments which private business may introduce.

18.2.5. Technology

The final set of modifications focuses on the technology required to protect against the intrusion on cultural rights and to ensure equitable global access to obtain copyright content lawfully. Up until now, internet users have deployed territorial location devices, including proxy servers, to utilise or view online material, which in other circumstances would not be accessible from their regional areas. If such devices are banned, technological adjustments will have to be introduced, with additional support from the applicable limitations or expectations in copyright law. To meet such technology requirements, Trimble proposed a 'digital passport[52] and stated the following:

> Legal cyber-travel, [that is the evasion of geolocation that prevents the user from viewing certain Internet content, from the user's territorial location]. Might stand conditioned upon the use of a digital passport that would identify not only the user's location or domicile but also the user's identity or account. Such a condition would permit cyber-travel but require that the user maintains accurate information about their identity. This solution would allow cyber-travel but defeat anonymization; users would be able to obscure their current location if, for instance, the 'digital passport' required information about the user's domicile or residence but not the user's current location.

By ensuring that consumers can enjoy their lawfully procured services when they are travelling or working abroad, Trimble's 'digital passport' and other similar technological adjustments will make the implicated services more attractive. The adjustments, therefore, will benefit not only consumers but also content providers. To be certain, content providers may have priced the service based on content availability in only the user's home country, for instance the user will have to pay a premium price for global access. In reality, many of these providers may simply have a tough time negotiating the licenses needed to ensure user access outside the place of procurement.

As previously noted, there has been a growing demand for 'cross-border' data flow, in particular, that of paid subscriber services which remained a primary concern for the EU

[52] TRIMBLE, M. (2012) *The future of cybertravel: Legal implications of the evasion of geolocation.* Las Vegas. University of Nevada. http://scholars.law.unlv.edu/ [Accessed 18 May 2016].

Commission's 'Licences for Europe' Stakeholders Dialogue back in 2013.[53] As the EU Commission observed in a document announcing pledges made by major content providers:

> Today, subscribers to audio-visual services online, for instance, consumers watching movies via an Internet service provider or web-store, are often denied access to services legally procured in their European Union member country when they cross national borders.[54]

While the stakeholder dialogue and the associated pledges focused on access to content and services within the EU, the lack of cross-border portability affects users throughout the globe. The need for such portability is highly understandable. As the EC professed in an earlier writing entitled 'A Digital Agenda for Europe':

> Consumers expect, rightly, that they can access content online at least as effectively as in the offline world. Europe lacks a united market in the content sector. For instance, to set-up a pan-European service, an online music store would have to negotiate with various rights management societies based in 28 countries. Consumers can buy CDs in every shop but are often unable to purchase music from online platforms across the EU because rights stand licensed on a national basis. Additionally, this contrasts with the relatively straightforward commercial atmosphere and dissemination networks in other areas, especially the US, and replicates other disjointed markets such as those in Asia.[55]

The lack of cross-border portability of content and services can also backfire on content providers. As Patry (2011)[56] observed:

> Many tens of millions of dollars are left on the table in Europe alone because of the inability to get pan-European licenses. Instead, licensees have to negotiate on a country-by-country basis with national collecting societies, music publishers, and record labels, to name only the top three groups, to say nothing of countries where there are no collecting societies. Authors lose because deals stand not completed, the public loses because there is a dearth of authorised, comprehensive services, and copyright law as a system loss for both these reasons.

To some extent, the need for cross-border portability reminds us of some earlier proposals concerning a right to hack or a right to circumvent.

---

[53] Licences for Europe. (2013) *Structured stakeholder dialogue.* EC Europa. https://ec.europa.eu/ [Accessed 8 April 2016].
[54] Licences for Europe. (2013) *Ten pledges to bring more content online*. EC Europa. http://ec.europa.eu [Accessed 8 April 2016].
[55] European Union. (2014) *The EU explained: Digital agenda for Europe*. Europa EU. https://europa.eu/european-union/ [Accessed 8 April 2016].
[56] PATRY, W. (2011) *How to fix copyright.* New York: Oxford University Press, Inc. Chapter 7.

For instance, USA Congress, through Congressman Boucher (2003) introduced the Digital Media Consumers Rights Act, which sought to re-establish the past balance that had been appreciated by the 'fair use' principle in copyright law.[57] Cohen (1998) argued the 'Licensees … ought to be given 'rights of electronic self-help' when necessary to preserve the balance that [the] Copyright Act is intended to establish.'[58] Furthermore, Shapiro (1999) underscored the need for allowing people to engage in what he described as 'Fair hacking' or 'Fair breach', in analogy to fair use.[59] As part of the Canadian copyright law reform, Geist (2005) further proposed to 'include a positive user right to circumvent a technological measure for lawful purposes'.[60]

Although these decade-old proposals sought to protect fair use of first sale rights or to restore the traditional balance in the copyright system, such plans were comparable to the technological modifications in this section. Similar to the identified amendments, these earlier proposals sought to ensure that consumer expectations were met. Moreover, if technical changes are required to protect against the intrusion on cultural rights, it would not be too far-fetched to argue that these alterations are required by pre-existing obligations in international human rights treaties that relate to the protection of cultural rights.[61]

18.3. Conclusion

Cloud technology has provided one of the most logical digital storage and software application platforms for the global distribution of copyright content. While it is understandable why content providers are eager to bring their current territorially based business models into cloud, it has been shown that this approach is ill-advised on two counts. Firstly, although justifications exist to introduce regional restrictions, these restrictions come with serious unintended consequences that harm both content providers and consumers. Secondly, and more importantly, geographic restrictions will hamper the future development of the cloud. Therefore, to ensure that cloud technology can be fruitfully developed, five adjustments are identified that could be presented to ease the sanction of worldwide dissemination of cloud-

[57] *H.R.1201 - Digital Media Consumers' Rights Act of 2005 109th Congress (2005-2006)*. Congress.Gov. https://www.congress.gov/ [Accessed May 5 2016].
[58] COHEN, J.E. (1998) *Copyright and the jurisprudence of self-help.* George Town University Law Center. http://scholarship.law.georgetown.edu/ [Accessed 23 February 2016]. pp. 52–53.
[59] SHAPIRO, A.L. (1999) *The control revolution: How the internet is putting individuals in charge and changing the world we know. 2nd ed.* New York: Public Affairs. p. 179.
[60] GEIST, M. (2005) *Anti-circumvention legislation and competition policy: Defining a Canadian way?* Irwin Law. https://www.irwinlaw.com/ [Accessed 23 February 2016]. pp. 248–249.
[61] YU, P.K. (2012) *Region codes and the territorial mess.* Cardozo Arts & Entertainment Law Journal. https://papers.ssrn.com/ [Accessed 4 April 2016]. p. 246.

based copyright materials. It remains to be seen if with this unified global circulation of content the potential of cloud could be fully realised, much to the benefit of content providers, technology developers and importantly consumers.

19. Conclusion

It is evident from the study and assessment of the available information that the cloud has truly developed into a global community instrument, which has brought about a direct requirement for the intensification of data security, personal data protection and IPRs. These are concerns for both individuals and cloud service providers, irrespective of the line of business, department of government or online assignations. More importantly, these concerns were initially raised and shared by the legal community, who in different areas face the challenge of providing adequate protection, as well as dealing with some other legal issues around the cloud and its operations. There is also the question of understanding what the proper law applicable to cloud technology is. The discussion above has highlighted the uniqueness of these challenges and may be summarised in three main considerations.

The first consideration are the rules and regulations related to the cloud. The discussion presented applicable legislation which has recently been enacted in the EU, USA and a smaller part in the RSA along with other countries around the world. The developing cloud industry is attracting the attention of legislators and government officials across the globe who now see themselves in the position of users, regulators, controllers, organisers and researchers.

As users, governments are adopting public, private and hybrid cloud deployments for operational use to take advantage of its financial and technical efficiency, innovative features and ability to facilitate collaborative environments. Furthermore, governments are also regulators of the cloud industry, by working through legislation, judicial and regulatory agencies and other departments to develop and implement policies to regulate and protect the individuals, companies and others within the cloud environment.

As a subset of the governments' legislative activities, the authorities also facilitate as a controller; administrations may participate actively in the standards development process that is demonstrated by the EU, which had set up the Working Party for the interaction and facilitation of data sharing between companies. Moreover, governments encouraged the building of groups to deal with cloud computing issues. As organisers, governments not only publicly endorse cloud technologies as newly adopted users, but also called on the public to accept the cloud as well. In the role of researchers, governments seek to understand the

technical problems and information society challenges that technology presents in research initiatives conducted directly by the government or by private organisations it funds.

The second consideration are the challenges posed by the operational environment of the cloud, while taking cognisance of the activities, positioned by governments, around regulation and policy improvements. There are still the areas of national and international boundaries and borders, which are challenged by the architectural environment of the cloud. A view of the risks associated with security, personal data protection and IPRs are topics which form part of the concern.

However, with the addition of territorial location, cross-border data flows and jurisdictional complexities, the discussion opens up in particular to the virtual operational characteristics of the cloud and whether the regulators have considered all the changing aspects of the cloud when developing policies and regulations. The USA initiated laws in the form of safe harbour protection rules and attempted to engage as many countries globally to adopt the rules and assist in providing cross-border data flow protection. More recently the EU has enacted the new Privacy Shield Framework regulation, upgrading the safe harbour protection laws by providing extended forms of data transmission and cross-border data protection between the EU and the USA while RSA has also provided the limitation of liability protection through section 70 of the ECTA.

The study further offered an analysis of the avoidance by users of territorial locations that prevent the users from viewing certain internet or cloud materials from the user's physical location. Through the web, users can access the cloud in a country other than their own, which is limited by sector-specific regulations. The study provided a high-level view of the legal status and the opinions that exist in support of developing new solutions to allow the use of the cloud legitimately beyond the sector-specific limitations, without undermining the development of the cloud, while at the same time preserving the law.

The present-day importance of the questions regarding the future of cloud is intensified by the desire of governments and the private sector to erect borders on the cloud to achieve compliance with the territorially-defined regulation. While it is possible to have sector-specific regulations through the use of regional or geolocation tools at present, this method of choice will not be the territorial practice of internet or cloud restrictions in the future. However, authorities would best look for network neutrality solutions and unified global distribution to resolve these issues.

Even with all these safeguards in place the international private law challenges and problems still rest before the Courts. The very complex issue of jurisdiction is at the heart of how and where infringements may be resolved. Very few new legal cases have tested the full strength of these regulations and while the discussion provided a broad outline of private international law, a more comprehensive understanding of the problem questions remains. Further work and analysis would need to be performed to reach in-depth and productive answers to some of the associated problems that continue in private international law.

The third consideration are the challenges posed by personal data protection, copyright and IP in the cloud. The study has focused on the underlying legal issues for cloud computing, from the security of the services provided to the protection of personal data. However, progressively, the copyright and IPRs legal issues are gaining prominence. The assessment of the contractual terms and license conditions from a broad range of cloud services to covering the aspects of 'fair use' of copyrighted work in the cloud and copyright safeguards has revealed both common elements and contrasts.

Many cloud providers include essentials in their terms and conditions asserting wide-ranging disclaimers of liability or any warranty that the service will operate as described, or indeed at all. Conversely, prospective customers may find that the threshold for disclosure to a third party, the extent to which data will be preserved following the end of a contract and the legal system under which the contract was offered will vary widely from provider to provider.

Alternatively, public or administrative law intervention or regulatory pressure may be brought to bear against providers to ensure that, for example, users are offered terms and conditions that are compliant with national and international consumer protection law. The cloud requirements element of national and international legal frameworks is as an ongoing endeavour and must continue to be monitored for changes to the private law terms on which such services are offered. As the cloud marketplace expands and matures, it is expected that such conditions will evolve and diversify to more closely reflect both customer concerns and the local legal framework under which those users operate.

Finally, the study showed that most of the rules and regulations that combined make up the national and international legal framework for the information society have been beneficial to nurturing the uptake of online and cloud services and encouraging users to participate in the information society. However, over the past decade and mostly post the adoption of the rules and regulations, there appears to be a hindrance by the increased complexity of the cloud environment and the introduction of new trends and technologies. While the legal issues of some rules and regulations can be resolved through small incremental updates, others require

a more fundamental revision. A so-called version 2.0 upgrade will ensure that the national and international legal framework will be prepared for the evolving cloud computing environment and a Single Global Information Space and digital legal framework.

Bibliography

References and sources used and consulted

BOOKS

B

BAINBRIDGE, D. and HOWELL, C. — Bainbridge D. and Howell C. (2011) *Intellectual Property Law*. 2nd ed. Law Express series. England: Pearson Education Limited.

BLACK, J. — BLACK, J. (2008) Constructing and contesting legitimacy and accountability in polycentric regulatory regimes. *Journal Regulation and Governance*. Asia: Blackwell Publishing Asia Pty Ltd.

BRASSEY, M. et al. — BRASSEY, M. et al. (2002) *Competition Law.* Cape Town: Juta Publishing.

C

CHEUNG, A.S.Y. and WEBER, R.H. — CHEUNG, A.S.Y. and WEBER, R.H. (2015) *Privacy and the legal issues in cloud computing*. Cheltenham: Edward Elgar Publishing.

CORREA, C.M. — CORREA, C.M. (2000) *Intellectual Property Rights, WTO, and Developing Countries The TRIPS Agreement and Policy Options*. London: Zed Books Ltd.

D

DUDLEY, A. — DUDLEY, A. et al. (2012) *Investigating cyber law and cyber ethics: Issues, impacts and practices.* Hershey PA: Information Science Reference.

DUGARD, J. (2013) — DUGARD, J. (2013) *International Law, A South African Perspective*. 4th ed. Cape Town: Juta & Co.

G

GINSBURG, J.C. and TREPPOZ, E. — GINSBURG, J.C. and TREPPOZ, E. (2015*) International Copyright Law: U.S. and E.U. perspectives: Text and cases*. Cheltenham: Edward Elgar. p. 413, Sec IV.

H

HUNTER, D. — HUNTER, D. (2012) *The Oxford Introductions to U.S. Law: Intellectual Property.* New York Oxford Publishers.

K

KLOPPER, H.B. — KLOPPER, H.B. et al. (2011) *Law of Intellectual Property in South Africa*. Cape Town: LexisNexis.

KLOTTER, J.C. — KLOTTER, J.C. (2012). *Justice Administration Legal Series*. 13th ed. Section 5. USA: Anderson Publishing Waltham.

KNOT, G. — KNOT, G. (2009) *Ripped: How the wired generation revolutionised music paperback*. New York: Simon and Schuster, Inc.

L

LESSIG, L. — LESSIG, L. (2006) *CODE version 2*. New York: Perseus Books.

LEWIS, D. — LEWIS, D. (2008*) 'Chilling competition'. International Antitrust Law and Policy: Fordham Competition Law.* New York: Juris Legal Information.

M

MARCHINI, R — MARCHINI, R. (2015) *Cloud computing. A practical introduction to the legal issues.* 2nd ed. London: BSI Standards Limited.

MERCURIO, B. and JUNG NI, K — MERCURIO, B. and JUNG NI, K. (ed.) (2014) *Science and technology in international economic law: Balancing competing interests*. Abingdon: Routledge.

MERGES, R.P., MENELL, P.S. and LEMLEY, M.A. — MERGES, R.P., MENELL, P.S. and LEMLEY, M.A. (2012) *Intellectual Property in the new technological age. 6th ed.* New York: Aspen Casebook Series, Wolters Kluwer Law and Business.

MILLARD, C — MILLARD, C. (ed.) (2014) *Cloud computing law*. Oxford: Oxford Scholarship Online. Part IV Cloud Regulation and Governance.

MURRAY, A — MURRAY, A. (2007) *The regulation of cyberspace: Control in the online environment*. Abingdon: Routledge-Cavendish.

P

PATRY, W. — PATRY, W. (2009) *Moral panics and the copyright wars*. New York: Oxford University Press, Inc.

PATRY, W. — PATRY, W. (2011) *How to fix copyright*. New York: Oxford University Press, Inc.

PUTROVA, N. — PURTOVA, N. (2012).*Property rights in personal data. A European perspective*. Netherlands: Kluwer Law International.

R

ROUTLEDGE. — ROUTLEDGE. (2012) *Intellectual Property Law 2012-2013. 8th ed*. England: Routledge publishing.

S

SCHEDLER, A. et al. (eds.) — SCHEDLER, A. et al. (eds.) (1999) *Conceptualising accountability the self-restraining state: Power and accountability in new democracies*. London: Lynne Reiner Publishers.

SCHONBERGER, V.M. and CUKIER, K. — SCHONBERGER, V.M. and CUKIER, K. (2013) *Big Data: A revolution that will transform how we live, work*. London: John Murray Publishers.

SHAPIRO, A.L. — SHAPIRO, A.L. (1999) *The control revolution: How the internet is putting individuals in charge and changing the world we know. 2nd ed*. New York: Public Affairs.

T

THOMAS, E. PUTTINI, R. and ZAIGHAM, M. — THOMAS, E. PUTTINI, R. and ZAIGHAM, M. (2013) *Cloud computing: Concepts, technology & architecture.* Cape Town: The Prentice Hall Service Technology Series.

TIAN, Y. — TIAN, Y. (2009) *Rethinking intellectual property: The political economy of copyright.* London: Routledge-Cavendish.

W

WISEMAND, L. — WISEMAN, L. (2012). *Copyright and the challenge of the new*. Netherlands: Wolters Kluwer Information Law Series, 25.

JOURNALS

A

ABA Journal — KENNEDY, D. (2009) Working in the cloud. *ABA Journal*.

Albany publishers Law Journal of Science and Technology — DEMPSEY, J.X. (1997) Communications privacy in the digital age: Revitalising the federal wiretap laws to enhance privacy. *Albany publishers Law Journal of Science & Technology*, 8 (1).

The American Journal of Comparative Law	PATRY, W. (2000) Choice of law and international copyright. *The American Journal of Comparative Law.*
C	
Cardozo Arts and Entertainment Law Journal	GINSBURG, J.C. (1997) Copyright without borders? Choice of forum and choice of law for copyright infringement in cyberspace. *Cardozo Arts and Entertainment Law Journal.*
	GORDON, W.J. et al. (1994) Virtual reality, appropriation, and property rights in art: A roundtable discussion. *Cardozo Arts and Entertainment Law Journal.*
	YU, P.K. (2012) Region codes and the territorial mess. *Cardozo Arts and Entertainment Law Journal.*
Cardozo Journal of International and Comparative Law	VINELLI, R. (2009) Bringing down the walls: How technology is being used to thwart parallel importers amid the international confusion concerning exhaustion of rights. *Cardozo Journal of International and Comparative Law*.
E	
European Intellectual Property review	ANDERSON, G.N. (2010) Are individuals waking up to the privacy implications of social-networking sites? *European Intellectual Property Review*, 32 (3).
Electronic Journal of Comparative Law	FIORINI, A. (2008) The codification of private international law in Europe. *Electronic Journal of Comparative Law*, 12 (1).
European Journal of Current Legal Issues	ROLF, H. et al. (2014) Cloud computing: A cluster of complex liability issues. *European Journal of Current Legal Issues*.
F	
Fordham Intellectual Property, Media and Entertainment Law Journal	MELZER, M.A. (2011) Copyright enforcement in the cloud. Fordham Intellectual Property. *Media and Entertainment Law Journal,* 21 (2).
I	
Intellectual Property Law Journal	*South African Intellectual Property Law Journal* (2013), 1, 2013 Cape Town: Juta Law.
J	
The John Marshall Journal of Information Technology & Privacy Law	MURRAY A. (2008) Symbiotic regulation. *The John Marshall Journal of Information Technology & Privacy Law.*
Journal of Behavioural Decision Making	LOWENSTEIN, G. and ISSACHAROFF, S. (1994) Source dependence in the valuation of objects. *Journal of Behavioural Decision Making*, 7, CMU.
Journal of Business & Technology Law	HOOVER, J.N. (2013.) Compliance in the ether: Cloud computing, data security and business regulation. *Journal of Business & Technology Law*. 8 (1), Art. 18. http://digitalcommons.law [Accessed 12 May 2015].
The Journal of Economic Perspectives	KAHNEMAN, D., KNETSCH, J.L. and THALER, R.H. (1991) Anomalies: The endowment effect, loss aversion, and status quo bias. *The Journal of Economic Perspectives, Princeton.*
Journal of Information Technology and Politics	JAEGER, P., LIN, J. and GRIMES, M. (2008) Cloud computing and information policy: Computing in a policy cloud? Journal of Information Technology and Politics.

http://www.tandfonline.com/doi/pdf/10.1080/19331680802425479 [Accessed 24 April 2016].

Journal of Internet Law

NARAYANAN, V. (2012) Harnessing the cloud: International law implications of cloud computing. *Journal of Internet Law*, 14 (1).

WITTOW, M.H. and BULLER, D.J. (2010) Cloud computing: Emerging legal issues for access to data, anywhere, anytime. *Journal of Internet Law*.

Journal of Law, Medicine and Ethics

SWEENEY, L. (1997) Weaving technology and policy together to maintain confidentiality. *Journal of Law, Medicine and Ethics*.

Journal of the Patent & Trademark Office Society

MARTIN, T.D. (2010*)* Hey! You! Get off my cloud: Defining and protecting the metes and bounds of privacy, security and property in cloud computing. *Journal of the Patent & Trademark Office Society*.

Journal of World Intellectual Property

DRAHOS, P. (2002) Developing countries and international Intellectual Property standard setting. *The Journal of World Intellectual Property*, 5 (5).

Journal Regulation and Governance

BLACK, J. (2008) Constructing and contesting legitimacy and accountability in polycentric regulatory regimes. *Journal Regulation and Governance.* Blackwell Publishing Asia Pty Ltd.

L

Law Journal of Science & Technology

DEMPSEY, J.X. (1997) Communications privacy in the digital age: Revitalising the Federal wiretap laws to enhance privacy. *Albany publishers Law Journal of Science & Technology,* 8 (1).

R

Rutgers Computer & Technology Law Journal

YIJUN, T. (2005). Reform of existing database legislation and future database legislation strategies: Towards a better balance in the database law. *Rutgers Computer & Technology Law Journal*, 31 (2).

S

Stanford Technology Law Review

HON, W.K., MILLARD, C. and WALDEN, I. (2012b) Negotiating cloud contracts, looking at clouds from both sides now. *Stanford Technology Law Review*.

W

The Wall Street Journal

VALENTINO-DEVRIES, J. and SINGER-VINE, J. (2012) They know what you're shopping for. *The Wall Street Journal*.

World Intellectual Property Organization Journal

ABBOT, F.M. (2009) Seizure of generic pharmaceuticals in transit based on allegations of patent infringement: A threat to international trade, development and public welfare. *World Intellectual Property Organization Journal* (WIPO), 1.

WATAL, J. (2011) From Punta Del Este to Doha and Beyond: Lessons from the TRIPs negotiating processes, analysis of intellectual property issues. *World Intellectual Property Organization Journal* (WIPO), 3 (1).

LEGISLATION

EUROPEAN UNION

GERMANY

Law on the Protection of Designs
(As amended up to Law of October 19, 2013)
Law of 1996 Amending the Trade Mark Law
Act on Copyright and Related Rights (Copyright Act, as amended up to Law of October 1, 2013)
Law on the Administration of Copyright and Related rights
(Amended up to Law of October 1, 2013)

SOUTH ARICA

CONSTITUTION

Constitution of The Republic of South Africa No. 108 of 1996 as amended up to 2012.

TREATIES AND STATUTES.

Trademark Law Treaty.
WIPO Copyright Treaty.
WIPO Performances and Phonograms Treaty.
Patent Cooperation Treaty [March 16, 1999].
Convention Establishing the World Intellectual Property Organization (March 23, 1975).
Paris Convention for the Protection of Industrial Property (December 1, 1947).
Berne Convention for the Protection of Literary and Artistic Works October 3, 1928).
Intellectual Property Laws Amendment Act 2013
(Act No. 28 of 2013) (2013).
Intellectual Property Rights from Publicly Financed Research and Development Act 2008 (Act No. 51 of 2008).
The Protection of Personal Information Act No. 4 of 2013 of South Africa, Policy.
Copyright Act, 1978 (Act No. 98 of 1978 as amended up to Copyright Amendment Act 2002) 2002.
Intellectual Property Laws Amendment Act 1997
(Act No. 38 of 1997).
Intellectual Property Laws Rationalisation Act 1996
(Act No. 107 of 1996).
National Credit Act No. 34 of 2005
Electronic Communications and Transaction Act 25 of 2002 (SA)
Competition Act No. 89 of 1998 (Date of commencement of sections 1-3, 6, 11, 19-43, 78, 79 & 84 on 30 November 1998. The remaining sections of the Act commenced on 1 September 1999.
Regulations No. R.675 of 2010 of the Intellectual Property Rights from Publicly Financed Research and Development Act 2008.
Regulations No. R.223 of March 9, 2001, relating to the Promotion of Access to Information Act 2000 (Act No. 2 of 2000) (2001).
Copyright Regulations 1978 (as amended by GN 1375 in GG 9807 of June 28, 1985).
Registration of Copyright in Cinematograph Films Regulations 1980.

UNITED KINGDOM

The Broadcasting Act 1996 (Chapter 55).
Copyright, etc. and Trade Marks (Offences and Enforcement) Act 2002 (Chapter 25).
Copyright, Designs and Patents Act 1988 (Chapter 48).

The UNITED STATES OF AMERICA

The Constitution of the United States of America (1787).

Prioritising Resources and Organization for Intellectual Property Act of 2008 (Public Law 110-403, 122 Stat. 4256).
To Implement the North American Free Trade Agreement (Public Law No. 103-182, 107 Stat. 2057).
Family Entertainment and Copyright Act of 2005 (Public Law 109-9, 119 Stat. 218).
No Electronic Theft (Net) Act (Public Law 105-147, 111 Stat. 2678).
U.S. Copyright Law, 17. U.S.C. §§ 101 et seq. (Consolidated Copyright Laws as of December 2011).

CASE LAW.

C

Case Law

Itar-Tass Russian News Agency et al., Plaintiff, v. Russian Kurier, INC. et al., Defendant. Al J. DANIEL, Jr. and Michael New City, Appellants, v. Itar-Tass Russian New Agency et al., and Julian H. Lowenfeld and Moskovsky Komsomolets and AR Publishing Co. Inc., Appellees. Docket No. 97-7444. Decided: April 03, 1998. United States Court of Appeals, Second Circuit.

Northwestern Memorial Hospital v John Ashcroft, United States Court of Appeals, Seventh Circuit, Attorney General of the United States, Defendant-Appellant. No. 04-1379. Court Decision: 362 Federal Reporter, 3d Series 923; 2004 Mar 26 (date of decision). Case Law.

Competition Tribunal

Commission v. Senwes Case CCT 61/11 [2012] ZACC 6 and the Tribunal has found Telkom guilty of contravening sections 8(b) and 8(d)(i) on 7 August 2012 in Commission v. Telkom SA Ltd case 11/CR/Feb04.

Curia Europa

The British Horseracing Board Ltd v. William Hill Organisation Ltd, C-203/02, 2004, Reference for a preliminary ruling concerns the interpretation of Article 7 and Article 10(3) of Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases (OJ 1996 L 77, p. 20, 'the directive').

Case 130-79 eDate Advertising GmbH v. X (C-509/09) and Olivier Martinez and Robert Martinez v. MGN Limited (C-161/10). References for a preliminary ruling: Bundesgerichtshof - Germany and Tribunal de Grande Instance de Paris - France. Regulation (EC) No. 44/2001 - Jurisdiction and the enforcement of judgments in civil and commercial matters - Jurisdiction 'in matters relating to tort, delict or quasi-delict' - Directive 2000/31/EC - Publication of information on the internet - Adverse effect on personality rights - Place where the harmful event occurred or may occur - Law applicable to information society services. Joined cases C-509/09 and C-161/10.

Case C-5/11 criminal proceedings against Titus Alexander Jochen Donner [2012] ecr Judgment of the Court (Fourth Chamber) of 21 June 2012. Criminal proceedings against Titus Alexander Jochen Donner. Reference for a preliminary ruling: Bundesgerichtshof - Germany. Free movement of goods - Industrial and commercial property - Sale of reproductions of works in a Member State in which the copyright on those works is not protected - Transport of those goods to another Member State in which the infringement of the copyright is sanctioned under criminal law - Criminal proceedings against the transporter for aiding and abetting the unlawful distribution of a work protected by copyright law.

Coreck Maritime GmbH v. Handelsveem BV and Others. Reference for a preliminary ruling: Hoge Raad der Nederlanden - Netherlands. Brussels

Convention - Article 17 - Clause conferring jurisdiction - Formal conditions - Effects. Case C-387/98.

Daniela Mühlleitner v. Ahmad Yusufi & Wadat Yusufi, (Jurisdiction in civil and commercial matters – Jurisdiction over consumer contracts – Regulation (EC) No. 44/2001 – Article 15(1)(c) – Possible limitation of that jurisdiction to distance contracts) Case C 190/11.

The European Commission v. Federal Republic of Germany. Failure of a Member State to fulfil obligations – Electronic communications – Directive 2002/19/EC – Directive 2002/21/EC – Directive 2002/22/EC – Networks and services - National rules – New markets. Case C-424/07. (2009).

The European Commission v. Federal Republic of Germany. (Advocate General Opinion) Case C-424/07. (2009) Curia Europa. http://curia.europa.eu/juris/liste.jsf?language=en&jur=C,T,F&num=c-424/07&td=ALL [Accessed 15 May 2016].

Federal Republic of Germany v. European Parliament and Council of the European Union. Directive 98/43/EC – Advertising and sponsorship of tobacco products – Legal basis – Article 100a of the EC Treaty (now, after amendment, Article 95 EC). Case C-376/98.

France Telecom SA v. Commission of the European Communities. Case C-202/07 P.

Google Inc. v. Vidal-Hall Neutral Citation Number: [2015] EWCA Civ 311. Royal Court of Justice.

Handelskwekerij G.J. Bier B.V. v. Mines de Potasse d'Alsace S.A. (preliminary ruling requested by the Gerechtshof of The Hague) Case 21/76.

Judgement based on. Regulation (EC) No. 44/2001 – Jurisdiction and the enforcement of judgments in civil and commercial matters – Jurisdiction 'in matters relating to tort, delict or quasi-delict' – Directive 2000/31/EC – Publication of information on the internet – Adverse effect on personality rights – Place where the harmful event occurred or may occur – Law applicable to information society services.

The judgement of the Court (Grand Chamber) (2010) In Joined Cases C 316/07, C 358/07 to C 360/07, C 409/07 and C 410/07.
The judgement of the Court (Second Chamber) (2010) Case C 258/08, Ladbrokes Betting & Gaming Ltd, Ladbrokes International Ltd v. Stichting de Nationale Sporttotalisator.

Lokman Emrek v. Vlado Sabranovic (Area of freedom, security and justice – Jurisdiction in civil and commercial matters – Regulation No. 44/2001– Consumer contracts – Article 15(1)(c) – Activity directed to another Member State – Need for a causal link between the activities of the trader directed to the Member State of the consumer – Strong evidence – Conurbation) Case C 218/12.

L'Oréal SA and others v. eBay International AG and Others. Reference for a preliminary ruling: High Court of Justice (England & Wales), Chancery Division - United Kingdom. Case C-324/09.

Maximillian Schrems v. Data Protection Commissioner joined party: Digital Rights Ireland Ltd, Case C 362/14 2015.

Oscar Bronner GmbH & Co. KG v. Mediaprint Zeitungs- und Zeitschriftenverlag GmbH & Co. KG, Mediaprint Zeitungsvertriebsgesellschaft mbH & Co. KG and Mediaprint Anzeigengesellschaft mbH & Co. KG, Case C-7/97 (1998).

Peter Pammer v. Reederei Karl Schlüter GmbH & Co KG (C 585/08), and Hotel Alpenhof GesmbH v. Oliver Heller (C 144/09), 2010.

Peter Pinckney v. KDG Mediatech AG, Case C 170/12.

The Queen, on the application of Vodafone Ltd and Others v. Secretary of State for Business, Enterprise and Regulatory Reform. Reference for a preliminary ruling: High Court of Justice (England & Wales), Queen's Bench Division (Administrative Court) – United Kingdom. Regulation (EC) No. 717/2007 – Roaming on public mobile telephone networks within the Community – Validity – Legal basis – Article 95 EC – Principles of proportionality and subsidiarity. Case C-58/08.

United Kingdom of Great Britain and Northern Ireland v. European Parliament and Council of the European Union. Regulation (EC) No. 460/2004 – European Network and Information Security Agency – Choice of legal basis. Case C-217/04.

Wintersteiger AG v. Products 4U Sondermaschinenbau GmbH, C 523/10.

Cyber Law Harvard

Cartoon Network et al., v. Cablevision et al, 536 F.3d 121 (2d Cir. 2008).

D

Dejure

BGH decision BGH GRUR 1983, 377 – Brombeer-Muster.

E

ECHR

Bankovic and Others v. Belgium and Others (Application No. 52207/99). Grand Chamber 1. Decision of 12 December 2001.

Matthews v. the United Kingdom. (Application No. 24833/94 39, Grand Chamber. ECHR 1999-1.

Eur-Lex

Fiona Shevill, Ixora Trading Inc., Chequepoint SARL and Chequepoint International Ltd v. Presse Alliance SA. Reference for a preliminary ruling: House of Lords - United Kingdom. Brussels Convention - Article 5 (3) - Place where the harmful event occurred - Libel by a newspaper article. Case C-68/93.

Football Dataco Ltd, Scottish Premier League Ltd, Scottish Football League, PA Sport UK Ltd v. Sportradar GmbH, Sportradar AG, Case C 173/11 ECLI:EU:C:2012:642, 2012.

Volker und Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v. Land Hessen. References for a preliminary ruling: Verwaltungsgericht Wiesbaden - Germany. Joined cases C-92/09 and C-93/09.

Euro Rapid Press

Court of Justice of the European Union PRESS RELEASE No. 115/11 Luxembourg, 25 October 2011. Press and Information Judgment in Joined Cases

C-509/09 and C-161/10 E-Date Advertising GmbH v. X and Olivier Martinez and Robert Martinez v. MGN Limited.

E-Date Advertising GmbH v. X and Olivier Martinez and Robert Martinez v. MGN Limited. Europa Rapid Press.

Fraley — *Fraley et al. v. Facebook, Inc., et al., Case No. CV-11-01726 RS.*

H

H2O Harvard Law School — *SUBAFILMS, LTD; The Hearst Corp., Plaintiffs-counter-defendants-Appellees, v. MGM-PATHE COMMUNICATIONS CO., FKA MGM/UA Communications Co. and as United Artists Corporation; MGM/UA Home Video, Inc.; Warner Home Video, Inc.; Warner Bros. Inc., Defendants-counter-claimants-Appellants. And SUBAFILMS, LTD; The Hearst Corp., Plaintiffs-Appellants, v. MGM-PATHE COMMUNICATIONS CO., FKA MGM/UA Communications Co. and as United Artists Corporation; MGM/UA Home Video, Inc.; Warner Home Video, Inc.; Warner Bros. Inc.; United Artists Corporation, Defendants-Appellees. Nos. 91-56248, 91-56379 and 91-56289. United States Court of Appeals, Ninth Circuit. Argued and Submitted February 24, 1994. Decided May 13, 1994.*

The T.J. Hooper. The Northern No. 30 and No. 17. The Montrose. In re Eastern Transp. Co. New England Coal & Coke Co. v. Northern Barge Corporation. H.N. Hartwell & Son, Inc. v. Same. No. 430. Circuit Court of Appeals, Second Circuit. July 21, 1932. 60 F.2d 737 (1932).

I

INFO CURIA — *Case-law of the Court of Justice. The judgement of the Court (Second Chamber) 3 June 2010. Case C-258/08, Ladbrokes Betting & Gaming Ltd, Ladbrokes International Ltd v. Stichting de Nationale Sporttotalisator*:

The judgement of the Court (Grand Chamber) 8 September 2010. In Joined Cases C-316/07, C-358/07 to C-360/07, C-409/07 and C-410/07.

IP in Brief — *UMG Recordings, Inc. v. Veoh Networks Inc., 665 F. Supp. 2d 1099 (C.D. Cal.2009).*

J

JOLT Law Harvard — *Io Group, Inc. v. Veoh Networks, Inc. N.D. Cal., August 27, 2008, No. C06-03926 HRL.*

Viacom Int'l Inc. v. YouTube, Inc., 07 Civ. 2103 (S.D.N.Y. April 18, 2013). JOLT Law Harvard. http://jolt.law.harvard.edu/digest/copyright/district-court-grants-summary-judgment-to-youtube-in-viacom-v-youtube-again. [Accessed 15 April 2016].

L

Law Blog SA — *Galago Publishers (Pty) Ltd & another v. Erasmus 1989 (1) SA 276 (A) at 283 C.*

Law Publishers — *Judgements on Copyright 18, Case, Technical Information Systems Pty Ltd v. Marconi Pty Ltd, STRANEX, M. (n.d.).*

Leagle — Parkson v Central DuPage Hospital Nos. 80-503, 80-504 cons. 105III. Appellate Court of Illinois, First District third division. 435 N.E.2d 140. Leagle.

P

Private Study — *Hawkes & Sons (London) Limited v Paramount Film Service, Limited [1934] 1 Ch. 593 (C.A.).*

R

Royal Court of Justice. — *Google Inc. v. Vidal-Hall Neutral Citation Number: [2015] EWCA Civ 311*

S

Southern African Legal Information Institute — *Competition Commission v. BMW South Africa (Pty) Ltd t/a BMW Motorrad (97/CR/Sep08) [2010] ZACT 21.*

Financial Mail (Pty) Ltd and Others v. Sage Holdings Ltd and Another (612/90) [1993] ZASCA 3; 1993 (2) SA 451 (AD); [1993] 2 All SA 109 (A).

Haupt t/a Soft Copy v. Brewers Marketing Intelligence (Pty) Ltd and others 2006 (4) SA 458 SCA.

King v. South African Weather Services (716/07) [2008] ZASCA 143; 2008 BIP 330 (SCA); 2009 (3) SA 13 (SCA); [2009] 2 All SA 31 (SCA).

Mayne v. Main (182/99) [2001] ZASCA 35; [2001] 3 All SA 157 (A).

Payen Components South Africa Ltd v. Bovic Gaskets CC and Others (448/93) [1995] ZASCA 57; 1995 (4) SA 441 (AD); [1995] 2 All SA 600 (A) (25 May 1995).

Vanguard Rigging (Pty) Ltd v. Nordengen and Another (983/2012) [2012] ZAGPJHC 284.

U

The University of Cambridge. Centre for Intellectual Property and Information Law. — *Cramp & Sons Ltd v. Frank Smythson Ltd [1944] AC 329.*

Ladbroke v. William Hill [1964] 1 All ER 465.

US Supreme Court — *Equal Employment Opportunity Commission v. Arabian American Oil Company Nos. 89-1838, 89-1845Argued Jan. 16, 1991, Decided March 26, 1991, 499 U.S. 244 Certiorari to the United State Court of Appeals for the fifth Circuit.*

Feist Publications Inc. v. Rural Tel. Svc. Co., Inc. Supreme Court of the United States, 499 U.S. 340 (1991).

Kirtsaeng, DBA Bluechristne99 v John Wiley and Sons, Inc. Certiorari to the United State Court of Appeals for the second Circuit, No. 11–697. Argued October 29, 2012—Decided March 19, 2013. Supreme Court.

INTERNET

A

A4CLOUD — A4CLOUD. (n.d.) *Cloud accountability project.* A4CLOUD. http://www.a4cloud.eu/. [Accessed 22 April 2016].

ADAM and ADAMS — ADAM and ADAMS (2012). *Senwes: A victory for the Competition Commission but a potential Pandora's Box.* Polity. http://www.polity.org.za/ [Accessed 29 April 2016].

THE ADVISORY INSTITUTE — THE ADVISORY INSTITUTE. (2013) *The cloud takes shape: Global cloud survey |the implementation challenge.* KPMG. http://www.kpmg-institutes.com/ [Accessed 18 April 2016].

AGRELL, P. and BOGETOFT, P. — AGRELL, P. and BOGETOFT, P. (2002) *Ex-post Regulation Pre-project 2 – Final Report*. SUMICSID. http://www.sumicsid.com/ [Accessed 2 April 2016].

AHMED, T. — AHMED, T. (n.d.) *Comparative analysis of copyright protection of databases the path to follow*: Research Gate. http://www.researchgate.net. [Accessed 09 June 2015].

ALEXIADIS, P. — ALEXIADIS, P. (2012) *Balancing the application of ex post and ex ante disciplines under community law in electronic communications markets: Square pegs in Round holes.* Gibson Dunn. http://www.gibsondunn.com/ [Accessed 14 April 2016].

ALLENS. — ALLENS. (2004) *Australia-United States Free Trade Agreement: Impacts on IP, communications and technology*, ALLENS. http://www.allens.com.au/. [Accessed 27 September 2016].

ANONYMOUS. — ANONYMOUS. (n.d.) *Extra protection for digital media: Digital Millennium Copyright Act, Region Coding.* University of Florida. http://www.clas.ufl.edu/. [Accessed 5 April 2016].

ANONYMOUS. (2013) *A428 - TLC: Antitrust, Telecom Italia abused its dominant position in the network infrastructure*. Autorità Garante Della Concorrenza e Del Mercato. http://www.agcm.it/ [Accessed 17 May 2016].

ANONYMOUS. (2016) *Terms of service*, Dropbox. https://www.dropbox.com/ [Accessed 12 December 2016]. Section 'Services "AS IS".

APPLE Inc. — APPLE Inc. (n.d.) *iCloud terms and conditions.* Apple Legal. http://www.apple.com/ [Accessed 22 August 2016].

ASAY, M. — ASAY, M. (2009) *Facebook changes terms of service to control more user data*. CNET. http://www.cnet.com/ [Accessed 21 April 2016].

AUSTRALIAN GOVERNMENT — AUSTRALIAN GOVERNMENT. (2014) *Deregulation. The Australian Government is reducing the regulatory burden for business and the community*. Department of Communications. https://www.communications.gov.au/ [Accessed 21 September 2016].

AUSTRALIAN GOVERNMENT Privacy Act 1988. https://www.oaic.gov.au/ [Accessed 6 February 2016].

B

BARBARO, M. and ZELLER, T. — BARBARO, M. and ZELLER, T. (2006) *A face is exposed for AOL searcher no. 4417749*, Research Gate. https://www.researchgate.net/ [Accessed 28 March 2016].

BAUDIN, C. et al. — BAUDIN, C. et al. (2015) *Practical guide to Platform as a Service PaaS. Cloud Standards Customer Council*. CSCC. http://www.Cloud-council.org/. [Accessed 15 February 2016].

BAVASSO, A. — BAVASSO, A. (2009) *Recoupment in predatory pricing: France Telecom v. Commission*. Allan and Overy. http://www.allenovery.com/ [Accessed 8 May 2016].

BEREC — BEREC. (2012) *Guidelines for quality of service in the scope of net neutrality.* Body of European Regulators of Electronic Communications. BEREC. http://berec.europa.eu/ [Accessed 10 February 2016].

BERMAN, P.S. — BERMAN, P.S. (2005) *Towards a cosmopolitan vision of conflict of laws: redefining governmental interests in a global era.* George Washington University Law School. http://scholarship.law.gwu.edu/ [Accessed 3 May 2016].

BORAN, M. — BORAN, M. (2011) Stream of online TV shows and movies starts flowing. *Irish Times*. http://www.irishtimes.com/ [Accessed 23 April 2016].

BOREK, C. et al. — BOREK, C. et al. (2013) *Lost in the clouds: The impact of copyright scope on investment in cloud computing ventures*. IDEI. http://idei.fr/sites/ [Accessed 21 April 2016].

BORT, J. — BORT, J. (2015) Google just took the lead in the dangerous game called 'race to zero'. *Business Insider*. http://www.businessinsider.com/ [Accessed 30 April 2016].

BOSHOFF, W.H. — BOSHOFF, W.H. (2014) *Antitrust market definition: rationale, challenges and opportunities in South African competition policy*. Competition Commission. http://www.compcom.co.za/ [Accessed 15 January 2016].

BIRD and BIRD — BIRD and BIRD. (n.d.). *Cloud computing & your legal questions answered*. Two Birds. http://www.twobirds.com/ [Accessed: 23 May 2015].

BOSTON COUNSULTING GROUP — BOSTON CONSULTING GROUP. (2012) *The value of digital identity*. Liberty Global. http://www.libertyglobal.com/. [Accessed 11 February 2016].

BRADSHAW, S. MILLARD, C. and WALDEN, I. — BRADSHAW, S. MILLARD, C. and WALDEN, I. (2010) *Contracts for clouds: Comparison and analysis of the terms and conditions of cloud computing services*. SSRN. http://papers.ssrn.com/ [Accessed 11 March 2016].

BROWN, G. — BROWN, G. (2010) *Brown defends DNA database and CCTV roll-out*. Truth Alliance Network. http://truthalliance.net/ [Accessed 4 February 2016].

BUCCAFUSCO, C. and SPRIGMAN, C. — BUCCAFUSCO, C. and SPRIGMAN, C. (2010) *Valuing Intellectual Property: An Experiment.* SSRN. http://papers.ssrn.com/ [Accessed 16 March 2016].

BULLER, D.J. and WITTOW, M.H. — BULLER, D.J. and WITTOW, M.H. (2010) *Cloud computing: Emerging legal issues, data flows, the mobile user*. K and L Gates. http://www.klgates.com/ [Accessed: 13 June 2015].

BUTLER, B. — BUTLER, B. (2013) *Gartner: Top 10 cloud storage providers*. Net Work World. http://www.networkworld.com/ [Accessed 21 March 2016].

C

CABINET OFFICE — CABINET OFFICE. (2011) *Government ICT strategy.* Cabinet Office London. https://www.gov.uk/ [Accessed 21 May 2016].

CATTEDDU, D. and HOGBEN, G. — CATTEDDU, D. and HOGBEN, G. (2009) *Cloud computing, benefits, risks and recommendations for information security*. The European Network and Information

Security Agency. (ENISA). https://resilience.enisa.europa.eu/ [Accessed 22 August 2016].

CEPIS — CEPIS. (2013) *Statement on the draft EU General Data Protection Regulation*. CEPIS Council. http://www.cepis.org/media/ [Accessed 24 February 2016].

CITY OF LOS ANGELES — CITY OF LOS ANGELES. (2009) *Professional Services Contract between the City of Los Angeles and Computer Science Corp. for the SaaS E-mail and Collaboration Solution*. SECS. https://sites.google.com/ [Accessed 24 February 2016].

CLARKE, G. — CLARKE, G. (2011) *'Apple's iCloud runs on Microsoft and Amazon services: Who says Azure isn't cool and trendy now'*. The Register. http://www.theregister.co.uk/. [Accessed 2 August 2016].

CLOUD SECURITY ALLIANCE — CLOUD SECURITY ALLIANCE. (2011) *Security guidance for critical areas of focus in cloud computing V3.0.* Cloud Security Alliance CSA. https://cloudsecurityalliance.org/ [Accessed 15 December 2015].

CLOUD STANDARD CUSTOMER COUNCIL — CLOUD STANDARD CUSTOMER COUNCIL. (n.d.) *Practical guide to Platform as a Service PaaS* http://www.Cloud-council.org/ [Accessed 15th February 2016].

CLOUD STANDARDS CUSTOMER COUNCIL. (2016). Public cloud service agreements: What to expect and what to negotiate, Version 2.0.1. CSCC. http://www.cloud-council.org/deliverables/CSCC-Public-Cloud-Service-Agreements-What-to-Expect-and-What-to-Negotiate.pdf [Accessed 22 September 2016)

COATES, J. — COATES, J. (2010) *The Australian Parliament goes CC – with v3.0*. Creative Commons. http://creativecommons.org.au/ [Accessed 10 May 2016].

COHEN, J.E. — COHEN, J.E. (1998) *Copyright and the jurisprudence of self-help*. George Town University Law Center. http://scholarship.law.georgetown.edu/ [Accessed 23 February 2016].

COLUMBUS, L. — COLUMBUS, L. (2013) *Making cloud computing pay*. Forbes. https://www.forbes.com/ [Accessed 23 April 2016].

COMMITTEE ON CIVIL LIBERTIES — COMMITTEE ON CIVIL LIBERTIES. *On the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data on the free* movement of *such Department of Justice and Home Affairs. Report (General Data Protection Regulation) (COM (2012) 0011-C7-0025/2012-2012/0011(COD)) Amendment 34 Recital 49*: http://www.europarl.europa.eu/. [Accessed 12 January 2016].

COMMITTEE ON CIVIL LIBERTIES. *Justice and Home Affairs. (2013) on the proposal for a regulation of the European Parliament and of the Council 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) (COM (2012)0011 – C7-0025/2012 – 2012/0011(COD)).* European Parliament. http://www.europarl.europa.eu/ [Accessed 10 March 2016].

COMPETITION TRIBUNAL OF SOUTH AFRICA — COMPETITION TRIBUNAL OF SOUTH AFRICA. (2015) *Large Merger – Vodacom (Proprietary) Limited/Neotel (Proprietary) Limited*. Competition Tribunal. http://www.comptrib.co.za/ [Accessed 18 April 2016]

COPYRIGHT — *COPYRIGHT Act 1968, Commonwealth Consolidated Acts*. http://www.austlii.edu.au/ [Accessed 22 September 2016].

COPYRIGHT Law of the United States and Related Laws Contained in Title 17 of the United States Code. Copyright Gov. https://www.copyright.gov/. [Accessed 17 September 2016].

COPYRIGHT Amendment Act 125 of 1992. http://www.gov.za/ [Accessed 3 May 2015].

COPYRIGHT Amendment Bill b3 2017. Department of Trade and Industry. http://www.gov.za/ [Accessed 8 April 2016].

COPYRIGHT and Rights in Databases Regulations 1997 No. 3032 as amended. Legislation UK. http://www.legislation.gov.uk. [Accessed 16 March 2016].

CORDELL, N. — CORDELL, N. (2013) *Intellectual Property in the cloud*. Allen and Overy. http://www.allenovery.com/ [Accessed 4 January 2016].

CORNELL UNIVERSITY — CORNELL UNIVERSITY. (2012) *Chapter 36 – Foreign Intelligence Surveillance Subchapter IV*. Cornell University Law School. https://www.law.cornell.edu/. [Accessed 26 February 2016].

COUNCIL — *COUNCIL of the European Union, 2014, Proposal for a regulation of the European Parliament and of the Council 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)-Pseudonymised, Euro privacy.* http://register.consilium.europa.eu/. [Accessed 21 March 2016].

COUNCIL Regulation (EC) No. 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters. Eur-Lex. http://eur-lex.europa.eu/. [Accessed 10 March 2016].

COUNCIL Regulation (EC) No. 40/94 of 20 December 1993 on the Community trade mark. Eur-Lex. http://eur-lex.europa.eu/. [Accessed 6 April 2016].

COUNCIL of the European Union, 2000, Council Regulation (EC) No. 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters. Eur-Lex. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001R0044:en:HTML. [Accessed 15 January 2016].

CRAIG, R. et al. — CRAIG, R. et al. (2009) *Cloud computing in the public sector: Public manager's guide to evaluating and adopting cloud computing*. CISCO. http://www.cisco.com/. [Accessed 17 March 2016].

CRANE, J. — CRANE, J. (2012) *The death of outsourcing and other IT management trends.* Forbes. http://www.forbes.com/ [Accessed 20 August 2016].

CREATIVE COMMONS — CREATIVE COMMONS. (n.d.) *About the licences*. Creative Commons. http://creativecommons.org.au/ [Accessed 10 May 2016].

D

DATA PROTECTION COMMISSIONER — DATA PROTECTION COMMISSIONER. (n.d.) *Anonymisation and Pseudonymisation*. Data Protection. https://dataprotection.ie/ [Accessed 10 May 2016].

DATA PROTECTION WORKING PARTY — DATA PROTECTION WORKING PARTY. (2010) *WP 179 Opinion 8/2010 on applicable law*. EC Europa. http://ec.europa.eu/justice/ [Accessed 17 February 2016].

DEAZLEY, R. — DEAZLEY, R. (n.d.) *School of law commentaries, (Primary sources on Copyright 1450-1900)*. University of Birmingham. http://www.copyrighthistory.org/. [Accessed 4 April 2016].

DEFINITIONS — DEFINITIONS. (2016) *Anonymization definition*. Definitions.net. www.definitions.net [Accessed 11 January 2016].

DENHAM, E. — DENHAM, E. (2009) *Findings under the Personal Information Protection and Electronic Documents Act (PIPEDA)*. Office of the Privacy Commission of Canada. https://www.priv.gc.ca/ [Accessed 22 April 2016].

DEPARTMENT OF COMMUNICATIONS — DEPARTMENT OF COMMUNICATIONS. (2000) *A Green Paper on Electronic Commerce for South Africa Government*. Department of Communications. http://www.gov.za/sites/ [Accessed 11 April 2016].

DEPARTMENT OF COMMUNICATIONS. (2013) *South Africa connect: creating opportunities, ensuring inclusion, South Africa's broadband policy*. Department of Communications. http://www.gov.za/sites/ [Accessed 11 May 2016].

DEPARTMENT OF HEALTH AND HUMAN SCIENCES — DEPARTMENT OF HEALTH AND HUMAN SCIENCES. *45 CFR Parts 160 and 164 Standards for Privacy of Individually Identifiable Health Information; Final Rule*. HHS Government, http://www.hhs.gov/. [Accessed 12 February 2016].

DE SILVA, S. — DE SILVA, S. (2014) *5th Meeting of European Commission Expert Group on Cloud Computing Contracts Liability Discussion Paper*. EC Europa. http://ec.europa.eu/ [Accessed 23 August 2016].

DIGITAL CIVIL RIGHTS IN EUROPE — DIGITAL CIVIL RIGHTS IN EUROPE. (n.d.) *Article 29 Working Party on online social networking.* EDRI. http://history.edri.org/. [Accessed 22 April 2016].

DINWOODIE, G.B. — DINWOODIE, G.B. (2000) *A new copyright order: Why national courts should create global norms*. University of Pennsylvania Scholarship Law. http://scholarship.law.upenn.edu/ [Accessed 21 April 2016].

DOBSCHAT, C. — DOBSCHAT, C. (2013) *Surprise: Telekom-Drossel for all customers and traffic exceptions for "partner" confirmed*. Mobile Geeks. https://translate.google.com/ [Accessed 8 May 2016].

DOLMANS, M. and LEYDEN, A. — DOLMANS, M. and LEYDEN, A. (n.d.) Internet & antitrust: An overview of EU and national case law. *Competition Laws Bulletin*. https://www.clearygottlieb.com/ [Accessed 4 May 2016].

DONOHUE, M. and YPSILANTI, D. — DONOHUE, M. and YPSILANTI, D. (2009) *Briefing paper for the ICCP Technology Foresight Forum. Cloud Computing and Public Policy*. OECD. https://www.oecd.org/ [Accessed 15 March 2016].

DONOVAN, K., NORTH, J. and FONSEKA, R. — DONOVAN, K., NORTH, J. and FONSEKA, R. (2014) *Fair use exception to copyright infringement: The cloud is the limit*. Modaq. http://www.mondaq.com/ [Accessed 10 April 2016].

DROPBOX — DROPBOX. (2014) *Dropbox terms of service posted*. Dropbox, https://www.dropbox.com/ [Accessed 12 April 2016].

E

ENSOR, L. — ENSOR, L. (2017) *Revision plans for Copyright Bill raise MP's ire*, Business day, https://www.businesslive.co.za/bd/national/2017-08-21-revision-plans-for-copyright-bill-raise-mps-ire/ [Accessed 28 August 2017]

ERNEST — ERNEST. (n.d.) *Copyright in names*: Ernest. http://www.ernest.net/ [Accessed 16 March 2016].

ESPION — ESPION, (n.d.) *White Paper: Data Protection in the cloud*. Espion Group. https://www.espiongroup.com/ [Accessed 15 April 2016].

EURO CLOUD — EURO CLOUD. (2015) *Major mistakes in data privacy – data protection in the cloud*. Euro Cloud. https://www.eurocloud.org/ [Accessed 10 August 2016].

EUROPEAN COMMISSION — EUROPEAN COMMISSION. (2012) *Article 29 Data Protection Working Party*. EC Europa. http://ec.europa.eu/ [Accessed 9 January 2016].

EUROPEAN COMMISSION. *Building confidence in the cloud: A proposal for industry and government action for Europe to reap the benefits of cloud computing.* http://ec.europa.eu/ [Accessed 16 September 2015].

EUROPEAN COMMISSION. (2012) *Proposal for a Regulation of the European Parliament and of the Council 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)* Eur-Lex. http://eur-lex.europa.eu/. [Accessed 6 February 2016].

EUROPEAN COMMISSION. (2012) *Unleashing the potential of cloud computing in Europe. Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and the Committee of Regions*. Eur-Lex. http://eur-lex.europa.eu/. [Accessed 11 May 2016].

EUROPEAN COMMISSION. (2013) *Public Consultation on the review of the EU copyright rules*. EC Europa. http://ec.europa.eu/ [Accessed 8 April 2016].

EUROPEAN COMMISSION. (2016) *Overview on binding corporate rules*. EC Europa. http://ec.europa.eu/. [Accessed 12 December 2016].

EUROPEAN COMMISSION. Working party. (2005) *Working document on data protection issues related to Intellectual Property rights*. European Commission, Internal Market Directorate-General, Brussels. http://ec.europa.eu/. [Accessed 14 September 2015].

EUROPEAN COMMISSION. *Decision of 28 January 1992 establishing transitional measures for trade in bovine animals in relation to the cessation of vaccination against foot-and-mouth disease and revoking Decisions 91/13/EEC and 91 /177/EEC*. Eur-Lex. http://eur-lex.europa.eu/. [Accessed 23 March 2016].

EUROPEAN COMMISSION. *Regulation (EU) No. 330/2010 of 20 April 2010 on the application of Article 101(3) of the treaty on the Functioning of the European Union to categories of vertical agreements and concerted practices*. Eur-Lex. http://eur-lex.europa.eu/. [Accessed 20 April 2016].

EUROPEAN COMMISSION. *Article 29 Data Protection Working Party, 2009, Opinion 5/2009 on online social networking.* EC Europa., http://ec.europa.eu/. [Accessed 22 April 2016].

EUROPEAN COMMISSION. *Article 29 Data Protection Working Party Opinion 05/2012 on Cloud Computing Adopted July 1st 2012*. EC Europa. http://ec.europa.eu/ [Accessed 6 January 2016].

EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY

EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY. (2012) *Cloud computing benefits, risks and recommendations for information security rev b*. ENISA. http://www.bing.com/ [Accessed 16 January 2016].

EUROPEAN COURT OF HUMAN RIGHTS

EUROPEAN COURT OF HUMAN RIGHTS. (2010) *European Convention on Human Rights as amended by Protocols Nos. 11 and 14 supplemented by Protocols Nos. 1, 4, 6, 7, 12 and 13*. ECHR. http://www.echr.coe.int/ [Accessed 2 May 2016].

EUROPEAN COURT

EU COURTS DEBATE. (2007) *Legal analysis of a single market for the information society (SMART 2007/0037)*. EC Europa. http://ec.europa.eu/. [Accessed 26 March 2016].

European Convention on Human Rights, Council of Europe. http://www.echr.coe.int/ [Accessed 18 February 2016].

EUROPEAN PARLIAMENT

Communication from the Commission to the European Parliament and the Council, (2013) On the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU, EC Europa. http://ec.europa.eu/ [Accessed 15 July 2016].

Directive 95/46/EC of the European Parliament and 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. EC Europa. http://ec.europa.eu. [Accessed 22 April 2016].

Directive 96/91/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases. Eur-Lex. http://eur-lex.europa.eu/. [Accessed 12 March 2016].

Directive 2000/31/EC 2000 art 3 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'). Eur-Lex. http://eur-lex.europa.eu/ [Accessed 12 May 2016].

Directive 2002/19/EC of the European Parliament and the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive). Eur-Lex. http://eur-lex.europa.eu. [Accessed 18 May 2016].

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) Official Journal L 201, 31/07/2002 P. 0037 – 0047. Eur-Lex. http://eur-lex.europa.eu/. [Accessed 25 May 2016].

Directive 2009/24/EC of the European Parliament and the Council of 23 April 2009, on the legal protection of computer programs. Eur-Lex. http://eur-lex.europa.eu/ [Accessed 18 March 2016].

Directorate for Financial and Enterprise Affairs, Competition Committee. *(2012) Roundtable on Market Definition.* OECD. http://ec.europa.eu/ [Accessed 15 April 2016].

E-commerce directive, liability of intermediaries. EC Europa. https://ec.europa.eu/ [Accessed 26 March 2016].

EU copyright reform: Revisiting the principle of territoriality Briefing September 2015. Euro Parliament. http://www.europarl.europa.eu/ [Accessed 6 April 2016].

European Parliament, 1995, EU Data Protection 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. Eur-lex. http://eur-lex.europa.eu/ [Accessed 6 February 2016].

European Council: Directive 96/91 EC of the European Parliament of 11 March 1996 on the legal protection of databases. Eur-Lex. http://eur-lex.europa.eu/. [Accessed 16 March 2016].

European Parliament and of the Council of 22, 1998*. Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations.* Official Journal L 204, 21/07/1998 P. 0037 – 0048. Eur-Lex. http://eur-lex.europa.eu/ [Accessed 12 April 2016].

European Parliament and of the Council of 8 June 2000, Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') Official Journal L 178, 17/07/2000 P. 0001 – 0016. Eur-Lex. http://eur-lex.europa.eu/. [Accessed 12 April 2016].

European Parliament. Directive 2009/24/EC of the European Parliament and the Council of 23 April 2009, on the legal protection of computer programs. Eur-Lex. http://eur-lex.europa.eu/ [Accessed 18 March 2016].

European Parliament. Proposal for a Regulation of the European Parliament and the Council 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) [SEC (2012) 73 final]: Euro Parliament. http://www.europarl.europa.eu/ [Accessed 6 February 2016].

European Parliament and the Council of April 2016, 2016 Regulation 16/679, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). EC Europa, http://ec.europa.eu/. [Accessed 25 May 2016].

European Union (2012). Article 29 Data Protection Working Party Opinion 05/2012 on Cloud Computing Adopted July 1 2012, EC Europa. http://ec.europa.eu/ [Accessed 6 January 2016].

European Union. (2014) The EU explained: Digital agenda for Europe. EC Europa. https://europa.eu/. [Accessed 8 April 2016].

Information from European Union Intuition's, Bodies, Offices and Agencies European Commission. (2010) Guidelines on Vertical Restraints, (2010/C 130/01). Eur-Lex. http://eur-lex.europa.eu/ [Accessed 12 January 2016].

Information from the European Union Institutions and Bodies Commission. (2009) Communication from the Commission, Guidance on the Commission's enforcement priorities in Applying Article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings (2009/C 45/02). Eur-Lex. http://eur-lex.europa.eu/ [Accessed 19 February 2016].

Licences for Europe. (2013) Structured stakeholder dialogue. EC Europa. https://ec.europa.eu/ [Accessed 8 April 2016].

Licences for Europe. (2013) Ten pledges to bring more content online. EC Europa. http://ec.europa.eu/ [Accessed 8 April 2016].

Official Journal of the European Union. Recommendation 2003/311 of 11 February 2003 on relevant product and service markets within the electronic communications sector susceptible to ex ante regulation in accordance with Directive 2002/21 [2003] OJ L 114/45, ICT. https://www.ictregulationtoolkit.org/. [Accessed 6 January 2016].

Proposal for a Regulation of the European Parliament and the Council 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). Eur-Lex. http://eur-lex.europa.eu/. [Accessed 6 February 2016].

Regulation (EC) No. 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I). Eur-Lex. http://eur-lex.europa.eu/ [Accessed 2 April 2016].

Regulation (EC) No. 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations (Rome II). Eur-Lex. http://eur-lex.europa.eu/ [Accessed 4 April 2016].

Regulation (EU) No. 1215/2012 of the European Parliament and of the Council of 12 December 2012, on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast). Eur-Lex. http://eur-lex.europa.eu/ [Accessed 18 January 2016].

EUROPEAN TREATY SERIES

EUROPEAN TREATY SERIES. (1981) *No. 108 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*. RM Council of Europe. https://rm.coe.int/. [Accessed 8 February 2016].

EU-US Privacy Shield Framework (2016) https://www.privacyshield.gov/Program-Overview. [Accessed 15 April 2016].

EUROPEAN SPACE AGENCY

EUROPEAN SPACE AGENCY. *Copy right and databases*. ESA. http://www.esa.int/. [Accessed 20 August 2015].

F

FACEBOOK

FACEBOOK. (n.d.) *Facebook data collection and use policy*. Facebook. https://www.facebook.com/policy.php [Accessed 12 December 2016].

FACEBOOK. (2015) *Terms of service – Facebook*. Facebook. https://www.facebook.com/. [Accessed 14 March 2016].

FACEBOOK. (2015) *Terms of service, sharing your content and information.* Facebook. https://www.facebook.com/. [Accessed 12 March 2016].

FEDERAL PUBLIC SERVICE JUSTICE — FEDERAL PUBLIC SERVICE JUSTICE. *[C - 2004/09511] F. 2004 - 2935 16 JULY 2004. - Law Bearing the Code of Private International Law (1)*. Reflex Chrono. http://reflex.raadvst-consetat.be/ [Accessed 23 March 2016].

FOLEY — FOLEY. (n.d.) Cloud computing: A practical framework for managing cloud computing risk. Foley. https://www.foley.com/ [Accessed 10 March 2016].

FOREIGN INTELLIGENCE SURVEILLANCE ACT — *FOREIGN INTELLIGENCE SURVEILLANCE ACT of 1978, Justice Information Sharing U.S. Department of Justice*, Office of Justice Programs, Bureau of Justice Assistance. https://it.ojp.gov/. [Accessed 9 July 2016]

FREE TRADE AGREEMENTS — *Free Trade Agreements Australia. (2009) Office of the United States Trade Representative*. https://ustr.gov. [Accessed 12 October 2016].

Free Trade Agreements Singapore (2003) Office of the United States Trade Representative. https://ustr.gov [Accessed 29 September 2016].

FREE TRADE COMMISSION — FREE TRADE COMMISSION. (2012) *Protecting consumer privacy in an era of rapid change.* FTC. https://www.ftc.gov/ [Accessed 19 March 2016].

FREE TRADE COMMISSION. (2014) *Data brokers: A call for transparency and accountability*. FTC. https://www.ftc.gov [Accessed 23 March 2016].

G

GANTZ, J.F., MINTON, S. and TONCHEVA, A. — GANTZ, J.F., MINTON, S. and TONCHEVA, A. (2012) *Cloud computing's role in job creation. IDC White Paper sponsored by Microsoft.* Microsoft. https://news.microsoft.com/ [Accessed 16 April 2016].

GARTNER Inc. — GARTNER Inc. (2013) *Forecast: Public cloud services, worldwide, 2011-2017, 4Q13 Update*. Gartner. https://www.gartner.com/. [Accessed 7 December 2015].

GARTNER Inc. — GARTNER Inc. (2015) *Gartner identifies the top 10 strategic technology trends for 2016.* Gartner. http://www.gartner.com/ [Accessed 6 February 2016].

GASSER, U., FARIS, R. and JONES, R.H. — GASSER, U., FARIS, R. and JONES, R.H. (2013) *Internet monitor 2013: Reflections on the digital world*. The Berkman Center for Internet and Society Research Publication Series. https://papers.ssrn.com/ [Accessed 19 April 2016].

GASSER, U. and O'BRIEN, D. — GASSER, U. and O'BRIEN, D. (2014) *Governments and cloud computing: Roles, approaches, and policy considerations*. Berkman Center for internet and Society Research Publication. https://dash.harvard.edu/ [Accessed 17 May 2016].

GEBHART, G. — GEBHART, G. (2016) *What Facebook and WhatsApp's data sharing plans really mean for user privacy*. Electronic Frontier Foundation. EFF ORG. https://www.eff.org/ [Accessed 16 October 2016].

GEIST, M. — GEIST, M. (2005) *Anti-circumvention legislation and competition policy: Defining a Canadian way?* Irwin Law. https://www.irwinlaw.com/ [Accessed 23 February 2016].

GEOFFREY, C.C.I. — GEOFFREY, C.C.I. (2012) *Rethinking Jurisdiction under International Law*. Works Bepress. https://works.bepress.com/ [Accessed 15 March 2016].

GfK — GfK. (2016) *Marketing research-specializations.* GfK. http://www.gfk.com/ [Accessed 23 March 2016].

GIBSON, K. — GIBSON, K. (2015) *Keeping your secret recipe secret*. http://nu.it-online.co.za/ [Accessed 4 January 2016].

GOOGLE Inc. — GOOGLE Inc. (n.d.) *Google cloud platform terms of service*. Google. https://cloud.google.com/ [Accessed 16 January 2016].

GOOGLE Inc. (2014) *Terms of service. Your, content in our services*. Google Inc. https://www.google.com/ [Accessed 12 March 2016].

GREENLEAF, G. — GREENLEAF, G. (2015) *Global data privacy laws 2015: 109 countries, with European laws now a minority*. Privacy Laws & Business International Report. SSRN. http://papers.ssrn.com/. [Accessed 8 December 2015].

GURRY, F. — GURRY, F. (2013) *Address by the Director General WIPO Assemblies – September 23 to October 2, 2013*. WIPO. http://www.wipo.int/ [Accessed 23 April 2016].

H

HAINES, D. — HAINES, D. (2002) *The impact of the internet on the Judgements Project: Thoughts for the future*. Hague Conference on Private International Law. https://assets.hcch.net/ [Accessed 28 April 2016].

HALE, T.N. — HALE, T.N. (2008) *Transparency, accountability, and global governance*. Questa, trusted on line research. https://www.questia.com/ [Accessed 12 May 2016].

HARGREAVES, I. — HARGREAVES, I. (2011) *Digital opportunity: A review of intellectual property and growth.* Gov. UK Publications. https://www.gov.uk/ [Accessed 5 May 2016].

HARSHBARGER, J.A. — HARSHBARGER, J.A. (n.d.) *Cloud computing providers and data security Law: Building trust with United States companies*. Hein online. http://heinonline.org [Accessed 13 June 2015].

HAY, G.A. — HAY, G.A. (1982) *The economics of predatory pricing*. Cornell Law School. http://scholarship.law.cornell.edu/ [Accessed 26 April 2016].

HEALEY, A. — HEALEY, A. (n.d.) *Tracking individuals via their cell phones: Answering the Call*. Federal Law Enforcement Training Centres. https://www.fletc.gov/ [Accessed 4 February 2016].

HELLER, M. — HELLER, M. (2004) *The country of origin principle in E-commerce Directive: A conflict with conflict laws?* Eur Rev Priv L RQSL. http://www.rgsl.edu.lv/ [Accessed 12 April 2016].

HILLELSON, L. — HILLELSON, L. (n.d.) *Making the business case for the media industry transition to IP*. Broadcasting and Cable. https://www.cisco.com/ [Accessed 23 April 2016].

HITCH — HITCH Software Platform. (2016) *Provider terms of service*. Hitch HQ. https://www.hitchhq.com/ [Accessed 23 August 2016].

HOGENDORN, C. — HOGENDORN, C. (2007) *Broadband internet: Net neutrality versus open access*. Chogendorn. http://chogendorn.web.wesleyan.edu/ [Accessed 15 January 2016].

HOGAN LOVELLS — HOGAN LOVELLS. *Cloud computing: A primer on legal issues, including privacy and data security concerns*. CISCO. https://www.cisco.com/Web [Accessed 12 May 2015].

HON, W.K. et al. — HON, W.K. et al. (2014) *Cloud accountability: The likely impact of the proposed EU data protection regulation*. Research Gate. https://www.researchgate.net/ [Accessed 19 March 2016].

HON, W.K., MILLARD, C. and WALDEN, I. — HON, W.K., MILLARD, C. and WALDEN, I. (2011) *The problem of 'personal data' in cloud computing - what information is regulated? The cloud of unknowing, Part 1*. SSRN. http://papers.ssrn.com/ [Accessed 9 March 2016].

HON, W.K., MILLARD, C. and WALDEN, I. (2012a) *Who is responsible for 'personal data' in cloud computing? The cloud of unknowing, Part 2*. Queen Mary School of Law, Legal Studies. https://papers.ssrn.com/ [Accessed February 2016].

HON, W.K., MILLARD, C. and WALDEN, I. (2012b) Negotiating cloud contracts, looking at clouds from both sides now. *Stanford Technology Law Review*. https://journals.law.stanford.edu/sites/ [Accessed 16 February 2016].

HONG, K. — HONG, K. (2014) *Dropbox reaches 300m users, adding on 100m users in just six months*. The next Web. http://thenextWeb.com/ [Accessed 11January 2016].

HOOVER, J.N. — HOOVER, J.N. (2013) Compliance in the ether: Cloud computing, data security and business regulation. *Journal of Business & Technology Law*. 8 (1), Art. 18. Digital Commonshttp://digitalcommons.law.umaryland.edu/ [Accessed 12 May 2016].

HOU, L. et al. — HOU, L. et al. (2008) *Network neutrality in Europe*. Eurocpr. http://www.eurocpr.org/ [Accessed 21 May 2016].

H.R.1201 — *H.R.1201 - Digital Media Consumers' Rights Act of 2005 109th Congress (2005-2006).* Congress. Gov. https://www.congress.gov/ [Accessed May 5 2016].

HURLEY, D. — HURLEY, D. (2003) *Pole Star: Human rights in the information society, rights and democracy*. Brown. https://www.brown.edu/ [Accessed 12 May 2016].

HRYNASZKIEWICZ, I. et al. — HRYNASZKIEWICZ, I. et al. (2010) *Preparing raw clinical data for publication: guidance for journal editors, authors, and peer reviewers*. Comment in BMJ policy on data sharing. US National Library of Medicine National Institutes of Health. https://www.ncbi.nlm.nih.gov/ [Accessed 29 May 2016].

I

IBANEZ, J. — IBANEZ, J. (2005) *Who governs the internet?* The emerging regime of e-commerce, Pompeu Fabra. University Barcelona. https://ecpr.eu/ [Accessed 12 May 2016].

IBM — IBM. (2013) *IBM SaaS terms of service, smart cloud for business*. IBM. https://www-03.ibm.com/. [Accessed 9 April 2016].

INFORMATION COMMISSIONERS OFFICE — INFORMATION COMMISSIONERS OFFICE. *Data controller means*. ICO. https://ico.org.uk/ [Accessed 7 February 2016].

INFORMATION SYSTEMS AUDIT AND CONTROL ACCOSSIATION. (2011) *IT control objectives for cloud computing: Controls and assurance in the cloud*. ISACA. http://www.isaca.org/ [Accessed 12 February 2016].

IPR. (2004) *The Code of Private International Law (CPIL).* University of Gent. Institute for International Private Law. http://www.ipr.be/[Accessed 2 May 2016].

ISIBAYA – Registration. (n.d.) *Public Investment Corporation*. Isibaya. https://isibayafund.pic.gov.za/ [Accessed 15 June 2016].

ISRAELY, A. (2013) *Trends and applications. Big data poses legal issues and risks, database trends and applications*. http://www.dbta.com/ [Accessed 4 May 2015].

The Permanent Court of International Justice. (1927) Collection of judgments "The Case of the SS Lotus": Series A. No. 10 September 7th 1927. ICJ. http://www.icj-cij.org/ [Accessed 16 March 2016].

J

JACKSON, K. (2013) *A framework for cloud computing adoption in South African Government*. Cloud Credential Council. http://www.cloudcredential.org/ [Accessed 7 May 2016].

JACOB, R. Hon. Mr. Justice, (2000) *International Intellectual Property litigation in the next millennium.* Case Western Reserve University. http://scholarlycommons.law.case.edu/ [Accessed 8 August 2015].

K

KAGAN. J. (2013) Bricks, mortar, and google: defining the relevant antitrust market for internet-based companies. *NYLS Law Review*. http://www.nylslawreview.com/ [Accessed 17 January 2016].

KAHNEMAN, D., KNETSCH, J.L. and THALER, R.H. (1991). Anomalies: The endowment effect, loss aversion, and status quo bias*. The Journal of Economic Perspectives.* Princeton*.* https://www.princeton.edu/ [Accessed 16 March 2016].

KOELMAN, K. and HUGENHOLTZ, B. (1999) *Online service provider liability for copyright infringement*. University of Amsterdam. http://dare.uva.nl/ [Accessed 27 March 2016].

KNAPP, K. (2015) *Top considerations for choosing a cloud provider*. Search Cloud Computing. http://searchcloudcomputing.techtarget.com/ [Accessed 12 October 2016].

KRAVETS, D. (2012) *Facebook's $9.5 Million 'Beacon' settlement approved*. Wired. https://www.wired.com/ [Accessed 3 April 2016].

KROES, N. (2010) *Cloud computing and data protection*. Europa Press. http://europa.eu/rapid/ [Accessed 8 January 2016].

KROFT, S. (2014) *The data brokers: Selling your personal information*. CBS News. http://www.cbsnews.com/ [Accessed 24 March 2016].

L

LEAGLE. (2008) *In Re U.S. for Order Dir. A Prov. Of Elec, Commune*. Leagle. http://www.leagle.com/. [Accessed 11 January 2016].

LESSIG, L. — LESSIG, L. (2000) Code is law, on liberty in cyberspace. *Harvard Magazine*. http://harvardmagazine.com/. [Accessed 18 February 2016].

LEYDEN, J. — LEYDEN, J. (2006) *AOL sued over search engine data release, privacy breach suit launched*. The Register. https://www.theregister.co.uk/ [Accessed 29 March 2016].

LIGITEC — LIGITEC. (2012) *Lane v. Facebook: Privacy class action settlement requires Facebook to Pay $9.5 Million, but provides no direct benefits to most plaintiffs*. Leon Jacobson ESQ. http://www.nylitigationfirm.com/ [Accessed 21 April 2016].

M

MARTIN, T.D. — MARTIN, T.D. (2011) *Hey! You! Get off my cloud: Defining and protecting the metes and bounds of privacy, security, and property in cloud computing*. Hein online. http://heinonline.org [Accessed 13 June 2015].

MACKENZIE, N. — MACKENZIE, N. (2012) *Working paper, Replacing Section 8(D) of the Competitions Act with an Effects-Based Exclusionary Abuse of Dominance Provision*. Centre for Competition Economics. http://static1.squarespace.com/. [Accessed 25 April 2016].

MACKENZIE, N. (2014) *Rethinking exclusionary abuse in South Africa.* Competition Commission. http://www.compcom.co.za/ [Accessed 22 April 2016].

MANIVAKA, J. et al. — MANIVAKA, J. et al. (2013) *Disruptive technologies: Advances that will transform life, business, and the global economy*. McKinsey. http://www.mckinsey.com/ [Accessed 7 August 2016].

MARSH AND MCLENNAN — MARSH AND MCLENNAN. (2012) *The cloud risk framework, informing decisions about moving to the cloud.* Marsh and McLennan. http://f.datasrvr.com/ [Accessed 8 August 2016].

MAXEY, M. — MAXEY, M. (2008) *Cloud computing public or private? How to choose cloud storage*. Sys-con Media. http://mikemaxey.sys-con.com/ [Accessed 25 May 2015].

MAX PLANCK GROUP — MAX PLANCK GROUP. (2011) *Principles on conflict of laws in intellectual property prepared by the European Max Planck Group on conflict of laws in intellectual property (CLIP)*. Munich Max Planck. http://www.cl-ip.eu/ [Accessed 18 April 2016].

Mc CULLAGH, D. — Mc CULLAGH, D. (2010) *Feds push for tracking cell phones*. CNET news. http://www.cnet.com/ [Accessed 20 January 2016].

Mc GEEVER, M. — Mc GEEVER, M. (2007) *IPR in databases*. http://www.dcc.ac.uk/. [Accessed 20 October 2014].

Mc KENDRICK, J. — Mc KENDRICK, J. (2013) *16 key service quality metrics to boost cloud engagements*. ZDNET. http://www.zdnet.com/ [Accessed 22 August 2016].

MELISSA, E. and SCHMITT-ROSCHMANN, V. — MELISSA, E. and SCHMITT-ROSCHMANN, V. (2010) *German High court zaps anti-terror law*. Cleveland News. www.cleveland.com/world [Accessed 16 January 2016].

MESSIEH, N. — MESSIEH, N. (2011) *Publishers beware: Is CodexCloud the Grooveshark for e-books?* http://thenextWeb.com [Accessed 23 August 2014].

MINISTRY OF JUSTICE

MINISTRY OF JUSTICE. (2012) *Summary of responses, call for evidence on proposed EU data protection legislative framework*. Consult Justice. https://consult.justice.gov.uk/ [Accessed 12 March 2016].

MINISTER OF JUSTICE CANADA

MINISTER OF JUSTICE CANADA. *Personal Information Protection and Electronic Documents Act Codification. S.C. 2000, c. 5 Current to May 12, 2016* (Last amended on June 23, 2015). Ministry of Canada. http://laws-lois.justice.gc.ca/ [Accessed 11 March 2016].

Personal Information Protection and Electronic Documents Act Codification. S.C. 2000, c. 5 Current to May 12, 2016 (Last amended on June 23, 2015). Minister of Justice: http://laws-lois.justice.gc.ca/ [Accessed 11 March 2016].

MIALON, S.H. and BANERJEE, S.

MIALON, S.H. and BANERJEE, S. (2012) *Platform competition and access regulation on the internet*. Research Gate, https://www.researchgate.net/ [Accessed 11 January 2016].

MURLEY, D.

MURLEY, D. (2009) *Technology for everyone: Law libraries in the cloud*. Hein online. http://heinonline.org [Accessed 13 June 2015].

MURPHY, A.

MURPHY, A. (2012) Storing data in the cloud raises compliance challenges. Forbes. http://www.forbes.com/ [Accessed 22 March 2016].

MURPHY, E.

MURPHY, E. (2010) *Databases, doctrine & constitutional criminal procedure*. Hein online. http://heinonline.org (Accessed 13 June 2015).

N

NARAYANAN, A. and SHMATIKOV, V.

NARAYANAN, A. and SHMATIKOV, V. (2007) *Robust de-anonymization of large sparse datasets. Austin*. The University of Texas. https://www.cs.utexas.edu/ [Accessed 2 April 2016].

NARAYANAN, V.

NARAYANAN, V. (2012) *Harnessing the cloud: International Law implications of cloud computing.* http://heinonline.org [Accessed 13 June 2015].

NASUNI

NASUNI. (2013) *White Paper: The state of cloud storage*. NASUNI. http://www6.nasuni.com/ [Accessed 8 February 2016].

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. (2011) *Cloud computing reference architecture.* NIST. http://www.nist.gov/ [Accessed 15 February 2016].

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. (2011) *The NIST definition of cloud* computing SP 800 – 145. CSRC. http://csrc.nist.gov/ [Accessed 28 November 2015].

NETLINGO

NETLINGO. (1996) *Data mining, a.k.a. knowledge discovery in databases (KDD)*. Netlingo. http://www.netlingo.com/word/data-mining.php [Accessed 26 March 2016].

NOL, M.G.

NOL, M.G. (2006) *AOL research publishes 650,000 user queries. Applied Research. Big Data Distributed Systems*. Open Source. http://www.michael-noll.com/ [Accessed 8 February 2016].

NYE, J.S.

NYE, J. S. (2004) *Soft power: The means to success in world politics*. Harvard Belfer Center. http://www.belfercenter.org/ [Accessed 12 May 2016].

O

ODLYZKO, A. — ODLYZKO, A. (2009) *Network neutrality, search neutrality, and the never-ending conflict between efficiency and fairness in markets*. University of Minnesota. http://www.dtc.umn.edu/. [Accessed 14 May 2016].

ORGANISATION FOR ECONIMIC COOPERATION AND DEVELOPMENT — ORGANISATION FOR ECONIMIC COOPERATION AND DEVELOPMENT. (2015) *Chapter 3. Approaches to the protection of Trade Secrets*. OECD. http://www.oecd.org/ [Accessed 23 January 2016].

ORGANISATION FOR ECONIMIC COOPERATION AND DEVELOPMENT. (2009) *Briefing paper for the ICCP technology foresight forum*. OECD. https://www.oecd.org/. [Accessed 15 December 2015]

ORGANISATION FOR ECONIMIC COOPERATION AND DEVELOPMENT. (2003*) Peer Review. Competition Law and Policy in South Africa May 2003*. OECD. http://www.oecd.org/. [Accessed 12 January 2016].

ORGANISATION FOR ECONIMIC COOPERATION AND DEVELOPMENT. (2013) *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data [C (80)58/FINAL, as amended on 11 July 2013 by C (2013)79] extract of Part Two*. OECD. https://www.oecd.org/. [Accessed 8 December 2015].

OFFICE OF THE AUSTRALIAN INFORMATION COMMISSIONER — OFFICE OF THE AUSTRALIAN INFORMATION COMMISSIONER. *Australian Government Privacy Act* 1988: https://www.oaic.gov.au/. [Accessed 6 February 2016].

OFFICE OF GAS AND ELECTRICITY MARKETS — OFFICE OF GAS AND ELECTRICITY MARKETS. (2010) *RPI - X@20 Emerging thinking consultation document – Alternative ex ante and ex post regulatory frameworks*. Gas Department. Office of Gas and Electricity Markets. https://www.ofgem.gov.uk/. [Accessed 2 April 2016].

OFFICE OF THE PRIVACY COMMISSION — OFFICE OF THE PRIVACY COMMISSION of Canada. (n.d.) *Cloud computing for small and medium sized enterprises*. OIPC. https://www.oipc.bc.ca/. [Accessed 11 December 2015].

OFFICE OF THE PRIVACY COMMISSIONER for Personal Data, Hong Kong. (n.d.) *Information leaflet on cloud computing.* PCDP. https://www.pcpd.org.hk/ [Accessed 29 September 2015].

OHM, P. — OHM, P. (2010) Broken promises of privacy: Responding to the surprising failure of anonymization. *UCLA Law Review*. http://www.uclalawreview.org/ [Accessed 11 March 2016].

OMSTEIN, C. — OMSTEIN, C. (2015) How private is sensitive abortion information? *Pacific Standard.* https://psmag.com/. [Accessed 28 March 2016].

ORACLE — ORACLE. (n.d.) *Oracle software as a service agreement V 121509*. Oracle. http://www.oracle.com/ [Accessed 14 April 2016].

OSTERUD, E. — OSTERUD. E. (2013) EU Competition Law - abuse of dominance (Article 102 TFEU). University of Oslo. http://www.uio.no/ [Accessed 23 April 2016].

OUT-LAW — OUT-LAW. (2008) *Database rights: the basics*. Out-Law. http://www.out-law.com [Accessed 14 May 2015].

P

PARLIAMENT OF SOUTH AFRICA — *Parliament of the Republic of South Africa* http://www.parliament.gov.za/ [Accessed 11 May 2016].

PEARSON, S. — PEARSON, S. (2011) *Towards accountability in the cloud*. HP. http://www.hpl.hp.com/ [Accessed 27 March 2016].

PETRO, N. — PETRO, N. (2007) Software as a Service. *GP Solo Magazine.* http://www.americanbar.org/ [Accessed 27 November 2015]

PICKER, R.C. — PICKER, R.C. (2008) *Competition and privacy in Web 2.0 and the cloud*. SSRN. http://papers.ssrn.com/ [Accessed 4 February 2016].

POCAR, F. et al. (eds.) — POCAR, F. et al. (eds.) (2012) *Choice-of-Court Agreements in Favour of Third States' Jurisdiction in Light of the Suggestions by Members of the European Parliament, Recasting Brussels I*. Academia. http://www.academia.edu/ [Accessed 25 March 2016].

POT, J. — POT, J. (2011) *Codex cloud: Upload your books & read them online along with other people's uploads*. (http://www.makeuseof.com) [Accessed 23 August 2014].

R.

RASHBAUM, K.N., BENNET, B. and BEAUMON, T.H. — RASHBAUM, K.N., BENNET, B. and BEAUMON, T.H. (2014) *Outrun the Lions: A practical framework for analysis of legal issues in the evolution of cloud computing*. http://heinonline.org [Accessed 13 June 2015].

RASHDI, Z.A., DICK, M. and STONY, I. — RASHDI, Z.A., DICK, M. and STONY, I. (2015) *A conceptual framework for accountability in cloud computing service provision*. Australasian Conference on Information Systems (ACIS). https://acis2015.unisa.edu.au/ [Accessed 25 April 2016].

REED, C. — REED, C. (2010) *Information "ownership" in the cloud*. SSRN. http://papers.ssrn.com/ [Accessed 14 March 2016].

REIN, W. — REIN, W. (2011) *The changing meaning of "personal data"*. Lexology. http://www.lexology.com/ [Accessed 22 February 2016].

RICKY, M. and MAGALHAES, M.L. — RICKY, M. and MAGALHAES, M.L. (2015) *Cloud data jurisdiction: The provider, the consumer and data sovereignty*. Cloud Computing. http://www.cloudcomputingadmin.com/ [Accessed 17 February 2016]

ROBERTS, S. — ROBERTS, S. (2011) *'Administrability and business certainty in abuse of dominance enforcement: An economist's review of the South African record'*. Compcom. http://www.compcom.co.za/ [Accessed 8 August 2016].

ROBERT, S. (2013). *Privacy, technology and national security. An overview of intelligence collection.* Office of the Director on National Intelligence. Brookings Institution. https://www.dni.gov/ [Accessed 12 July 2016].

ROCET, J.C. and TIROLE, J. — ROCET, J.C. and TIROLE, J. (2003) *Platform competition in two-sided markets*. Research Center for Humanities and Social Sciences. http://www.rchss.sinica.edu.tw/ [Accessed 22 May 2106].

S

SAS — SAS. (n.d.) *Big data, what it is and why it matters*. SAS. https://www.sas.com/. [Accessed 29 May 2016].

SCHOFIELD, A. and ABRAHAMS, L. — SCHOFIELD, A. and ABRAHAMS, L. (2015) *Research study on the use of cloud services in the South African Government.* Joburg Centre for Software Engineering. Wits University. https://www.jcse.org.za/ [Accessed 15 May 2016].

SCHWARTZ, P.M.	SCHWARTZ, P.M. (2013) *Information privacy in the cloud*. Berkeley Law. http://scholarship.law.berkeley.edu/ [Accessed 20 March 2016].
SCHWARTZ, P.M. and SOLOVE, D. J.	SCHWARTZ, P.M. and SOLOVE, D.J. (2014) *Reconciling Personal Information in the United States and European Union*. Berkeley University., http://scholarship.law.berkeley.edu/ [Accessed 7 February 2016].
	SCHWARTZ, P.M. and SOLOVE, D.J. (2011) *The PII problem: Privacy and a new concept of personally identifiable information*. SSRN. http://papers.ssrn.com/. [Accessed 19 March 2016].
SCIENCE COMMONS	SCIENCE COMMONS. (2005) *Towards a science commons*. Science commons. http://sciencecommons.org [Accessed 23 August 2014].
SCOTT, R.J.	SCOTT, R.J. (2012) *Understanding the legal risks of cloud computing navigating the network security and data privacy issues associated with cloud services*. Thomas Reuters Aspatore. https://www.scottandscottllp.com/ [Accessed 15 May 2015].
SEAGATE	SEAGATE. (n.d.) Data centre management: Trends and challenges. SEAGATE. http://www.seagate.com/. [Accessed 16 January 2016].
SEGALL, S.	SEGALL, S. (2013) *Jurisdictional challenges in the United States Government's move to cloud computing technology*. Hein online. http://heinonline.org [Accessed 13 June 2015].
SHELTON, T.	SHELTON, T. (2013) *Business models for the social mobile cloud transform your business using social media, mobile internet and cloud computing*. Hoboken New Jersey: John Wiley and Sons Inc., http://adnanalhashmi.weebly.com/ [Accessed 14 October 2016].
SILALASHI, J.M.	SILALASHI, J.M. (2011) *Drafting a cloud computing contrac*t. Academia. http://www.academia.edu/ [Accessed 12 March 2016].
SINGEL, R.	SINGEL, R. (2009) *Netflix spilled your Brokeback Mountain secret, Lawsuit Claims.* Wired. https://www.wired.com/ [Accessed 28 March 2016].
SKYHIGH	SKYHIGH. (2015) *Cloud adoption and risk report Q2 2015*. SKYHIGH. https://uploads.skyhighnetworks.com/ [Accessed 7 May 2016].
SLUIJS, J.P.	SLUIJS, J.P. (2012*)* Network neutrality and internet market fragmentation*.* TILEC Discussion Paper No. 2012-015, *Common Market Law Review.* 49 (5), 2012. https://papers.ssrn.com/ [Accessed 24 April 2016].
SLUIJS, J.P., LAROUCHE, P. and SAUTER, W.	SLUIJS, J.P., LAROUCHE, P. and SAUTER, W. (2012) *Cloud computing in the EU policy sphere interoperability, vertical integration and the internal market*. Tilburg Law and Economics Center (TILEC). https://www.jipitec.eu/issues/jipitec-3-1-2012/3320/sluijs.pdf [Accessed 24 February 2016].
SMITH, B.	SMITH, B. (2010) *Building confidence in the cloud: A proposal for industry and government action for Europe to reap the benefits of cloud computing*. European Commission EC Justice News. http://ec.europa.eu/ [Accessed 16 September 2015].
	SMITH, B. (2010) *Cloud computing for business and society at the Brookings Institution*. Brookings Institution. Http://www.brookings.edu/ [Accessed 23 May 2015].

SOLOMECKE, C. — SOLOMECKE, C. (2013) *The legal aspects of cloud computing under Copyright law*. WBS Law. https://www.wbs-law.de/ [Accessed 12 April 2016].

SOUTH AFRICAN LAW COMMISSION — SOUTH AFRICAN LAW COMMISSION. (1998) *Report Project 47. Unreasonable stipulations in contracts and the rectification of contracts*. Justice Department. http://www.justice.gov.za/ [Accessed 3 February 2016].

SOUTH AFRICAN LAW REFORM COMMISSION — SOUTH AFRICAN LAW REFORM COMMISSION. (2005) *Privacy and Data Protection Discussion Paper 109 Project*. Justice Department. http://www.justice.gov.za/ (Accessed 6 January 2016).

SOUTH AFRICAN LEGAL INFORMATION INSTITUTE — SOUTH AFRICAN LEGAL INFORMATION INSTITUTE. (2014) *POPI - Is South Africa keeping up with international trends?* SAFLLI. http://www.saflii.org/ [Accessed 11 March 2016].

STONE, B. and STELTER, B. — STONE, B. and STELTER, B. (2009) Facebook withdraws changes in data use. *New York Times*. http://www.nytimes.com/ [Accessed 22 April 2016].

STONEBRAKER, M. — STONEBRAKER, M. (n.d.) "One Size Fits All": An idea whose time has come and gone. Computer Science and Artificial Intelligence Laboratory, MIT. https://cs.brown.edu/~ugur/fits_all.pdf [Accessed 12 February 2016].

STREEL, A. — STREEL, A. (2012) *Where should the European Union intervene to foster the internal market for eComms?* SSRN. https://papers.ssrn.com/ [Accessed 7 April 2016].

SVANTESSON, D.J.B. — SVANTESSON, D.J.B. (2014) *Delineating the reach of internet intermediaries' content blocking – "ccTLD Blocking", "Strict Geo-location Blocking" or a "Country Lens Approach"?* 11 (2). Scripted. https://script-ed.org/. [Accessed 12 April 2016].

SWEENEY, L. — SWEENEY, L. (2013) *Discrimination in online ad delivery.* SSRN. http://papers.ssrn.com/ [Accessed 23 March 2016].

SZOLDRA, P. — SZOLDRA, P. (2016) *This is everything Edward Snowden revealed in one year of unprecedented top-secret leaks*. Business Insider. http://www.businessinsider.com/ [Accessed 28 October 2016].

T

TAYLOR, S. — TAYLOR, S. (2013) *Reding warns against identity changes to bypass data privacy. Commissioner gets tough on pseudonymous data*. European Voice. http://www.politico.eu/ [Accessed 15 March 2016].

TIAN, G. — TIAN, G. (2014) *Don't sue us for search: Google's unnecessary safe harbour appeal*. University of Hertfordshire. http://www.herts.ac.uk/ [Accessed 15 February 2016].

TRICHKOVSKAX, C. — TRICHKOVSKAX, C. (2011) *Legal and privacy challenges of social networking sites*. Duo UIO. https://www.duo.uio.no/ [Accessed 24 January 2016].

TRIMBLE, M. — TRIMBLE, M. (2014) *Advancing national intellectual property policies in a transnational context*. University of Nevada. School of Law. https://papers.ssrn.com/ [Accessed 3 April 2016].

TRIMBLE, M. (2012) *The future of cybertravel: Legal implications of the evasion of geolocation*. Las Vegas. University of Nevada. http://scholars.law.unlv.edu/ [Accessed 18 May 2016].

2TWENTY4CONSULTING — 2TWENTY4CONSULTING. (2017) *GDPR and cloud service providers*. Legal Technology. https://www.legaltechnology.com/ [Update-Accessed 18 March 2017].

U

UNITARY PATENT — *Unitary patent: Uniform protection across 26 EU countries*. EC Europa. https://ec.europa.eu/ [Accessed 12 February 2016].

UNITED KINGDOM — *United Kingdom Data Protection Act of 1998. United Kingdom Government.* http://www.legislation.gov.uk/ [Accessed 12 February 2016].

The Copyright and Rights in Databases Regulations 1997 No. 3032 as amended. http://www.legislation.gov.uk/. (Accessed 16 March 2016).

Government of United Kingdom. (2017) *Countries of the EU and EEA, countries in the EU and EEA, The European Union (EU) is an economic and political union of 28 countries.* Government of the United Kingdom. https://www.gov.uk/ [Accessed 12 March 2017].

UNITES STATES — *Chapter Seventeen Intellectual Property Rights.* (2003) Office of the United States Trade Representative. https://ustr.gov/sites/. [Accessed 29 September 2016].

Circular 92. Copyright Law of the United States and Related Laws Contained in Title 17 of the United States Code. December 2016. Copyright Government. https://www.copyright.gov/ [Accessed 22 December 2016].

The Digital Millennium Copyright Act 1998 (DCMA) (USA). Copyright Gov. http://www.copyright.gov [Accessed 12 April 2016].

Guidance on the Protection of Personal Identifiable Information (PII). United States Department of Labour. https://www.dol.gov/ [Accessed 7 February 2016].

The Health Insurance Portability and Accountability Act of 1996. GPO. https://www.gpo.gov/ [Accessed 29 March 2016].

Safe Harbour Agreement. http://2016.export.gov/safeharbor/ [Accessed 22 November 2016].

Section 164.514a. Government Publishing Office. https://www.gpo.gov/ [Accessed 12 February 2016].

The USA PATRIOT Act 2006: Preserving Life and Liberty (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism). Department of Justice. https://www.justice.gov/ [Accessed 9 July 2016].

The USA PATRIOT Act: MYTH VS. REALITY. Justice Department. https://www.justice.gov/ [Accessed 25 February 2016].

United States Department of Labour. *Guidance on the Protection of Personal Identifiable Information (PII)*. Department of Labour. https://www.dol.gov/. [Accessed 12 April 2016].

UNIVERSITY

University of Cambridge Research. (2013) *Digital records could expose intimate details and personality traits of millions*. Cambridge Press. http://www.cam.ac.uk/ [Accessed 12 March 2016].

University of Cambridge. *Centre for Intellectual Property and Information Law. Ladbroke v. William Hill [1964] 1 All ER 465.* http://www.cipil.law.cam.ac.uk/. [Accessed 16 March 2016].

University of Cape Town. (n.d.) *Sources of law. E-transactions law*. http://www.etransactionslaw.uct.ac.za/ [Accessed 15 April 2016].

University of Harvard. (n.d.) *Basic guidelines for contracts and contract risk management*. Harvard University. http://rmas.fad.harvard.edu/ [Accessed 22 August 2016].

W

WALKER, S. and GREENE C.

WALKER, S. and GREENE C. (2007) *'What constitutes a material breach'*. The Lawyer. https://www.thelawyer.com/ [Accessed 12 August 2016].

WATROUS, L.

WATROUS, L. (2016) The cloud and the race to zero: Amazon and Google go at I.T. *Huffington Post*. http://www.huffingtonpost.com/ [Accessed 14 December 2016].

WEBER, R. H.

WEBER, R.H. (2010) *Internet of things – new security and privacy challenges*. Semantic Scholar. https://pdfs.semanticscholar.org/ [Accessed 18 January 2016].

WEBER, R.H. and GROSZ, M.

WEBER, R.H. and GROSZ, M. (2008) *Legitimate governing of the internet.* Syracuse University. https://listserv.syr.edu/ [Accessed 14April 2016].

WEITZNER, D.J. et al.

WEITZNER, D.J. et al. (200) *Information accountability.* MIT Computer Science and Artificial Intelligence Laboratory. http://dig.csail.mit.edu/ [Accessed 22 March 2016].

WHITTAKER, Z.

WHITTAKER, Z. (2014) *Dropbox under fire for 'DMCA takedown' of personal folders, but fears are vastly overblown*. ZDnet. http://www.zdnet.com/. [Accessed 14 April 2016].

WIDMER, U.

WIDMER, U. (2009) *Telecommunications Media & Technology. Cloud computing – ICT as a service*. Who's Who Legal http://whoswholegal.com/ [Accessed 4 May 2015].

WILCOX, M.

WILCOX, M. (2016) *The real reason why Google Flu Trends got big data analytics so wrong*. Forbes. http://www.forbes.com/ [Accessed 20 March 2016].

WILSON, S.

WILSON, S. (2014) *Facebook's facial recognition technology is a massive surveillance project*. ZDNET. http://www.zdnet.com/. [Accessed 21 November 2016].

WORLD INTELLECTUAL PROPERTY ORGANIZATION (WIPO)

WIPO Copyright Treaty. (Adopted in Geneva on December 20, 1996) WIPO Int. http://www.wipo.int/. [Accessed 17 January 2016].

WIPO. (1996) *Agreed statements concerning the WIPO Copyright Treaty*. WIPO. http://www.wipo.int/ [Accessed 26 February 2016].

WIPO. (2014) *Director Gurry Speaks on Naming New Cabinet, Future of WIPO.* IP watch. http://www.ip-watch.org/ [Accessed 21 April 2016].

WIPO. *Performances and Phonograms Treaty (WPPT) (adopted in Geneva on December 20, 1996)*. WIPO. http://www.wipo.int/ [Accessed 12 April 2016].

WIPO. *Main provisions and benefits of the Marrakesh Treaty (2013)*. WIPO. http://www.wipo.int/ [Accessed 12 April 2016].

WIPO. *Bern Convention Article* 5(4) (c). http://www.wipo.int/ [Accessed 19 March 2016].

WIPO. *Bern Convention Contracting Parties*. http://www.wipo.int/ [Accessed 20 March 2016].

WIPO. *Country overviews*. http://www.wipo.int/ [Accessed 12 April 2015].

WIPO. *Agreement on Trade-related Aspects of Intellectual Property Rights*. https://www.wto.org/. [Accessed 5 January 2016].

WIPO. *Marrakesh treaty to facilitate access to published works for persons who are blind, visually impaired or otherwise print disabled*. WIPO. http://www.wipo.int/ [Accessed 12 April 2016].

WIPO. *Agreement on Trade-related Aspects of Intellectual Property Rights (TRIPS) World Trade Organization, 1994*. World Trade Organization. https://www.wto.org/. [Accessed 5 January 2016].

WIPO. *Agreement on Trade-related Aspects of Intellectual Property Rights (TRIPS) agreement 1995*, World Trade Organization. https://www.wto.org/. [Accessed 12 January 2015].

WIPO. *Paris Convention for the Protection of Industrial Property 1883 (March 20, 1883, as amended on September 28, 1979)*. WIPO. http://www.wipo.int/ [Accessed 12 January 2015].

Z

ZUCKERBERG, M. ZUCKERBERG, M. (2007) *Thoughts on Beacon.* Facebook. https://www.facebook.com/ [Accessed 5 April 2016].

Reference list

A

ABBOT, F.M. (2009) Seizure of generic pharmaceuticals in transit based on allegations of patent infringement: A threat to international trade, development and public welfare*. World Intellectual Property Organization Journal (WIPO),* 1. p. 43, SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1535521 [Accessed 5 April 2016].

A4CLOUD. (n.d.) *Cloud accountability project*. A4CLOUD. http://www.a4cloud.eu/sites/default/files/A4cloud_brochure_web.pdf [Accessed 22 April 2016].

ADAM and ADAMS (2012). Senwes: A victory for the Competition Commission but a potential Pandora's Box. Polity. http://www.polity.org.za/article/senwes-a-victory-for-the-competition-commission-but-a-potential-pandoras-box-2012-05-10 [Accessed 29 April 2016].

THE ADVISORY INSTITUTE. (2013) *The cloud takes shape: Global cloud survey|the implementation challenge*. KPMG. http://www.kpmg-institutes.com/institutes/advisory-institute/articles/2013/02/cloud-takes-shape.html [Accessed 18 April 2016].

Agreement on Trade-related Aspects of Intellectual Property Rights (TRIPS) World Trade Organization, 1994. WTO. https://www.wto.org/english/docs_e/legal_e/27-trips.pdf. [Accessed 5 January 2016].

Agreement on Trade-related Aspects of Intellectual Property Rights (TRIPS) agreement 1995, World Trade Organization. https://www.wto.org/english/docs_e/legal_e/27-trips.pdf [Accessed 12 January 2015].

AGRELL, P. and BOGETOFT, P. (2002) *Ex-post regulation pre-project 2 – Final Report.* SUMICSID. *http://www.sumicsid.com/reg/papers/fp2_final.pdf* [Accessed 2 April 2016].

ALEXIADIS, P. (2012) *Balancing the application of ex post and ex ante disciplines under community law in electronic communications markets: Square pegs in round holes.* Gibson Dunn. http://www.gibsondunn.com/publications/Documents/Alexiadis-balancingtheApplicationofExPostandExAnteDisciplines.pdf [Accessed 14 April 2016].

ALLENS. (2004) *Australia-United States Free Trade Agreement: impacts on IP, communications and technology.* ALLENS. (http://www.allens.com.au/pubs/ip/foftafeb04.htm#Intel [Accessed 27 September 2016].

American Broadcasting Cos., Inc., et al. v Aereo, Inc., FKA Bamboom Labs, Inc. Certiorari to the United State Court of Appeals for the Second Circuit. No. 13–461. Argued April 22, 2014—Decided June 25, 2014. Supreme Court of United States. https://www.supremecourt.gov/opinions/13pdf/13-461_l537.pdf [Accessed 7 August 2016].

ANDERSON, G.N. (2010) Are individuals waking up to the privacy implications of social-networking sites? *European Intellectual Property Review*, 32 (3).

Anonymous. (n.d.) *Extra protection for digital media: Digital Millennium Copyright Act, Region Coding.* University of Florida. http://www.clas.ufl.edu/llc/copyright/RightsDMCA.html [Accessed 5 April 2016].

Anonymous. (2013) *A428 - TLC: Antitrust, Telecom Italia abused its dominant position in the network infrastructure.* Autorità Garante Della Concorrenza e Del Mercato.

http://www.agcm.it/en/newsroom/press-releases/2052-a428-tlc-antitrust-telecom-italia-abused-its-dominant-position-in-the-network-infrastructure-total-fine-of--103794-million.html [Accessed 17 May 2016].

Anonymous. (2016) *Terms of service*, Dropbox. https://www.dropbox.com/ [Accessed 12 December 2016]. Section 'Services "AS IS".

Apple Inc. (n.d.) *iCloud Terms and conditions.* Apple Legal. http://www.apple.com/legal/internet-services/icloud/en/terms.html [Accessed 22 August 2016].

Article 29 Data Protection Working Party, 2009*, Opinion 5/2009 on online social networking,* EC Europa, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_en.pdf [Accessed 22 April 2016].

Article 29 Data Protection Working Party Opinion 05/2012 on Cloud Computing Adopted July 1 2012, EC Europa. *http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf* [Accessed 6 January 2016].

ASAY, M. (2009) *Facebook changes terms of service to control more user data*. CNET. http://www.cnet.com/news/facebook-changes-terms-of-service-to-control-more-user-data/ [Accessed 21 April 2016].

Australian Government. (2014) *Deregulation. The Australian Government is reducing the regulatory burden for business and the community*. Department of Communications. https://www.communications.gov.au/deregulation [Accessed 21 September 2016].

Australian Government Privacy Act 1988. https://www.oaic.gov.au/privacy-law/privacy-act/ [Accessed 6 February 2016].

B

Bankovic and Others v. Belgium and Others (Application No. 52207/99). Grand Chamber 1. Decision of 12 December 2001. ECHR. http://echr.coe.int/Documents/Reports_Recueil_2001-XII.pdf [Accessed 4 May 2016].

BARBARO, M. and ZELLER, T. (2006) *A face is exposed for AOL searcher no. 4417749.* Research Gate. https://www.researchgate.net/publication/265660320_A_Face_is_exposed_for_AOL_searcher_no_4417749 [Accessed 28 March 2016].

Basic guidelines for contracts and contract risk management. Harvard University. http://rmas.fad.harvard.edu/basic-guidelines-contracts-and-contract-risk-management [Accessed 22 August 2016].

BAUDIN, C. et al. (2015) *Practical guide to Platform as a Service PaaS.* Cloud Standards Customer Council. CSCC. http://www.Cloud-council.org/CSCC-Practical-Guide-to-PaaS.pdf. [Accessed 15th February 2016].

BAVASSO, A. (2009) *Recoupment in predatory pricing: France Telecom v. Commission.* Allan and Overy. http://www.allenovery.com/publications/en-gb/Pages/Recoupment-in-predatory-pricing--France-Telecom-v-Commission.aspx [Accessed 8 May 2016].

BEREC. (2012) *Guidelines for quality of service in the scope of net neutrality.* Body of European Regulators of Electronic Communications. BEREC. http://berec.europa.eu/eng/document_register/subject_matter/berec/regulatory_best_practices/guidelines/1101-berec-guidelines-for-quality-of-service-in-the-scope-of-net-neutrality [Accessed 10 February 2016].

BERMAN, P.S. (2005) *Towards a cosmopolitan vision of conflict of laws: redefining governmental interests in a global era.* George Washington University Law School. http://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=1084&context=faculty_publications [Accessed 3 May 2016].

Bern Convention Contracting Parties. World Intellectual Property Organization, WIPO. http://www.wipo.int/treaties/en/ShowResults.jsp?treaty_id=15 [Accessed 20 March 2016].

Berne Convention for the Protection of Literary and Artistic Works Paris 1971 (Act of July 24, 1971, as amended on September 28, 1979), World Intellectual Property Organization. http://www.wipo.int/treaties/en/text.jsp?file_id=283698 [Access 12 January 2015].

BLACK, J. (2008) Constructing and contesting legitimacy and accountability in polycentric regulatory regimes. *Journal Regulation and Governance*. Blackwell Publishing Asia Pty Ltd.

BORAN, M. (2011) Stream of online TV shows and movies starts flowing. *Irish Times*. http://www.irishtimes.com/business/technology/stream-of-online-tv-shows-and-movies-starts-flowing-1.6482 [Accessed 23 April 2016].

BOREK, C. et al. (2013) *Lost in the clouds: The impact of copyright scope on investment in cloud computing ventures.* IDEI. http://idei.fr/sites/default/files/IDEI/documents/tnit/papers/2013/lost_in_the_clouds.pdf [Accessed 21 April 2016].

BORT, J. (2015) Google just took the lead in the dangerous game called 'race to zero'. *Business Insider.* http://www.businessinsider.com/google-leads-cloud-storage-race-to-zero-2015-5 [Accessed 30 April 2016].

BOSHOFF, W.H. (2014) *Antitrust market definition: rationale, challenges and opportunities in South African competition policy.* Competition Commission. http://www.compcom.co.za/wp-content/uploads/2014/09/Boshoff-Market-Definition.pdf [Accessed 15 January 2016].

The Boston Consulting Group. (2012) *The value of digital identity.* Liberty Global. http://www.libertyglobal.com/PDF/public-policy/The-Value-of-Our-Digital-Identity.pdf [Accessed 11 February 2016].

BRADSHAW, S., MILLARD, C. and WALDEN, I. (2011) *The terms they are a -changin'. Watching cloud contracts take shape.* The Center for Technology Innovation. The Brookings Institution. https://www.brookings.edu/wp-content/uploads/2016/06/03_cloud_computing_contracts.pdf [Accessed 12 August 2016].

BRADSHAW, S. MILLARD, C. and WALDEN, I. (2010) *Contracts for clouds: Comparison and analysis of the terms and conditions of cloud computing services.* SSRN. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1662374 [Accessed 11 March 2016].

The British Horseracing Board Ltd v. William Hill Organisation Ltd, C-203/02, 2004, Reference for a preliminary ruling concerns the interpretation of Article 7 and Article 10(3) of Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases (OJ 1996 L 77, p. 20, 'the directive'), 2004. Curia Europa. http://curia.europa.eu/juris/showPdf.jsf?text=&docid=49633&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=1452357 [Accessed 27 March 2016].

BRASSEY, M. et al. (2002) *Competition Law.* Cape Town: Juta Publishing.

BROWN, G. (2010) *Brown defends DNA Database and CCTV roll-out.* Truth Alliance Network. http://truthalliance.net/Archive/News/tabid/67/ID/4708/Brown-defends-DNA-database-and-CCTV-roll-out-as-he-rejects-Camerons-claim-that-Britain-has-a-broken-society.aspx [Accessed 4 February 2016].

BUCCAFUSCO, C. and SPRIGMAN, C. (2010) *Valuing intellectual property: An experiment*. SSRN. Social Science Research Network. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1568962 [Accessed 16 March 2016].

BULLER, D.J. and WITTOW, M.H. (2010) *Cloud computing: Emerging legal issues, data flows,* the mobile user. K and L Gates. http://www.klgates.com/files/upload/Journal_Internet_Law.pdf [Accessed: 13 June 2015].

BUTLER, B. (2013) *Gartner: Top 10 cloud storage providers.* Net Work World. http://www.networkworld.com/article/2162466/cloud-computing/gartner-top-10-cloud-storage-providers.html [Accessed 21 March 2016].

C

CABINET OFFICE. (2011) *Government ICT strategy.* Cabinet Office London. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/85968/uk-government-government-ict-strategy_0.pdf [Accessed 21 May 2016].

Cartoon Network et al. v. Cablevision et al. 536 F.3d 121 (2d Cir. 2008). Berkman Center for Internet & Society. http://cyber.law.harvard.edu/people/tfisher/IP/2008%20Cartoon%20Abridged.pdf. [Accessed 15 February 2016].

Case 130-79 eDate Advertising GmbH v. X (C-509/09) and Olivier Martinez and Robert Martinez v. MGN Limited (C-161/10). References for a preliminary ruling: Bundesgerichtshof - Germany and Tribunal de Grande instance de Paris - France. Regulation (EC) No. 44/2001 - Jurisdiction and the enforcement of judgments in civil and commercial matters - Jurisdiction 'in matters relating to tort, delict or quasi-delict' - Directive 2000/31/EC - Publication of information on the internet - Adverse effect on personality rights - Place where the harmful event occurred or may occur - Law applicable to information society services. Joined cases C-509/09 and C-161/10. Curie Europa. http://curia.europa.eu/juris/liste.jsf?&num=C-509/09 [Accessed 12 May 2016].

Case C-5/11 criminal proceedings against Titus Alexander Jochen Donner [2012] ecr Judgment of the Court (Fourth Chamber) of 21 June 2012. Criminal proceedings against Titus Alexander Jochen Donner. Reference for a preliminary ruling: Bundesgerichtshof - Germany. Free movement of goods - Industrial and commercial property - Sale of reproductions of works in a Member State in which the copyright on those works is not protected - Transport of those goods to another Member State in which the infringement of the copyright is sanctioned under criminal law - Criminal proceedings against the transporter for aiding and abetting the unlawful distribution of a work protected by copyright law. Curia Europa.

http://curia.europa.eu/juris/document/document.jsf?text=&docid=124189&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=867573 [Accessed 21 January 2016].

CATTEDDU, D. and HOGBEN, G. (2009) *Cloud computing, benefits, risks and recommendations for information security.* The European Network and Information Security Agency. (ENISA). https://resilience.enisa.europa.eu/cloud-security-and-resilience/publications/cloud-computing-benefits-risks-and-recommendations-for-information-security [Accessed 22 August 2016].

CEPIS. (2013) *Statement on the draft EU General Data Protection Regulation.* CEPIS Council. http://www.cepis.org/media/EUDataProtection.20131.pdf [Accessed 24 February 2016].

Chapter 2 Bill of Rights 1996. Department of Justice. http://www.justice.gov.za/legislation/constitution/SAConstitution-web-eng-02.pdf [Accessed 25 March 2016].

Chapter Seventeen Intellectual Property Rights. (2003) Office of the United States Trade Representative. https://ustr.gov/sites/default/files/uploads/agreements/fta/chile/asset_upload_file912_4011.pdf [Accessed 29 September 2016].

CHEUNG, A.S.Y. and WEBER, R.H. (2015) *Privacy and the legal issues in cloud computing*. Cheltenham: Edward Elgar Publishing.

City of Los Angeles. (2009) *Professional Services Contract between the City of Los Angeles and Computer Science Corp. for the SaaS E-mail and Collaboration Solution.* SECS. https://sites.google.com/a/lageecs.lacity.org/la-geecs-blog/home/faqs-1/City_SECSContract-20091110.doc [Accessed 24 February 2016].

Circular 92. Copyright Law of the United States and Related Laws Contained in Title 17 of the United States Code. December 2016. Copyright Government. https://www.copyright.gov/title17/title17.pdf [Accessed 22 December 2016].

CLARKE, G. (2011) *'Apple's iCloud runs on Microsoft and Amazon services: Who says Azure isn't cool and trendy now'.* The Register. http://www.theregister.co.uk/2011/09/02/icloud_runs_on_microsoft_azure_and_amazon/ [Accessed 2 August 2016].

CLOUD STANDARDS CUSTOMER COUNCIL. (2016). Public cloud service agreements: What to expect and what to negotiate, Version 2.0.1. CSCC. http://www.cloud-council.org/deliverables/CSCC-Public-Cloud-Service-Agreements-What-to-Expect-and-What-to-Negotiate.pdf [Accessed 22 September 2016].

Cloud Security Alliance. (2011) *Security guidance for critical areas of focus in cloud computing V3.0*, Cloud Security Alliance CSA. https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf. [Accessed 15 December 2015].

COATES, J. (2010) *The Australian Parliament goes CC – with v3.0*, Creative Commons. http://creativecommons.org.au/tag/australian-federal-government/ [Accessed 10 May 2016].

COHEN, J.E. (1998) *Copyright and the jurisprudence of self-help.* George Town University Law Center. http://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=1817&context=facpub [Accessed 23 February 2016].

COLUMBUS, L. (2013) *Making cloud computing pay.* Forbes. https://www.forbes.com/sites/louiscolumbus/2013/04/10/making-cloud-computing-pay-2/#abae0e45656d [Accessed 23 April 2016].

Commission Decision of 28 January 1992 establishing transitional measures for trade in bovine animals in relation to the cessation of vaccination against foot-and-mouth disease and revoking Decisions 91/13/EEC and 91/177/EEC. Eur-Lex. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31992D0105&from=EN [Accessed 23 March 2016].

Commission Regulation (EU) No. 330/2010 of 20 April 2010 on the application of Article 101(3) of the Treaty on the Functioning of the European Union to categories of vertical agreements and concerted practices. Eur-Lex. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:102:0001:0007:EN:PDF. [Accessed 20 April 2016].

Commission v. Senwes Case CCT 61/11 [2012] ZACC 6 and the Tribunal has found Telkom guilty of contravening sections 8(b) and 8(d)(i) on 7 August 2012 in Commission v. Telkom SA Ltd case 11/CR/Feb04. Competition Tribunal. http://www.comptrib.co.za/cases/high-court-judgement/retrieve_case/1397 [Accessed 29 April 2016].

Committee on Civil Liberties. Justice and Home Affairs. (2013) on the proposal for a regulation of the European Parliament and of the Council 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) (COM (2012)0011 – C7-0025/2012 – 2012/0011(COD)., European Parliament. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2F%2FEP%2F%2FTEXT%2BREPORT%2BA7-2013-0402%2B0%2BDOC%2BXML%2BV0%2F%2FEN&language=EN [Accessed 10 March 2016].

Communication from the Commission to the European Parliament and the Council, (2013) On the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU, EC Europa. *http://ec.europa.eu/justice/data-protection/files/com_2013_847_en.pdf* [Accessed 15 July 2016].

Competition Act No. 89 of 1998 (Date of commencement of sections 1-3, 6, 11, 19-43, 78, 79 & 84 on 30 November 1998. The remaining sections of the Act commenced on 1 September 1999.) Competition Commission. http://www.compcom.co.za/wp-content/uploads/2014/09/pocket-act-august-20141.pdf [Accessed 15 March 2016].

Competition Commission v. BMW South Africa (Pty) Ltd t/a BMW Motorrad (97/CR/Sep08) [2010] ZACT 21 (17 March 2010). South African Legal Information Institute. http://www.saflii.org/za/cases/ZACT/2010/21.html [Accessed 7 March 2016].

Competition Tribunal of South Africa. (2015) *Large Merger – Vodacom (Proprietary) Limited/Neotel (Proprietary) Limited.* Competition Tribunal. http://www.comptrib.co.za/publications/case-documents/large-merger-vodacom-proprietary-limited-neotel-proprietary-limited/ [Accessed 18 April 2016].

The Constitution of the Republic of South Africa No. 108 0f 1996, as amended. Government of South Africa. http://www.gov.za/sites/www.gov.za/files/images/a108-96.pdf [Accessed 21 February 2016].

Copyright Act, 1978 (Act No. 98 of 1978 as amended up to Copyright Amendment Act 2002) 2002. National Legislator. http://www.nlsa.ac.za/downloads/Copyright%20Act.pdf [Accessed 3 May 2015].
Copyright Act 1968, Commonwealth Consolidated Acts. http://www.austlii.edu.au/au/legis/cth/consol_act/ca1968133/ [Accessed 22 September 2016].

Copyright Law of the United States and Related Laws Contained in Tıtle 17 of the United States Code. Copyright Gov. https://www.copyright.gov/title17/title17.pdf [Accessed 17 September 2016].

Copyright Amendment Bill b3 2017. DOTI. http://www.gov.za/documents/copyright-amendment-bill-b13-2017-16-may-2017-0000 [Accessed 22 July 2017].

Copyright Amendment Act 125 of 1992, http://www.gov.za/sites/www.gov.za/files/a125_1992.pdf. [Accessed 3 May 2015].

Copyright Amendment Draft Bill, 2015, Department of Trade and Industry. http://www.gov.za/sites/www.gov.za/files/39028_gon646c.pdf [Accessed 10 April 2016].

The Copyright and Rights in Databases Regulations 1997 No. 3032 as amended. Legislation UK. http://www.legislation.gov.uk/uksi/1997/3032/contents/made [Accessed 16 March 2016].

Coreck Maritime GmbH v. Handelsveem BV and Others. Reference for a preliminary ruling: Hoge Raad der Nederlanden - Netherlands. Brussels Convention - Article 17 - Clause conferring jurisdiction - Formal conditions - Effects. Case C-387/98. Curia Europa. http://curia.europa.eu/juris/liste.jsf?language=en&num=C-387/98. [Accessed 25 March 2016]. Para.19. [Accessed 8 April 2016].

CORDELL, N. (2013) *Intellectual Property in the Cloud*. Allen and Overy. *http://www.allenovery.com/SiteCollectionDocuments/Intellectual_property_in_the_Cloud_May_2013.PDF* [Accessed 4 January 2016].

CORNELL UNIVERSITY. (2012) *Chapter 36 – Foreign Intelligence Surveillance Subchapter IV – Access to certain Business Records for Foreign Intelligence Purposes, S 1861. Access to certain business records for foreign intelligence and international terrorism investigations.* Cornell University Law School. https://www.law.cornell.edu/uscode/pdf/uscode50/lii_usc_TI_50_ST_36_CH_IV_SE_1861.pdf. [Accessed 26 February 2016].

Council of the European Union. (2014) Proposal for a regulation of the European Parliament and of the Council 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)-Pseudonymised, Euro privacy. http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2017831%202013%20INIT [Accessed 21 March 2016].

Council Regulation (EC) No. 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters. Eur-Lex. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001R0044:en:HTML [Accessed 10 March 2016].

Council Regulation (EC) No. 40/94 of 20 December 1993 on the Community trade mark. Eur-Lex. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:l26022a [Accessed 6 April 2016].

The Council of the European Union. (2000) Council Regulation (EC) No. 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters. Eur-Lex. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001R0044:en:HTML [Accessed 15 January 2016].

Court of Justice of the European Union PRESS RELEASE No. 115/11 Luxembourg, 25 October 2011, Press and Information Judgment in Joined Cases C-509/09 and C-161/10 E-Date Advertising GmbH v. X and Olivier Martinez and Robert Martinez v. MGN Limited, Europa. Rapid Press. europa.eu/rapid/press-release_CJE-11-115_en.pdf. [Accessed 15 January 2016].

CRAIG, R. et al. (2009) *Cloud computing in the public sector: Public manager's guide to evaluating and adopting cloud computing.* CISCO. http://www.cisco.com/c/dam/en_us/about/ac79/docs/sp/Cloud_Computing.pdf [Accessed 17 March 2016].

Cramp & Sons Ltd v. Frank Smythson Ltd [1944] AC 329, 1944. CIPIL. University of Cambridge. Centre for Intellectual Property and Information Law. http://www.cipil.law.cam.ac.uk/virtual-museum/cramp-sons-ltd-v-frank-smythson-ltd-1944-ac-329 [Accessed 16 March 2016].

CRANE, J. (2012) *The death of outsourcing and other IT management trends.* Forbes. http://www.forbes.com/sites/ciocentral/2012/12/28/the-death-of-outsourcing-and-other-it-management-trends/#310015df75c7 [Accessed 20 August 2016].

CREATIVE COMMONS. (n.d.) *About the licences.* Creative Commons. http://creativecommons.org.au/learn/licences/ [Accessed 10 May 2016].

D

Daniela Mühlleitner v. Ahmad Yusufi & Wadat Yusufi, (Jurisdiction in civil and commercial matters – Jurisdiction over consumer contracts – Regulation (EC) No. 44/2001 – Article 15(1)(c) – Possible limitation of that jurisdiction to distance contracts) Case C-190/11. Curia Europa. http://curia.europa.eu/juris/document/document.jsf?text=&docid=126428&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=997554 [Accessed 21 January 2016].

Data Protection Commissioner. (n.d.) Anonymisation and Pseudonymisation. Data Protection. https://dataprotection.ie/viewdoc.asp?DocID=1594&ad=1 [Accessed 10 May 2016].

Data Protection Working Party. (2010) *WP 179 Opinion 8/2010 on applicable law.* EC Europa. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_en.pdf [Accessed 17 February 2016].

DEAZLEY, R. (n.d.) *School of law commentaries, (Primary sources on Copyright 1450-1900).* University of Birmingham. http://www.copyrighthistory.org/cam/tools/request/showRecord?id=commentary_uk_1844 [Accessed 4 April 2016].

DEJURE. (1983) *BGH decision BGH GRUR 1983, 377 – Brombeer-Muster*. Dejure. http://dejure.org/dienste/vernetzung/rechtsprechung?Gericht=BGH&Datum=1983-06-30&Aktenzeichen=III%20ZR%20114%2F82 [Accessed 18 March 2016].

DENHAM, E. (2009) *Findings under the Personal Information Protection and Electronic Documents Act (PIPEDA*). Office of the Privacy Commission of Canada. https://www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.pdf [Accessed 22 April 2016].

Department of Health and Human Services: *45 CFR Parts 160 and 164 Standards for Privacy of Individually Identifiable Health Information; Final Rule.* HHS Government. http://www.hhs.gov/hipaa/for-professionals/privacy/ [Accessed 12 February 2016].

Definitions. (2016) *Anonymization.* Definitions.net. http://www.definitions.net/definition/anonymization. [Accessed 11 January 2016].

DEMPSEY, J.X. (1997) Communications privacy in the digital age: Revitalising the Federal wiretap laws to enhance privacy. *Albany publishers Law Journal of Science & Technology*, 8 (1).

Department of Communications. (2000) *A Green Paper on Electronic Commerce for South Africa.* Government Department of Communications. http://www.gov.za/sites/www.gov.za/files/electronic_commerce_1.pdf [Accessed 11 April 2016].

Department of Communications. (2013). *South Africa connect: Creating opportunities, ensuring inclusion, South Africa's broadband policy*. Department of Communications. http://www.gov.za/sites/www.gov.za/files/37119_gon953.pdf [Accessed 11 May 2016].

DE SILVA, S. (2014) *5th Meeting of European Commission Expert Group on Cloud Computing Contracts Liability Discussion Paper.* EC Europa. http://ec.europa.eu/justice/contract/files/liability_discussion_paper_en.pdf [Accessed 23 August 2016].

Digital civil rights in Europe (n.d.) *Article 29 Working Party on online social networking.* EDRI. http://history.edri.org/edri-gram/number7.13/article-29-social-networks [Accessed 22 April 2016].

*The Digital Millennium Copyright Act 1998 (DCMA) (*USA). Copyright Gov. http://www.copyright.gov/legislation/dmca.pdf [Accessed 12 April 2016].

DINWOODIE, G.B. (2000) *A new copyright order: Why national courts should create global norms.* University of Pennsylvania Scholarship Law. http://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=3295&context=penn_law_review [Accessed 21 April 2016].

Directive 95/46/EC of the European Parliament and 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. EC Europa. http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf [Accessed 22 April 2016].

Directive 96/91/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases. Eur-Lex. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31996L0009&from=EN [Accessed 12 March 2016].

Directive 2000/31/EC 2000 art 3 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'). Eur-Lex. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:en:HTML [Accessed 12 May 2016].

Directive 2002/19/EC of the European Parliament and the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive). Eur-Lex. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0022&from=EN [Accessed 18 May 2016].

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) Official Journal L 201, 31/07/2002 P. 0037 – 0047. Eur-Lex. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML. [Accessed 25 May 2016].

Directive 2009/24/EC of the European Parliament and the Council of 23 April 2009, on the legal protection of computer programs. Eur-Lex. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:111:0016:0022:EN:PDF [Accessed 18 March 2016].

Directorate for Financial and Enterprise Affairs, Competition Committee. (2012) *Roundtable on market definition.* OECD. http://ec.europa.eu/competition/international/multilateral/2012_jun_market_definition_en.pdf [Accessed 15 April 2016].

DOBSCHAT, C. (2013) *Surprise: Telekom-Drossel for all customers and traffic exceptions for "Partner" confirmed.* Mobile Geeks. https://translate.google.com/translate?hl=en&sl=de&u=https://www.mobilegeeks.de/uberraschung-telekom-drossel-fur-alle-kunden-und-traffic-ausnahmen-fur-partner-bestatigt/&prev=search [Accessed 8 May 2016].

DOLMANS, M. and LEYDEN, A. (n.d.) Internet & antitrust: An overview of EU and national case law. *Competition Laws Bulletin*. https://www.clearygottlieb.com/~/media/cgsh/files/publication-pdfs/internet-antitrust-an-overview-of-eu-and-national-case-law.pdf. [Accessed 4 May 2016].

DONOHUE, M. and YPSILANTI, D. (2009) *Briefing paper for the ICCP Technology Foresight Forum: Cloud Computing and Public Policy.* OECD. https://www.oecd.org/sti/ieconomy/43933771.pdf [Accessed 15 March 2016].

DONOVAN, K., NORTH, J. and FONSEKA, R. (2014) *Fair use exception to copyright infringement: The cloud is the limit.* Modaq. http://www.mondaq.com/australia/x/293866/Copyright/Fair+use+exception+to+copyright+infringement+The+cloud+is+the+limit [Accessed 10 April 2016].

DRAHOS, P. (2002) Developing countries and international intellectual property standard setting. *The Journal of World Intellectual Property,* 5 (5). pp. 765–789, Wiley. *http://onlinelibrary.wiley.com/doi/10.1111/j.1747-1796.2002.tb00181.x/pdf* [Accessed 2 April 2016].

DROPBOX. (2014) *Dropbox terms of service posted.* Dropbox. https://www.dropbox.com/terms2014. [Accessed 12 April 2016].

DUDLEY, A. et al. (2012) *Investigating cyber law and cyber ethics: Issues, impacts and practices.* Hershey PA: Information Science Reference.

DUGARD, J. (2013) *International Law, A South African Perspective*. 4th ed. Cape Town: Juta & Co.

E-Commerce directive, liability of intermediaries. EC Europa. *https://ec.europa.eu/digital-single-market/en/e-commerce-directive* [Accessed 26 March 2016].

E-Date Advertising GmbH v. X and Olivier Martinez and Robert Martinez v. MGN Limited. Europa Rapid Press. europa.eu/rapid/press-release_CJE-11-115_en.pdf [Accessed 15 January 2016].

Electronic Communications and Transaction Act 25 of 2002 (SA) (ECTA). Government of South Africa. Southern African Legal Information Institute. http://www.saflii.org/za/legis/consol_act/ecata2002427.pdf [Accessed 26 March 2016].

ENSOR, L. (2017) *Revision plans for Copyright Bill raise MP's ire*, Business day, https://www.businesslive.co.za/bd/national/2017-08-21-revision-plans-for-copyright-bill-raise-mps-ire/ [Accessed 28 August 2017]

Equal Employment Opportunity Commission v Arabian American Oil Company Nos. 89-1838, 89-1845 Argued Jan. 16, 1991, Decided March 26, 1991 499 U.S. 244 Certiorari to the United State Court of Appeals for the fifth Circuit. Supreme Justia. https://supreme.justia.com/cases/federal/us/499/244/case.html [Accessed 5 April 2016].

ERNEST. (n.d.) *Copyright in names*: Ernest. http://www.ernest.net/writing/CopyrightInAName.pdf [Accessed 16 March 2016].

ESPION. (n.d.) *White Paper: Data Protection in the Cloud*, Espion Group. https://www.espiongroup.com/images/uploads/downloads/Espion_Whitepaper_-_Data_Protection_In_The_Cloud.pdf [Accessed 15 April 2016].

EU copyright reform: Revisiting the principle of territoriality Briefing September 2015. Euro Parliament. http://www.europarl.europa.eu/RegData/etudes/BRIE/2015/568348/EPRS_BRI(2015)568348_EN.pdf [Accessed 6 April 2016].

EU Courts Debate*. (2007) Legal analysis of a single market for the information society (SMART 2007/0037).* EC Europa. http://ec.europa.eu/information_society/newsroom/cf/itemdetail.cfm?item_id=7022 [Accessed 26 March 2016].

EURO CLOUD. (2015) *Major mistakes in data privacy – data protection in the cloud*. Euro Cloud. https://www.eurocloud.org/news/detail/news/major-mistakes-in-data-privacy-data-protection-in-the-cloud.html [Accessed 10 August 2016].

European Commission. (2012) *Article 29 Data Protection Working Party.* EC Europa. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf [Accessed 9 January 2016].

European Commission. (2012) *Article 29 Data Protection Working Party. This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC (as revised by 2009/136/EC) where relevant.* EC Europa. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf [Accessed 9 January 2016].

European Commission. (2012) *Proposal for a Regulation of the European Parliament and of the Council 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)* Eur-Lex. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012PC0011&from=EN [Accessed 6 February 2016].

European Commission.(2012) *Proposal for a Regulation of the European Parliament and of the Council 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) [SEC (2012) 73 final],* European Parliament. http://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2012/0011/COM_COM%282012%290011_EN.pdf [Accessed 6 February 2016].

European Commission. (2012) *Unleashing the Potential of Cloud Computing in Europe. Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and the Committee of Regions.* Eur-Lex.http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF [Accessed 11 May 2016].

European Commission. (2013) *Public Consultation on the review of the EU copyright rules.* EC Europa. http://ec.europa.eu/internal_market/consultations/2013/copyright-rules/docs/consultation-document_en.pdf [Accessed 8 April 2016].

European Commission. (2016) *Overview on binding corporate rules.* EC Europa. http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/index_en.htm [Accessed 12 December 2016].

European Commission v. Federal Republic of Germany. Failure of a Member State to fulfil obligations – Electronic communications – Directive 2002/19/EC – Directive 2002/21/EC – Directive 2002/22/EC – Networks and services – National rules – New markets. Case C-424/07. (2009) Curia Europa. http://curia.europa.eu/juris/liste.jsf?language=en&jur=C,T,F&num=c-424/07&td=ALL [Accessed 15 May 2016].

European Commission v. Federal Republic of Germany. (Advocate General Opinion) Case C-424/07. (2009). Curia Europa. http://curia.europa.eu/juris/liste.jsf?language=en&jur=C,T,F&num=c-424/07&td=ALL. [Accessed 15 May 2016].

European Commission Working Party. (2005) *Working document on data protection issues related to Intellectual Property rights.* European Commission, Internal Market Directorate-General, Brussels. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2005/wp104_en.pdf [Accessed 14 September 2015].

European Convention on Human Rights. Council of Europe. http://www.echr.coe.int/Documents/Convention_ENG.pdf [Accessed 18 February 2016]. Article 8.

European Network and Information Security Agency. (2012) *Cloud computing benefits, risks and recommendations for information security rev b*. ENISA. http://www.bing.com/search?FORM=SWBW15&q=Cloud%20Computing%20Benefits%2C%20Risks%20and%20Recommendations%20for%20Information%20Security%20rev%20b%20December%202012. [Accessed 16 January 2016].

European Court of Human Rights. (2010) *European Convention on Human Rights as amended by Protocols Nos. 11 and 14 supplemented by Protocols Nos. 1, 4, 6, 7, 12 and 13.* ECHR. http://www.echr.coe.int/Documents/Convention_ENG.pdf [Accessed 2 May 2016].

European Parliament and of the Council of 22, 1998. *Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations***.** Official Journal L 204, 21/07/1998 P. 0037 – 0048. Eur-Lex. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31998L0034 [Accessed 12 April 2016].

European Parliament and of the Council of 8 June 2000*. Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce').* Official Journal L 178, 17/07/2000 P. 0001 – 0016. Eur-Lex. http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1464703648135&uri=CELEX:32000L0031 [Accessed 12 April 2016].

The European Parliament and the Council of April 2016, 2016 Regulation 16/679, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). EC Europa. http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf [Accessed 25 May 2016]. Recital 26.

European Parliament, 1995, EU Data Protection 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. Eur-lex. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN [Accessed 6 February 2016].

The European Parliament and the Council of April 2016, 2016 Regulation 16/679, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). EC Europa. http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf. [Accessed 25 May 2016].

European Union (2012). *Article 29 Data Protection Working Party Opinion 05/2012 on Cloud Computing Adopted July 1st 2012.* EC Europa. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf [Accessed 6 January 2016].

European Union. (2014) *The EU explained: Digital agenda for Europe*. Europa EU. https://europa.eu/european-union/topics/digital-economy-society_en [Accessed 8 April 2016].

European Treaty Series (1981) *No. 108 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.* RM Council of Europe. *https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680078b37* [Accessed 8 February 2016].

EU-US Privacy Shield Framework (2016) https://www.privacyshield.gov/Program-Overview [Accessed 15 April 2016].

F

FACEBOOK. (n.d.) *Facebook data collection and use policy.* Facebook. https://www.facebook.com/policy.php [Accessed 12 December 2016].

FACEBOOK. (2015) *Terms of service - Facebook*. Facebook. https://www.facebook.com/legal/terms. [Accessed 14 March 2016].

FACEBOOK. (2015) *Terms of service, sharing your content and information*. Facebook. https://www.facebook.com/terms [Accessed 12 March 2016].

Federal Public Service Justice [C - 2004/09511] F. 2004 - 2935 16 JULY 2004. - Law Bearing the Code of Private International Law (1). Reflex Chrono. http://reflex.raadvst-consetat.be/reflex/index.reflex?docid=87708&lang=fr [Accessed 23 March 2016].

Federal Republic of Germany v. European Parliament and Council of the European Union. Directive 98/43/EC – Advertising and sponsorship of tobacco products – Legal basis – Article 100a of the EC Treaty (now, after amendment, Article 95 EC). Case C-376/98. Curia Europa. http://curia.europa.eu/juris/liste.jsf?language=en&num=C-376/98 [Accessed 15 May 2016].

Feist Publications Inc. v. Rural Tel. Svc. Co., Inc. Supreme Court of the United States, 499 U.S. 340 (1991). JUSTIA US Supreme Court. https://supreme.justia.com/cases/federal/us/499/340/case.html [Accessed 22 March 2016].

Financial Mail (Pty) Ltd and Others v. Sage Holdings Ltd and Another (612/90) [1993] ZASCA 3; 1993 (2) SA 451 (AD); [1993] 2 All SA 109 (A) (18 February 1993). Southern African Legal Information Institute. http://www.saflii.org/za/cases/ZASCA/1993/3.html [Accessed 14 March 2016].

Fiona Shevill, Ixora Trading Inc., Chequepoint SARL and Chequepoint International Ltd v. Presse Alliance SA. Reference for a preliminary ruling: House of Lords - United Kingdom. Brussels Convention - Article 5 (3) - Place where the harmful event occurred - Libel by a newspaper article. Case C-68/93. Eur-Lex. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A61993CJ0068. [Accessed 23 March 2016].

FIORINI, A. (2008) The codification of private international law in Europe. *Electronic Journal of Comparative Law*, 12 (1). *https://www.ejcl.org/121/art121-7.pdf*. [Accessed 23 March 2016].

Football Dataco Ltd, Scottish Premier League Ltd, Scottish Football League, PA Sport UK Ltd v. Sportradar GmbH, Sportradar AG, Case C-173/11 ECLI:EU:C:2012:642, 2012. Eur-Lex. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62011CJ0173&from=EN [Accessed 12 March 2016].

FOLEY. (n.d.) Cloud computing, A practical framework for managing cloud computing risk. Foley. https://www.foley.com/files/Publication/493fc6cc-aa03-4974-a874-022e36d12184/Presentation/PublicationAttachment/c9bd65f3-a6fd-4acb-96de-d1c0434f1eb7/CloudComputingPracticalFrameworkforManagingCloudComputingRisk.pdf. [Accessed 10 March 2016].

The Foreign Intelligence Surveillance Act of 1978, Justice Information Sharing U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance. https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1286. [Accessed 9 July 2016]

The Foreign Intelligence Surveillance Act of 1978, FISA. https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1286. [Accessed 25 February 2016].

Fraley et al. v. Facebook, Inc., et al., Case No. CV-11-01726 RS. Fraley. http://www.fraleyfacebooksettlement.com/ [Accessed 25 February 2016].

France Telecom SA v. Commission of the European Communities. *Case C-202/07 P.* Curia Europa. http://curia.europa.eu/juris/liste.jsf?language=en&num=C-202/07 [Accessed 6 May 2106].

Free Trade Agreements Australia. (2009) Office of the United States Trade Representative. https://ustr.gov/trade-agreements/free-trade-agreements/australian-fta [Accessed 12 October 2016].

Free Trade Agreements Singapore 2003, Office of the United States Trade Representative. https://ustr.gov/sites/default/files/uploads/agreements/fta/singapore/asset_upload_file222_4063.pdf [Accessed 29 September 2016].

Free Trade Commission. (2012) *Protecting consumer privacy in an era of rapid change.* FTC. https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers [Accessed 19 March 2016]. p. 56.

Free Trade Commission. (2014) *Data brokers: A call for transparency and accountability*. FTC. https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf [Accessed 23 March 2016].

G

Galago Publishers (Pty) Ltd & another v. Erasmus 1989 (1) SA 276 (A) at 283 C. Law Blog SA. https://lawblogsa.files.wordpress.com/2013/03/galago-pub-v-erasmus.pdf [Accessed 1 May 2016].

GANTZ, J.F., MINTON, S. and TONCHEVA, A. (2012) *Cloud computing's role in job creation*. IDC White Paper sponsored by Microsoft. https://news.microsoft.com/download/features/2012/IDC_Cloud_jobs_White_Paper.pdf [Accessed 16 April 2016].

GARTNER Inc. (2013) Forecast: Public cloud services, worldwide, 2011-2017, 4Q13 Update. Gartner. *https://www.gartner.com/doc/2642020/forecast-public-cloud-services-worldwide* [Accessed 7 December 2015].

GARTNER Inc. (2015) *Gartner identifies the top 10 strategic technology trends for 2016.* Gartner. http://www.gartner.com/newsroom/id/3143521 [Accessed 6 February 2016].

GASSER, U., FARIS, R. and JONES, R.H. (2013) *Internet Monitor 2013: Reflections on the Digital World.* The Berkman Center for Internet and Society Research Publication Series. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2366840 [Accessed 19 April 2016].

GASSER, U. and O'Brien, D. (2014) *Governments and cloud computing: Roles, approaches, and policy considerations.* Berkman Center for Internet and Society Research Publication. https://dash.harvard.edu/bitstream/handle/1/16460373/Gasser2014-6.pdf?sequence=1 [Accessed 17 May 2016].

General Data Protection Regulation (EU). *Regulation (EU) 2016/679.* EC Europa. http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf. [Accessed 25 May 2016].

GEBHART, G. (2016) *What Facebook and WhatsApp's data sharing plans really mean for user privacy*. Electronic Frontier Foundation. EFF ORG. https://www.eff.org/deeplinks/2016/08/what-facebook-and-whatsapps-data-sharing-plans-really-mean-user-privacy-0 [Accessed 16 October 2016].

GEIST, M. (2005) *Anti-circumvention legislation and competition policy: Defining a Canadian way?* Irwin Law. https://www.irwinlaw.com/sites/default/files/attached/Two_04_Geist.pdf [Accessed 23 February 2016].

GEOFFREY, C.C.I. (2012) *Rethinking jurisdiction under International Law*, Works Bepress. https://works.bepress.com/chinedu_ihenetugeoffrey/11/ [Accessed 15 March 2016].

GfK. (2016) *Marketing research-specializations.* GfK. http://www.gfk.com/en-za/ [Accessed 23 March 2016].

GIBSON, K (2015) *Keeping your secret recipe secret*. NU.IT. http://nu.it-online.co.za/?p=177 [Accessed 4 January 2016].

GINSBURG, J.C. (1997) Copyright without borders? Choice of forum and choice of law for copyright infringement in cyberspace. *Cardozo Arts and Entertainment Law Journal.* https://cyber.harvard.edu/property00/jurisdiction/ginsburg.html [Accessed 5 August 2016].

GINSBURG, J.C. and TREPPOZ, E. (2015*) International copyright law: U.S. and E.U. perspectives: Text and cases*. Cheltenham: Edward Elgar. p. 413, Sec IV.

GOOGLE Inc. (n.d.) Google cloud platform terms of service. Google. *https://cloud.google.com/terms/* [Accessed 16 January 2016].

GOOGLE Inc. (2014) *Terms of service. Your, content in our services.* Google Inc. https://www.google.com/policies/terms/ [Accessed 12 March 2016].

Google Inc. v. Vidal-Hall Neutral Citation Number: [2015] EWCA Civ 311. Royal Court of Justice. Government. https://www.gov.im/lib/docs/odps/cl_google_v_vidalhall_2015_ewca_civ.pdf [Accessed 12 February 2016].

GORDON, W.J. et al. (1994) Virtual reality, appropriation, and property rights in art: A roundtable discussion. *Cardozo Arts and Entertainment Law Journal*. http://heinonline.org/HOL/LandingPage?handle=hein.journals/caelj13&div=21&id=&page= [Accessed 4 April 2016].

Government of United Kingdom. (2017) *Countries of the EU and EEA, Countries in the EU and EEA, The European Union (EU) is an economic and political union of 28 countries*. Government of the United Kingdom. https://www.gov.uk/eu-eea [Accessed 12 March 2017].

GREENLEAF, G. (2015) Global data privacy laws 2015: 109 countries, with European laws now a minority. *Privacy Laws & Business International Report*. SSRN. *http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2603529* [Accessed 8 December 2015].

Guidance on the Protection of Personal Identifiable Information (PII). United States Department of Labour. https://www.dol.gov/general/PoPIi [Accessed 7 February 2016].

GURRY, F. (2013) *Address by the Director General WIPO Assemblies – September 23 to October 2, 2013.* WIPO. http://www.wipo.int/about-wipo/en/dgo/speeches/a_51_dg_speech.html [Accessed 23 April 2016].

H

HAINES, D. (2002) *The impact of the internet on the Judgements Project: Thoughts for the future.* Hague Conference on Private International Law. https://assets.hcch.net/upload/wop/gen_pd17e.pdf [Accessed 28 April 2016].

HALE, T.N. (2008) *Transparency, accountability, and global governance*. Questa, trusted on line research. https://www.questia.com/read/1G1-176859137/transparency-accountability-and-global-governance [Accessed 12 May 2016].

Handelskwekerij G.J. Bier B.V. v. Mines de Potasse d'Alsace S.A. (preliminary ruling requested by the Gerechtshof of The Hague) Case 21/76. Curia Europa. http://curia.europa.eu/juris/showPdf.jsf?docid=89372&doclang=EN [Accessed 16 January 2016].

HARGREAVES, I. (2011) *Digital opportunity: A review of intellectual property and growth.* Gov. UK Publications. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/32563/ipreview-finalreport.pdf [Accessed 5 May 2016].

Haupt t/a Soft Copy v. Brewers Marketing Intelligence (Pty) Ltd and others 2006 (4) SA 458 SCA. 2006. Southern African Legal Information Institute. http://www.saflii.org/za/cases/ZASCA/2006/40.html [Accessed 16 March 2016].

HAY, G.A. (1982) *The economics of predatory pricing.* Cornell Law School. http://scholarship.law.cornell.edu/cgi/viewcontent.cgi?article=1624&context=facpub [Accessed 26 April 2016].

HEALEY, A. (n.d.) *Tracking individuals via their cell phones: Answering the call.* Federal Law Enforcement Training Centres. *https://www.fletc.gov/sites/default/files/imported_files/training/programs/legal-division/downloads-articles-and-faqs/research-by-subject/miscellaneous/TrackingIndividualsviaTheirCellularPhones.pdf* [Accessed 4 February 2016].

The Health Insurance Portability and Accountability Act of 1996. GPO. https://www.gpo.gov/fdsys/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf [Accessed 29 March 2016].

HELLER, M. (2004) *The country of origin principle in E-commerce Directive: A conflict with conflict laws?* Eur Rev Priv L RQSL. *http://www.rgsl.edu.lv/images/stories/publications/RWP6Hellner.pdf* [Accessed 12 April 2016].

HILLELSON, L. (n.d.) *Making the business case for the media industry transition to IP.* Broadcasting and Cable. https://www.cisco.com/c/dam/en_us/solutions/industries/downloads/media-industry-transition-ip-making-business-case.pdf [Accessed 23 April 2016].

HITCH Software Platform. (2016) *Provider terms of service*. Hitch HQ. https://www.hitchhq.com/help/provider-terms-of-service/ [Accessed 23 August 2016].

HOGENDORN, C. (2007) *Broadband internet: Net neutrality versus open access.* Chogendorn. http://chogendorn.web.wesleyan.edu/oa.pdf [Accessed 15 January 2016].

HON, W.K. et al. (2014) *Cloud accountability: The likely impact of the proposed EU data protection regulation.* Research Gate. https://www.researchgate.net/publication/269037024_Cloud_Accountability_The_Likely_Impact_of_the_Proposed_EU_Data_Protection_Regulation [Accessed 19 March 2016].

HON, W.K., MILLARD, C. and WALDEN, I. (2011) *The problem of 'personal data' in cloud computing - what information is regulated? The cloud of unknowing, Part 1.* SSRN. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1783577 [Accessed 9 March 2016].

HON, W.K., MILLARD, C. and WALDEN, I. (2012a) *Who is responsible for 'personal data' in cloud computing? The cloud of unknowing, Part 2*. Queen Mary School of Law, Legal Studies. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1794130 [Accessed February 2016].

HON, W.K., MILLARD, C. and WALDEN, I. (2012b) Negotiating cloud contracts, looking at clouds from both sides now. *Stanford Technology Law Review*. https://journals.law.stanford.edu/sites/default/files/stanford-technology-law-review/online/cloudcontracts.pdf. [Accessed 16 February 2016].

HONG, K. (2014) *Dropbox reaches 300m users, adding on 100m users in just six months*. The next Web. http://thenextWeb.com/insider/2014/05/29/dropbox-reaches-300m-users-adding-100m-users-just-six-months/#gref [Accessed 11January 2016].

HOOVER, J.N. (2013) Compliance in the ether: Cloud computing, data security and business regulation. *Journal of Business & Technology Law*. 8 (1), Art. 18. Digital Commons. http://digitalcommons.law.umaryland.edu/jbtl/vol8/iss1/18/. [Accessed 12 May 2015].

HOU, L. et al. (2008) *Network neutrality in Europe.* Eurocpr. http://www.eurocpr.org/data/2008/Paper11-Liyang.pdf [Accessed 21 May 2016].

H.R.1201 - Digital Media Consumers' Rights Act of 2005 109th Congress (2005-2006). Congress. Gov. https://www.congress.gov/109/bills/hr1201/BILLS-109hr1201ih.pdf [Accessed May 5 2016].

HRYNASZKIEWICZ, I. et al. (2010) *Preparing raw clinical data for publication: guidance for journal editors, authors, and peer reviewers. Comment in BMJ policy on data sharing.* US National Library of Medicine National Institutes of Health. https://www.ncbi.nlm.nih.gov/pubmed/20110312 [Accessed 29 May 2016].

HUBERT GROUP. (2016) Cloud computing and contracts. Hubert Group. http://journal.iaccm.com/contracting-excellence-journal/cloud-computing-and-contracts [Accessed 3 September 2016].

HURLEY, D. (2003) *Pole Star: Human rights in the information society, rights and democracy*. Brown. https://www.brown.edu/academics/professional/cybersecurity/img/In_The_News/hurley-polestar [Accessed 12 May 2016].

I

IBANEZ, J. (2005) *Who governs the internet? The emerging regime of e-commerce.* Pompeu Fabra. University Barcelona. https://ecpr.eu/Filestore/PaperProposal/25e3ce87-d527-44e9-9f1a-54fd4822cb86.pdf [Accessed 12 May 2016].

IBM. (2013) *IBM SaaS terms of service, smart cloud for business*. IBM. https://www-03.ibm.com/software/sla/sladb.nsf/pdf/8218-07/$file/Z125-8218-07_03-2013_en_US.pdf [Accessed 9 April 2016].

Information Commissioners Office. (n.d.) *Data controller means - a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any*

personal data are, or are to be, processed', ICO UK. https://ico.org.uk/for-organisations/guide-to-data-protection/key-definitions/ [Accessed 7 February 2016].

Information from European Union Intuition's, Bodies, Offices and Agencies European Commission. (2010) *Guidelines on Vertical Restraints, (2010/C 130/01).* Eur-Lex. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:130:0001:0046:EN:PDF [Accessed 12 January 2016].

Information from the European Union Institutions and Bodies Commission. (2009) *Communication from the Commission, Guidance on the Commission's enforcement priorities in Applying Article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings (2009/C 45/02).* Eur-Lex. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52009XC0224(01)&from=EN [Accessed 19 February 2016].

Information Systems Audit and Control Association. (2011) *IT Control Objectives for Cloud Computing: Controls and Assurance in the Cloud*. ISACA. *http://www.isaca.org/chapters2/kampala/newsandannouncements/Documents/IT%20contro%20objectives%20for%20Cloud%20computing.pdf* [Accessed 12 February 2016].

Io Group, Inc. v. Veoh Networks, Inc.N.D. Cal., August 27, 2008, No. C06-03926 HRL. JOLT Law Harvard. http://jolt.law.harvard.edu/digest/copyright/io-group-v-veoh-networks [Accessed 15 April 2016].

IP IN BRIEF. (2010) *UMG Recordings, Inc. v Veoh Networks Inc., 665 F. Supp. 2d 1099 (C.D. Cal.2009)*. IP in Brief. http://www.ipinbrief.com/wp-content/uploads/2010/10/umg-v.-veoh-district-court-opinion.pdf [Accessed 15 April 2016].

IPR. (2004) *The code of private international law (CPIL).* University of Gent. Institute for International Private Law. http://www.ipr.be/data/B.WbIPR%5BEN%5D.pdf [Accessed 2 May 2016].

Isibaya – Registration. (n.d.) *Public Investment Corporation*. Isibaya. https://isibayafund.pic.gov.za/Pages/Home.aspx [Accessed 15 June 2016].

ISRAELY, A. (2013) *Trends and applications. Big data poses legal issues and risks*, *database trends and applications*. http://www.dbta.com/Editorial/Trends-and-Applications/Big-Data-Poses-Legal-Issues-and-Risks-93666.aspx [Accessed 4 May 2015].

Itar-Tass Russian News Agency et al., Plaintiff, v Russian Kurier, INC. et al., Defendant. Al J. DANIEL, Jr. and Michael New city, Appellants, v. Itar-Tass Russian New Agency, et al., and Julian H. Lowenfeld and Moskovsky Komsomolets and AR Publishing Co. Inc., Appellees. Docket No. 97-7444. Decided: April 03, 1998. United States Court of Appeals, Second Circuit. Case Law. http://caselaw.findlaw.com/us-2nd-circuit/1097235.html [Accessed 11 April 2016].

ITV Broadcasting Ltd and Others v. TV Catch Up Ltd. *Reference for a preliminary ruling: High Court of Justice (England & Wales) (Chancery Division) - United Kingdom. Directive 2001/29/EC - Article 3(1) - Broadcasting by a third party over the internet of signals of commercial television broadcasters - 'Live streaming' - Communication to the public. Case C-607/11*. Curia Europa. http://curia.europa.eu/juris/liste.jsf?language=en&num=C-607/11 [Accessed 7 August 2016].

J

JACKSON, K. (2013) *A framework for cloud computing adoption in South African Government.* Cloud Credential Council.http://www.cloudcredential.org/a-framework-for-cloud-computing-adoption-in-south-african-government/ [Accessed 7 May 2016].

JACOB, R. Hon. Mr. Justice, (2000) *International Intellectual Property litigation in the next millennium*, Case Western Reserve University.
http://scholarlycommons.law.case.edu/cgi/viewcontent.cgi?article=1500&context=jil [Accessed 8 August 2015].

JAEGER, P., LIN, J. and GRIMES, M. (2008) Cloud computing and information policy: Computing in a policy cloud? Journal of Information Technology and Politics.
http://www.tandfonline.com/doi/pdf/10.1080/19331680802425479 [Accessed 24 April 2016].

JEFFERSON, T. (1999) Political writings, letter to John Taylor. Cambridge: Cambridge Books.
Judgement based on. Regulation (EC) No. 44/2001 – Jurisdiction and the enforcement of judgments in civil and commercial matters – Jurisdiction 'in matters relating to tort, delict or quasi-delict' – Directive 2000/31/EC – Publication of information on the internet – Adverse effect on personality rights – Place where the harmful event occurred or may occur – Law applicable to information society services. Curia Europa.
http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130d6741dabcf213a46f0aae1e10bb880fcae.e34KaxiLc3eQc40LaxqMbN4PahmRe0?text=&docid=111742&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=139352 [Accessed 15 January 2016].

Judgement of the Court (Grand Chamber) (2010) In Joined Cases C-316/07, C-358/07 to C-360/07, C-409/07 and C-410/07. Curia Europa.
http://curia.europa.eu/juris/document/document.jsf?docid=80772&mode=lst&pageIndex=1&dir=&occ=first&part=1&text=&doclang=EN&cid=790283 [Accessed 20 March 2016].

Judgement of the Court (Second Chamber) (2010) Case C-258/08, Ladbrokes Betting & Gaming Ltd, Ladbrokes International Ltd v. Stichting de Nationale Sporttotalisator. Curia Europa.
http://curia.europa.eu/juris/document/document.jsf?docid=81086&mode=lst&pageIndex=1&dir=&occ=first&part=1&text=&doclang=EN&cid=792292 [Accessed 16 March 2016].

K

KAGAN. J. (2013) *Bricks, mortar, and google: defining the relevant antitrust market for internet-based companies*. *NYLS Law Review.* http://www.nylslawreview.com/wp-content/uploads/sites/16/2013/11/55-1.Kagan_.pdf [Accessed 17 January 2016].

KAHNEMAN, D., KNETSCH, J.L. and THALER, R.H. (1991) Anomalies: The endowment effect, loss aversion, and status quo bias. *The Journal of Economic Perspectives*, 5 (1). pp. 193–206. Princeton.
https://www.princeton.edu/~kahneman/docs/Publications/Anomalies_DK_JLK_RHT_1991.pdf [Accessed 16 March 2016].

KENNEDY, D. (2009) Working in the cloud. *ABA Journal*.
http://www.abajournal.com/magazine/article/working_in_the_clouds/ [Accessed 27 November 2015].

King v. South African Weather Services (716/07) [2008] ZASCA 143; 2008 BIP 330 (SCA); 2009 (3) SA 13 (SCA); [2009] 2 All SA 31 (SCA) (27 November 2008). Southern African Legal Information Institute. http://www.saflii.org/za/cases/ZASCA/2008/143.html [Accessed 20 March 2016].

Kirtsaeng, DBA Bluechristne99 v. John Wiley and Sons, Inc. Certiorari to the United State Court of Appeals for the second Circuit, No. 11–697. Argued October 29, 2012—Decided March 19, 2013.

Supreme Court. https://www.supremecourt.gov/opinions/12pdf/11-697_d1o2.pdf [Accessed 11 April 2016].

KLOPPER, H.B. et al. (2011) *Law of Intellectual Property in South Africa*. Cape Town: LexisNexis.

KOELMAN, K. and HUGENHOLTZ, B. (1999) *Online service provider liability for copyright infringement.* University of Amsterdam. http://dare.uva.nl/document/2/6027 [Accessed 27 March 2016].

KNAPP, K. (2015) *Top considerations for choosing a cloud provider.* Search Cloud Computing. http://searchcloudcomputing.techtarget.com/feature/Top-considerations-for-choosing-a-cloud-provider [Accessed 12 October 2016].

KNOT, G. (2009) *Ripped: How the wired generation revolutionized music paperback*. New York: Simon and Schuster, Inc.

KRAVETS, D. (2012) *Facebook's $9.5 Million 'Beacon' settlement approved.* Wired. https://www.wired.com/2012/09/beacon-settlement-approved/ [Accessed 3 April 2016].

KROES, N. (2010) *Cloud computing and data protection.* Europa Press. http://europa.eu/rapid/press-release_SPEECH-10-686_en.htm [Accessed 8 January 2016].

KROFT, S. (2014) *The data brokers: Selling your personal information.* CBS News. http://www.cbsnews.com/news/data-brokers-selling-personal-information-60-minutes/ [Accessed 24 March 2016].

L

Ladbroke v. William Hill [1964] 1 All ER 465, 1964. CIPIL. University of Cambridge. Centre for Intellectual Property and Information Law. http://www.cipil.law.cam.ac.uk/virtual-museum/ladbroke-v-william-hill-1964-1-all-er-465 [Accessed 16 March 2016].

LEAGLE. (2008) *In Re U.S. for Order Dir. A Prov. Of Elec, Commune.* Leagle. http://www.leagle.com/decision/20081119534FSupp2d585_11040/IN%20RE%20U.S.%20FOR%20ORDER%20DIR.%20A%20PROV.%20OF%20ELEC.%20COMMUN [Accessed 11 January 2016].

LESSIG, L. (2006) *CODE version 2.* New York: Perseus Books. http://codev2.cc/download+remix/Lessig-Codev2.pdf [Accessed 29 April 2016].

LESSIG, L. (2000) Code is law, on liberty in cyberspace. *Harvard Magazine*. http://harvardmagazine.com/2000/01/code-is-law-html [Accessed 18 February 2016].

LEWIS, D. (2008) *'Chilling competition',* Hawk ed. International Antitrust Law and Policy: Fordham Competition Law. New York: Juris Legal Information.

LEYDEN, J. (2006) *AOL sued over search engine data release, privacy breach suit launched.* The Register. https://www.theregister.co.uk/2006/09/26/aol_privacy_breach_lawsuit/ [Accessed 29 March 2016].

Licences for Europe. (2013*) Structured stakeholder dialogue.* EC Europa. https://ec.europa.eu/licences-for-europe-dialogue/en/content/about-site.html [Accessed 8 April 2016].

Licences for Europe. (2013) *Ten pledges to bring more content online.* EC Europa. http://ec.europa.eu/internal_market/copyright/docs/licences-for-europe/131113_ten-pledges_en.pdf [Accessed 8 April 2016].

LIGITEC. (2012) *Lane v. Facebook: Privacy class action settlement requires Facebook to pay $9.5 million, but provides no direct benefits to most plaintiffs*. Leon Jacobson ESQ. http://www.nylitigationfirm.com/lane_v_facebook_privacy_class_1/ [Accessed 21 April 2016].

Lokman Emrek v. Vlado Sabranovic (Area of freedom, security and justice – Jurisdiction in civil and commercial matters – Regulation No. 44/2001– Consumer contracts – Article 15(1)(c) – Activity directed to another Member State – Need for a causal link between the activities of the trader directed to the Member State of the consumer – Strong evidence – Conurbation) Case C-218/12. Curia Europa. http://curia.europa.eu/juris/document/document.jsf?text=&docid=139682&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=999880 [Accessed 18 January 2016].

L'Oréal SA and others v. eBay International AG and Others. Reference for a preliminary ruling: High Court of Justice (England & Wales), Chancery Division - United Kingdom. Case C-324/09. Curia Europa. http://curia.europa.eu/juris/liste.jsf?num=C-324/09 [Accessed 21 January 2016].

LOWENSTEIN, G. and ISSACHAROFF, S. (1994) Source dependence in the valuation of objects*. Journal of Behavioural Decision Making*, 7. Pp. 157–168. CMU. http://www.cmu.edu/dietrich/sds/docs/loewenstein/SourceDependence.pdf [Accessed 16 March 2016]. p.158.

M

MACKENZIE, N. (2012) Working paper, Replacing Section 8(D) of the Competitions Act with an Effects-Based Exclusionary Abuse of Dominance Provision. Centre for Competition Economics. http://static1.squarespace.com/static/52246331e4b0a46e5f1b8ce5/t/52d8ef10e4b0bd82f384cba8/1389948688828/REPLACING+SECTION+8%28D%29+OF+THE+SOUTH+AFRICAN+COMPETIT [Accessed 25 April 2016].

MACKENZIE, N. (2014) *Rethinking exclusionary abuse in South Africa.* Competition Commission. http://www.compcom.co.za/wp-content/uploads/2014/09/Rethinking-Exclusionary-Abuse-in-SA.pdf [Accessed 22 April 2016].

MANIVAKA, J. et al. (2013) *Disruptive technologies: Advances that will transform life, business, and the global economy.* McKinsey. http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/disruptive-technologies [Accessed 7 August 2016].

Marrakesh Treaty to facilitate access to published works for persons who are blind, visually impaired or otherwise print disabled. WIPO. http://www.wipo.int/treaties/en/ip/marrakesh/ [Accessed 12 April 2016].

MARCHINI, R. (2015) *Cloud Computing. A Practical Introduction to the Legal Issues.* 2nd ed. London: BSI Standards Limited.

MARSH. (2012) *The cloud risk framework, informing decisions about moving to the cloud.* Marsh and McLennan. http://f.datasrvr.com/fr1/812/29871/3424_MA12-11623_Cloud_Computing_Frmwk_UK_04-2012_final_nocrps.pdf [Accessed 8 August 2016].

MARTIN, T.D. (2010) Hey! You! Get off my cloud: Defining and protecting the metes and bounds of privacy, security and property in cloud computing. Journal of the Patent & Trademark Office Society. Selected Works. https://works.bepress.com/timothy_martin/3/ [Accessed 13 June 2015].

Matthews v. the United Kingdom. (Application No. 24833/94 39, Grand Chamber. ECHR 1999-1. ECHR. http://echr.coe.int/Documents/Reports_Recueil_2001-XII.pdf [Accessed 4 May 2016].

Mayne v. Main (182/99) [2001] ZASCA 35; [2001] 3 All SA 157 (A). Southern African Legal Information Institute. http://www.saflii.org/za/cases/ZASCA/2001/35.html. [Accessed 23 April 2016].

MAXEY, M. (2008) *Cloud computing public or private? How to choose cloud storage.* Sys-con Media. http://mikemaxey.sys-con.com/node/707840 [Accessed 25 May 2015].

Maximillian Schrems v. Data Protection Commissioner, joined party: Digital Rights Ireland Ltd, *Case C-362/14 2015.* (Reference for a preliminary ruling, Personal data, Protection of individuals with regard to the processing of such data, Charter of Fundamental Rights of the European Union, Articles 7, 8 and 47, Directive 95/46/EC, Articles 25 and 28, Transfer of personal data to third countries, Decision 2000/520/EC, Transfer of personal data to the United States, Inadequate level of protection, Validity, Complaint by an individual whose data has been transferred from the European Union to the United States, Powers of the national supervisory authorities). Curia Europa. http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=125031 [Accessed 15 April 2016].

Max Planck Group. (2011) *Principles on conflict of laws in intellectual property prepared by the European Max Planck Group on conflict of laws in intellectual property (CLIP).* Munich Max Planck. http://www.cl-ip.eu/_www/files/pdf2/Final_Text_1_December_2011.pdf [Accessed 18 April 2016].

Mc CULLAGH, D. (2010) *Feds push for tracking cell phones.* CNET news. http://www.cnet.com/news/feds-push-for-tracking-cell-phones/ [Accessed 20 January 2016].

Mc KENDRICK, J. (2013) *16 key service quality metrics to boost* cloud engagements. ZDNET. http://www.zdnet.com/article/16-key-service-quality-metrics-to-boost-cloud-engagements/ [Accessed 22 August 2016].

MELZER, M.A. (2011) Copyright enforcement in the cloud*. Fordham Intellectual Property, Media and Entertainment Law Journal*, 21 (2) 2011, Art. 9, VOLUME XXI, BOOK 2. http://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1492&context=iplj [Accessed 27 September 2016].

MERCURIO, B. and JUNG NI, K. (ed.) (2014) *Science and technology in international economic law: Balancing competing interests*. Abingdon: Routledge. Section on trade agreement cats and the digital technology mouse.

MERGES, R.P., MENELL, P.S., and LEMLEY, M.A. (2012) Intellectual property in the new technological age. 6th ed. New York: Aspen Casebook Series, Wolters Kluwer Law and Business.

MIALON, S.H. and BANERJEE, S. (2012) *Platform competition and access regulation on the internet.* Research Gate. https://www.researchgate.net/profile/Sue_Mialon/publication/228280683_Net_Neutrality_and_Open_Access_Regulation_on_the_Internet/links/0046352461633d9827000000.pdf/download?version=vrp [Accessed 11 January 2016].

Microsoft Corp. v. Commission of the European Communities Case T-201/04., (2007). Curia Europa *http://curia.europa.eu/juris/liste.jsf?language=en&num=T-201/04*. [Accessed 15 May 2016].

MILLARD, C. (ed.) (2014) *Cloud computing law.* Oxford: Oxford Scholarship Online. Part IV Cloud Regulation and Governance.

Ministry of Justice. (2012) *Summary of Responses, Call for Evidence on Proposed EU Data Protection Legislative Framework.* Consult Justice. https://consult.justice.gov.uk/digital-communications/data-protection-proposals-cfe/results/summary-responses-proposed-data-protection-legislation.pdf [Accessed 12 March 2016].

MURPHY, A. (2012) *Storing data in the cloud raises compliance challenges.* Forbes. http://www.forbes.com/sites/ciocentral/2012/01/19/storing-data-in-the-cloud-raises-compliance-challenges/#22e1bc96664a [Accessed 22 March 2016].

MURRAY, A. (2007) *The regulation of cyberspace: Control in the online environment*. Abingdon: Routledge-Cavendish.

MURRAY A. (2008) Symbiotic regulation. *The John Marshall Journal of Information Technology & Privacy Law*. http://repository.jmls.edu/cgi/viewcontent.cgi?article=1653&context=jitpl. [Accessed 29 April 2016].

N

NARAYANAN, A. and SHMATIKOV, V. (2007) *Robust de-anonymization of large sparse datasets*. Austin. The University of Texas. https://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf [Accessed 2 April 2016].

NARAYANAN, V. (2012) Harnessing the cloud: International law implications of cloud computing *Journal of Internet Law,* 14 (1). Research Gate. *https://www.researchgate.net/publication/290126282_Harnessing_the_cloud_International_law_implications_of_cloud-computing*. [Accessed 13 June 2015].

NASUNI White Paper: *The state of cloud storage.* NASUNI. http://www6.nasuni.com/rs/nasuni/images/nasuni-white-paper-state-of-cloud-storage-2013.pdf [Accessed 8 February 2016].

National Credit Act No. 34 of 2005. Acts online. https://www.acts.co.za/national-credit-act-2005/index.html [Accessed 15 July 2016].

National Institute of Standards and Technology. (2011) *Cloud computing reference architecture*, National Institute of Standards and Technology. http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909505 [Accessed on 15 February 2016].

National Institute of Standards and Technology. (2011) *The NIST Definition of cloud computing SP 800 – 145*. National Institute of Standards and Technology. http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf [Accessed 28 November 2015].

NETLINGO. (1996) *Data mining, a.k.a. Knowledge Discovery in Databases* (KDD). Netlingo. http://www.netlingo.com/word/data-mining.php [Accessed 26 March 2016].

Nol, M.G. (2006) *AOL research publishes 650,000 user queries.* Applied Research. Big Data Distributed Systems. Open Source. http://www.michael-noll.com/blog/2006/08/07/aol-research-publishes-500k-user-queries/ [Accessed 8 February 2016].

Northwestern Memorial Hospital v John Ashcroft, United States Court of Appeals, Seventh Circuit, Attorney General of the United States, Defendant-Appellant. No. 04-1379. Court Decision: 362 Federal Reporter, 3d Series 923; 2004 Mar 26 (date of decision). Case Law. http://caselaw.findlaw.com/us-7th-circuit/1206993.html [Accessed 28 March 2016].

NYE, J. S. (2004) *Soft power: The means to success in world politics*. Harvard Belfer Center. http://www.belfercenter.org/sites/default/files/legacy/files/joe_nye_wielding_soft_power.pdf [Accessed 12 May 2016].

O

ODLYZKO, A. (2009) *Network neutrality, search neutrality, and the never-ending conflict between efficiency and fairness in markets.* University of Minnesota. http://www.dtc.umn.edu/~odlyzko/doc/net.neutrality.pdf [Accessed 14 May 2016].

OECD. (2015) Chapter 3. Approaches to the protection of Trade Secrets. OECD. http://www.oecd.org/sti/ieconomy/Chapter3-KBC2-IP.pdf [Accessed 23 January 2016].

Office of Gas and Electricity Markets. (2010). *RPI - X@20 Emerging thinking consultation document – Alternative ex ante and ex post regulatory frameworks.* Office of Gas and Electricity Markets. https://www.ofgem.gov.uk/ofgem-publications/51950/et-alternatives.pdf [Accessed 2 April 2016].

Office of the Privacy Commission of Canada. (n.d.) *Cloud computing for small and medium sized enterprises.* OIPC. https://www.oipc.bc.ca/guidance-documents/1437 [Accessed 11 December 2015].

Office of the Privacy Commissioner for Personal Data, Hong Kong. (n.d.) *Information leaflet on cloud computing*. PCDP. https://www.pcpd.org.hk/english/resources_centre/publications/files/IL_cloud_e.pdf. [Accessed 29 September 2015].

Official Journal of the European Union. Recommendation 2003/311 of 11 February 2003 on relevant product and service markets within the electronic communications sector susceptible to ex ante regulation in accordance with Directive 2002/21 [2003] OJ L 114/45, ICT. https://www.ictregulationtoolkit.org/Documents/Document/Document/1491 [Accessed 6 January 2016].

OHM, P. (2010) Broken promises of privacy: Responding to the surprising failure of anonymization. *UCLA Law Review*. http://www.uclalawreview.org/pdf/57-6-3.pdf [Accessed 11 March 2016].

OMSTEIN, C. (2015) How private is sensitive abortion information? *Pacific Standard*. https://psmag.com/how-private-is-sensitive-abortion-information-e7345a4a7d69#.dy9l72gg2 [Accessed 28 March 2016].

ORACLE. (n.d.) *Oracle software as a service agreement V 121509*. Oracle. http://www.oracle.com/us/products/applications/crmondemand/software-service-uk-439846.pdf [Accessed 14 April 2016].

Organisation for Economic Cooperation and Development. (2009) *Briefing paper for the ICCP technology foresight forum.* OECD. https://www.oecd.org/sti/ieconomy/43933771.pdf [Accessed 15 December 2015].

Organisation for Economic Cooperation and Development. (2003) *OECD Peer Review. Competition Law and Policy in South Africa May 2003.* OECD. http://www.oecd.org/daf/competition/prosecutionandlawenforcement/2958714.pdf [Accessed 12 January 2016].

Organisation for Economic Cooperation and Development. (2013) *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data [C (80)58/FINAL, as amended on 11 July 2013 by C (2013)79] extract of Part Two.* OECD. https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf [Accessed 8 December 2015].

Oscar Bronner GmbH & Co. KG v. Mediaprint Zeitungs- und Zeitschriftenverlag GmbH & Co. KG, Mediaprint Zeitungsvertriebsgesellschaft mbH & Co. KG and Mediaprint Anzeigengesellschaft mbH & Co. KG, Case C-7/97 (1998). Curia Europa. http://curia.europa.eu/juris/liste.jsf?language=en&num=C-7/97 [Accessed 15 May 2016].

OSTERUD. E. (2013) *EU Competition Law - abuse of dominance (Article 102 TFEU)*. University of Oslo. http://www.uio.no/studier/emner/jus/jus/JUS5310/h12/undervisningsmateriale/abuse_-of_-dominance-_.pdf [Accessed 23 April 2016].

P

Parkson v. Central DuPage Hospital Nos. 80-503, 80-504 cons. 105III. Appellate Court of Illinois, First District third division 435 N.E.2d 140. Leagle. http://www.leagle.com/decision/1982955105IllApp3d850_1835/PARKSON%20v.%20CENTRAL%20DuPAGE%20HOSPITAL [Accessed 22 March 2016].

Paris Convention for the Protection of Industrial Property 1883 (March 20, 1883, as amended on September 28, 1979) World Intellectual Property Organisation. http://www.wipo.int/treaties/en/text.jsp?file_id=288514 [Accessed 12 January 2015].

Parliament of the Republic of South Africa http://www.parliament.gov.za/live/index.php [Accessed 11 May 2016].

PATRY, W. (2000) Choice of law and international copyright*. The American Journal of Comparative Law.* https://litigation-essentials.lexisnexis.com/webcd/app?action=DocumentDisplay&crawlid=1&doctype=cite&docid=48+Am.+J.+Comp.+L.+383&srctype=smi&srcid=3B15&key=e5460ced116b0b023acf45657d106827 [Accessed 15 January 2015].

PATRY, W. (2009) *Moral panics and the copyright wars*. New York: Oxford University Press, Inc.

PATRY, W. (2011) *How to fix copyright*. New York: Oxford University Press, Inc.

Payen Components South Africa Ltd v. Bovic Gaskets CC and Others (448/93) [1995] ZASCA 57; 1995 (4) SA 441 (AD); [1995] 2 All SA 600 (A) (25 May 1995). Southern African Legal Information Institute. http://www.saflii.org/za/cases/ZASCA/1995/57.html [Accessed 18 March 2016].

The Permanent Court of International Justice. (1927) *Collection of judgments "The Case of the SS Lotus": Series A. No. 10 September 7th 1927.* ICJ. http://www.icj-cij.org/pcij/serie_A/A_10/30_Lotus_Arret.pdf [Accessed 16 March 2016].

PEARSON, S. (2011) *Towards accountability in the cloud.* HP. http://www.hpl.hp.com/techreports/2011/HPL-2011-138.pdf [Accessed 27 March 2016].

Personal Information Protection and Electronic Documents Act Codification. S.C. 2000, c. 5 Current to May 12, 2016 (Last amended on June 23, 2015). Minister of Justice. http://laws-lois.justice.gc.ca/eng/acts/p-8.6/ [Accessed 11 March 2016].

The Protection of Personal Information Act No. 4 of 2013 of South Africa, *Policy, Law, Economics and Politics*. http://www.polity.org.za/article/protection-of-personal-information-act-no-4-of-2013-gazette-37067-2013-11-26 [Accessed 6 December 2015].

Peter Pammer v. Reederei Karl Schlüter GmbH & Co KG (C-585/08), and Hotel Alpenhof GesmbH v. Oliver Heller (C-144/09), 2010. Curia Europa. http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30d54bdea05742884961b6e6e3b36837595f.e34KaxiLc3qMb40Rch0SaxyKchn0?text=&docid=83437&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=163098 [Accessed 18 January 2016].

Peter Pinckney v. KDG Mediatech AG, Case C-170/12. Curia Europa. http://curia.europa.eu/juris/document/document.jsf?text=&docid=142613&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=150985 [Accessed 18 January 2016].

PETRO, N. (2007) Software as a Service. *GP Solo Magazine*. *http://www.americanbar.org/content/newsletter/publications/gp_solo_magazine_home/gp_solo_magazine_index/softwareasaservice.html* [Accessed 27 November 2015].

PICKER, R.C. (2008), *Competition and privacy in Web 2.0 and the cloud*, SSRN, Social Science Research Network. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1151985 [Accessed 4 February 2016].

POCAR, F. et al. (eds.) (2012) Choice-of-Court Agreements in Favour of Third States' Jurisdiction in Light of the Suggestions by Members of the European Parliament, Recasting Brussels I, Academia. http://www.academia.edu/2085249/ [Accessed 25 March 2016].

PRIVATE STUDY. (n.d.) *Hawkes & Sons (London) Limited v. Paramount Film Service, Limited [1934] 1 Ch. 593 (C.A.) Stated that 'private study' should be strictly construed.*

The Protection of Personal Information Act No. 4 of 2013 of South Africa, Policy, Law, Economics and Politics. http://www.polity.org.za/article/protection-of-personal-information-act-no-4-of-2013-gazette-37067-2013-11-26 [Accessed 6 December 2015].

Proposal for a Regulation of the European Parliament and the Council 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). Eur-Lex. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012PC0011&from=en [Accessed 6 February 2016].

Q

The Queen, on the application of Vodafone Ltd and Others v. Secretary of State for Business, Enterprise and Regulatory Reform. Reference for a preliminary ruling: High Court of Justice (England

& Wales), Queen's Bench Division (Administrative Court) – United Kingdom. Regulation (EC) No. 717/2007 – Roaming on public mobile telephone networks within the Community – Validity – Legal basis – Article 95 EC – Principles of proportionality and subsidiarity. Case C-58/08. Curia Europa. http://curia.europa.eu/juris/liste.jsf?language=en&num=C-58/08 [Accessed 17 May 2016].

R

RASHDI, Z.A., DICK, M. and STONY, I (2015) *A conceptual framework for accountability in cloud computing service provision*. Australasian Conference on Information Systems (ACIS). https://acis2015.unisa.edu.au/wp-content/uploads/2015/11/ACIS_2015_paper_221.pdf [Accessed 25 April 2016].

REED, C. (2010) *Information "ownership" in the cloud*. SSRN. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1562461. [Accessed 14 March 2016].

REED, C. (2012) *Making laws for cyberspace.* Oxford: Oxford University Press.

Regulation (EC) No. 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I). Eur-Lex. http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32008R0593 [Accessed 2 April 2016].

Regulation (EC) No. 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations (Rome II). Eur-Lex. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32007R0864&from=en [Accessed 4 April 2016].

Regulation (EU) No. 1215/2012 of the European Parliament and of the Council of 12 December 2012, on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast). Eur-Lex. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32012R1215&from=EN [Accessed 18 January 2016].

REIN, W. (2011) *The changing meaning of "personal data".* Lexology. http://www.lexology.com/library/detail.aspx?g=7f27f25f-0076-4ec0-86ac-7cf81c5a62d1 [Accessed 22 February 2016].

RICKY, M. and MAGALHAES, M.L. (2015) Cloud data jurisdiction: The provider, the consumer and data sovereignty. Cloud Computing. http://www.cloudcomputingadmin.com/articles-tutorials/compliance-regulations/cloud-data-jurisdiction-provider-consumer-and-data-sovereignty.html [Accessed 17 February 2016].

ROBERTS, S. (2011) *'Administrability and business certainty in abuse of dominance enforcement: An Economist's review of the South African record'*. Compcom. http://www.compcom.co.za/wp-content/uploads/2014/09/Administrability-bus-certainty-in-abuse-30092011.pdf [Accessed 8 August 2016].

ROBERT, S. (2013). *Privacy, technology and national security. An overview of intelligence collection.* Office of the Director on National Intelligence. Brookings Institution. https://www.dni.gov/index.php/newsroom/speeches-and-interviews/195-speeches-interviews-2013/896-privacy,-technology-and-national-security-an-overview-of-intelligence [Accessed 12 July 2016].

ROCET, J.C. and TIROLE, J. (2003) *Platform competition in two-sided markets,* Research Center for Humanities and Social Sciences. http://www.rchss.sinica.edu.tw/cibs/pdf/RochetTirole3.pdf [Accessed 22 May 2106].

ROLF, H. et al. (2014) Cloud computing: A cluster of complex liability issues. *European Journal of Current Legal Issues.* http://webjcli.org/article/view/303/418 [Accessed 14 May 2016].

S

Safe Harbour Agreement http://2016.export.gov/safeharbor/ [Accessed 22 November 2016].

SAS. (n.d.) Big Data, What it is and why it matters. *Big data is a term that describes the large volume of data – both structured and unstructured – that inundates a business on a day-to-day basis. But it's not the amount of data that's important. It's what organizations do with the data that matters. Big data can be analysed for insights that lead to better decisions and strategic business moves*. SAS. https://www.sas.com/en_us/insights/big-data/what-is-big-data.html [Accessed 29 May 2016].

SCHEDLER, A. et al. (eds.) (1999) *Conceptualizing accountability the self-restraining state: Power and accountability in new democracies*. London: Lynne Reiner Publishers.

SCHOFIELD, A. and ABRAHAMS, L. (2015) *Research study on the use of cloud services in the South African Government.* Joburg Centre for Software Engineering. Wits University. https://www.jcse.org.za/sites/default/files/%5Bfilename%5D.pdf [Accessed 15 May 2016].

SCHONBERGER, V.M. and CUKIER, K. (2013) *Big Data: A revolution that will transform how we live, work.* London: John Murray Publishers.

SCHWARTZ, P.M. (2013) *Information privacy in the cloud.* Berkeley Law. http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=2907&context=facpubs [Accessed 20 March 2016].

SCHWARTZ, P.M. and SOLOVE, D.J. (2014) *Reconciling Personal Information in the United States and European Union*: Berkeley University. http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=4252&context=californialawreview. [Accessed 7 February 2016].

SCHWARTZ, P.M. and SOLOVE, D.J. (2011) *The PII problem: Privacy and a new concept of personally identifiable information.* SSRN. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1909366 [Accessed 19 March 2016].

SCOTT, R.J. (2012) *Understanding the legal risks of cloud computing navigating the network security and data privacy issues associated with cloud services.* Thomas Reuters Aspatore. https://www.scottandscottllp.com/main/uploadedFiles/resources/Articles/ScottChapter.pdf [Accessed 15 May 2015].

SEAGATE. (n.d.) *Data centre management: Trends and challenges.* SEAGATE. http://www.seagate.com/gb/en/tech-insights/data-center-management-master-ti/. [Accessed 16 January 2016].

Section 164.514a. Government Publishing Office. https://www.gpo.gov/fdsys/pkg/CFR-2016-title45-vol1/pdf/CFR-2016-title45-vol1-sec164-514.pdf [Accessed 12 February 2016].

SHELTON, T. (2013) *Business models for the social mobile cloud transform your business using social media, mobile internet and cloud computing.* Where published? : John Wiley and Sons Inc., http://adnanalhashmi.weebly.com/uploads/2/3/7/6/23764062/business_models_for_the_social_mobile_cloud.pdf [Accessed 14 October 2016].

SHAPIRO, A.L. (1999) *The control revolution: How the internet is putting individuals in charge and changing the world we know.* 2nd. ed. New York: Public Affairs.

SILALASHI, J.M. (2011) Drafting a cloud computing contract. Academia. http://www.academia.edu/3208923/Drafting_a_Cloud_Computing_Contract [Accessed 12 March 2016].

SINGEL, R. (2009) *Netflix spilled your Brokeback Mountain secret, lawsuit claims*. Wired. https://www.wired.com/2009/12/netflix-privacy-lawsuit/ [Accessed 28 March 2016].

SKYHIGH. (2015*) Cloud adoption and risk report Q2 2015.* SKYHIGH. https://uploads.skyhighnetworks.com/2015/03/Skyhigh-Cloud-Report-Q1-2015d.pdf [Accessed 7 May 2016].

SLUIJS, J.P., LAROUCHE, P. and SAUTER, W. (2012a) *Cloud computing in the EU policy sphere interoperability, vertical integration and the internal market*. Tilburg Law and Economics Center, https://www.jipitec.eu/issues/jipitec-3-1-2012/3320/sluijs.pdf [Accessed 12 January 2016].

SLUIJS, J.P., LAROUCHE, P. and SAUTER, W. (2012b) *Cloud computing in the EU policy sphere interoperability, vertical integration and the internal market.* Tilburg Law and Economics Center (TILEC). https://www.jipitec.eu/issues/jipitec-3-1-2012/3320/sluijs.pdf [Accessed 24 February 2016].

SLUIJS, J.P. (2012) *Network neutrality and internet market fragmentation.* TILEC Discussion Paper No. 2012-015, Common Market Law Review, 49 (5), 2012. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2038733. [Accessed 24 April 2016].

SMITH, B. (2010) *Building confidence in the cloud: A proposal for industry and government action for Europe to reap the benefits of cloud computing.* European Commission EC Justice News. http://ec.europa.eu/justice/news/consulting_public/0003/contributions/organisations/microsoft_corporation_2nd_document_en.pdf [Accessed 16 September 2015].

SMITH, B. (2010) *Cloud computing for business and society at the Brookings Institution.* Brookings Institution. Http://www.brookings.edu/events/2010/01/20-cloud-computing [Accessed 23 May 2015].

SOLOMECKE, C. (2013) *The legal aspects of cloud computing under Copyright law.* WBS Law. https://www.wbs-law.de/eng/it-law/the-legal-aspects-of-cloud-computing-under-copyright-law-45886/ [Accessed 12 April 2016].

The South African Law Commission. (1998) *Report Project 47. Unreasonable stipulations in contracts and the rectification of contracts.* http://www.justice.gov.za/salrc/reports/r_prj47_contracts_1998apr.pdf [Accessed 3 February 2016].

The South African Law Reform Commission. (2005) *Privacy and Data Protection Discussion Paper 109 Project 124.* Justice Department. *http://www.justice.gov.za/salrc/dpapers/dp109.pdf* [Accessed 6 January 2016].

South African Legal Information Institute. (2014) *POPI – Is South Africa keeping up with international trends?* SAFLLI. http://www.saflii.org/za/journals/DEREBUS/2014/84.pdf [Accessed 11 March 2016].

STONE, B. and STELTER, B. (2009) Facebook withdraws changes in data use*. New York Times*. http://www.nytimes.com/2009/02/19/technology/internet/19facebook.html?_r=0 [Accessed 22 April 2016].

STONEBRAKER, M. (n.d.) "One Size Fits All": An idea whose time has come and gone. Computer Science and Artificial Intelligence Laboratory. MIT. https://cs.brown.edu/~ugur/fits_all.pdf [Accessed 12 February 2016].

STRANEX, M. (n.d.) *Judgements on Copyright 18, Case, Technical Information systems Pty Ltd v. Marconi Pty Ltd..* The Law Publisher CC, http://library.sun.ac.za/SiteCollectionDocuments/eresources/Judgments%20on%20Copyright-18.pdf [Accessed 2 March 2016]. *Adaptation of a computer programme for use by an end-user by the removal of the licence agreement by the party given the right to copy and distribute the programme for end-users constitutes an adaptation of the programme*.

STREEL, A. (2012) *Where should the European Union intervene to foster the internal market for eComms?* SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2112879 [Accessed 7 April 2016].

SUBAFILMS, LTD; The Hearst Corp., Plaintiffs-counter-defendants-Appellees, v. MGM-PATHE COMMUNICATIONS CO., FKA MGM/UA Communications Co. and as United Artists Corporation; MGM/UA Home Video, Inc.; Warner Home Video, Inc.; Warner Bros. Inc., Defendants-counter-claimants-Appellants. And SUBAFILMS, LTD; The Hearst Corp., Plaintiffs-Appellants, v. MGM-PATHE COMMUNICATIONS CO., FKA MGM/UA Communications Co. and as United Artists Corporation; MGM/UA Home Video, Inc.; Warner Home Video, Inc.; Warner Bros. Inc.; United Artists Corporation, Defendants-Appellees. Nos. 91-56248, 91-56379 and 91-56289. United States Court of Appeals, Ninth Circuit. Argued and Submitted February 24, 1994. Decided May 13, 1994. H2O Harvard Law School. https://h2o.law.harvard.edu/collages/5474 [Accessed 5 April 2016].

SVANTESSON, D.J.B. (2014) *Delineating the reach of internet intermediaries' content blocking – "ccTLD Blocking", "Strict Geo-location Blocking" or a "Country Lens Approach"?* 11 (2). Scripted. https://script-ed.org/wp-content/uploads/2014/10/svantesson.pdf [Accessed 12 April 2016].

SWEENEY, L. (2013) *Discrimination in online ad delivery.* SSRN. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2208240 [Accessed 23 March 2016].

SWEENEY, L. (1997) Weaving technology and policy together to maintain confidentiality. *Journal of Law, Medicine and Ethics*. http://onlinelibrary.wiley.com/doi/10.1111/j.1748-720X.1997.tb01885.x/abstract [Accessed 11 February 2016].

SZOLDRA, P. (2016) This is everything Edward Snowden revealed in one year of unprecedented top-secret leaks*. Business Insider*. http://www.businessinsider.com/snowden-leaks-timeline-2016-9. [Accessed 28 October 2016].

T

TAYLOR, S. (2013) *Reding warns against identity changes to bypass data privacy. Commissioner gets tough on pseudonymous data.* European Voice. http://www.politico.eu/article/reding-warns-against-identity-changes-to-bypass-data-privacy/ [Accessed 15 March 2016].

THOMAS, E. PUTTINI, R. and ZAIGHAM, M. (2013) *Cloud computing: Concepts technology & architecture.* Cape Town: The Prentice Hall Services Technology series.

The T.J. Hooper. The Northern No. 30 and No. 17. The Montrose. In re Eastern Transp. Co. New England Coal & Coke Co. v. Northern Barge Corporation. H.N. Hartwell & Son, Inc. v. Same. No. 430. Circuit Court of Appeals, Second Circuit. July 21, 1932. 60 F.2d 737 (1932). Harvard Law. https://h2o.law.harvard.edu/collages/4968 [Accessed 18 February 2016].

TIAN, G. (2014) *Don't sue us for search: Google's unnecessary safe harbour appeal.* University of Hertfordshire. *http://www.herts.ac.uk/tim-test-site/test-16-conversation-import/conversation-remote?sq_content_src=%2BdXJsPWh0dHBzJTNBJTJGJTJGdGhlY29udmVyc2F0aW9uLmNvbSUyRmRvbnQtc3VlLXVzLWZvci1zZWFyY2gtZ29vZ2xlcy11bm5lY2Vzc2FyeS1zYWZlLWhhcmJvdXItYXBwZWFsLTI0NDA1JmFsbD0x* [Accessed 15 February 2016].

TIAN, Y. (2009) *Rethinking intellectual property: The political economy of copyright*. London: Routledge-Cavendish.

TRICHKOVSKAX, C. (2011) Legal and privacy challenges of social networking sites. Duo UIO. https://www.duo.uio.no/bitstream/handle/10852/22928/CvetankaxTrichkovskaxThesis.pdf?sequence=1 [Accessed 24 January 2016].

TRIMBLE, M. (2014) *Advancing national intellectual property policies in a transnational context*, University of Nevada. School of Law. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2418620 [Accessed 3 April 2016].

TRIMBLE, M. (2012) *The future of cybertravel: Legal implications of the evasion of geolocation*. Las Vegas. University of Nevada. http://scholars.law.unlv.edu/cgi/viewcontent.cgi?article=1661&context=facpub [Accessed 18 May 2016].

2TWENTY4CONSULTING. (2017) *GDPR and cloud service providers.* Legal Technology. https://www.legaltechnology.com/wp-content/uploads/2017/03/GDPR-Essential-Guide-Cloud.pdf [Update-Accessed 18 March 2017].

U

Unitary patent: Uniform protection across 26 EU countries. EC Europa. https://ec.europa.eu/growth/industry/intellectual-property/patents/unitary-patent_en [Accessed 12 February 2016].

United Kingdom Data Protection Act of 1998. United Kingdom Government. http://www.legislation.gov.uk/ukpga/1998/29/contents [Accessed 12 February 2016].

United Kingdom of Great Britain and Northern Ireland v. European Parliament and Council of the European Union. Regulation (EC) No. 460/2004 – European Network and Information Security Agency – Choice of legal basis. Case C-217/04, Curia Europa. http://curia.europa.eu/juris/liste.jsf?language=en&num=C-217/04. [Accessed 17 May 2016].

University of Cambridge Research. (2013) *Digital records could expose intimate details and personality traits of millions.* Cambridge Press. http://www.cam.ac.uk/research/news/digital-records-could-expose-intimate-details-and-personality-traits-of-millions [Accessed 12 March 2016].

University of Cape Town. (n.d.) *Sources of law*. E-transactions law. http://www.etransactionslaw.uct.ac.za/elaw/lectures/intro/law_sources [Accessed 15 April 2016].

The USA PATRIOT Act 2006: Preserving Life and Liberty (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism), Department of Justice. https://www.justice.gov/archive/ll/highlights.htm [Accessed 9 July 2016].

The USA PATRIOT Act: *MYTH VS. REALITY*. Justice Department. https://www.justice.gov/archive/ll/subs/add_myths.htm [Accessed 25 February 2016].

V

VALENTINO-DEVRIES, J. and SINGER-VINE, J. (2012) They know what you're shopping for. *The Wall Street Journal.* http://www.wsj.com/articles/SB10001424127887324784404578143144132736214. [Accessed 7 March 2016].

Vanguard Rigging (Pty) Ltd v. Nordengen and Another (983/2012) [2012] ZAGPJHC 284 (30 November 2012). Southern African Legal Information Institute. http://www.saflii.org/za/cases/ZAGPJHC/2012/284.html [Accessed 14 March 2016].

Viacom Int'l Inc. v YouTube, Inc., 07 Civ. 2103 (S.D.N.Y. April 18, 2013). JOLT Law Harvard. http://jolt.law.harvard.edu/digest/copyright/district-court-grants-summary-judgment-to-youtube-in-viacom-v-youtube-again [Accessed 15 April 2016].

VINELLI, R. (2009) Bringing down the walls: How technology is being used to thwart parallel importers amid the international confusion concerning exhaustion of rights*. Cardozo Journal of International and Comparative Law*. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1346668 [Accessed 5 April 2016].

Volker und Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v. Land Hessen. References for a preliminary ruling: Verwaltungsgericht Wiesbaden - Germany. Joined cases C-92/09 and C-93/09. Eur-Lex. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62009CJ0092 [Accessed 30 May 2016].

W

WALKER, S. and GREENE C. (2007) '*What constitutes a material breach'.* The Lawyer. [https://www.thelawyer.com/issues/8-january-2007/get-out-flaws/ [Accessed 12 August 2016].

WATAL, J. (2011) *From Punta Del Este to Doha and Beyond: Lessons from the TRIPs negotiating processes*, analysis of intellectual property issues. *World Intellectual Property Organization Journal* (WIPO), 3 (1). http://www.wipo.int/edocs/pubdocs/en/intproperty/wipo_journal/wipo_journal_3_1.pdf [Accessed 8 April 2016].

WATROUS, L. (2016) The cloud and the race to zero: Amazon and Google go at I.T. *Huffington Post.* http://www.huffingtonpost.com/lucinda-watrous/the-cloud-and-the-race-to_b_10458826.html [Accessed 14 December 2016].

WEBER, R. H. (2010) *Internet of things – New security and privacy challenges.* Semantic Scholar. https://pdfs.semanticscholar.org/9d65/08a44e957d837490d69936db5a211432a411.pdf [Accessed 18 January 2016].

WEBER, R.H. and GROSZ, M. (2008) *Legitimate governing of the internet.* Syracuse University. https://listserv.syr.edu/scripts/wa.exe?A3=ind0809&L=GIGANET-MEMBERS&E=base64&P=1330&B=----------

06050808070401080403040 4&T=application%2Fpdf;%20name=%2220080905131356956.pdf%22&N=20080905131356956.pdf [Accessed 14 April 2016].

WEITZNER, D.J. et al. (2008) *Information accountability*. MIT Computer Science and Artificial Intelligence Laboratory. http://dig.csail.mit.edu/2008/06/info-accountability-cacm-weitzner.pdf [Accessed 22 March 2016].

WIDMER, U. (2009) *Telecommunications media & technology. Cloud computing – ICT as a service*, Who's Who Legal. http://whoswholegal.com/news/features/article/18246/cloud-computing-data-protection/ [Accessed 4 May 2015].

WILCOX, M. (2016) *The real reason why Google Flu Trends got big data analytics so wrong*. Forbes. http://www.forbes.com/sites/teradata/2016/03/04/the-real-reason-why-google-flu-trends-got-big-data-analytics-so-wrong/#335126501cb1 [Accessed 20 March 2016].

WILSON, S. (2014) *Facebook's facial recognition technology is a massive surveillance project.* ZDNET. http://www.zdnet.com/article/facebooks-facial-recognition-technology-is-a-massive-surveillance-project/ [Accessed 21 November 2016].

Wintersteiger AG v. Products 4U Sondermaschinenbau GmbH, C-523/10. Curia Europa. http://curia.europa.eu/juris/document/document.jsf?text=&docid=121744&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=150477 [Accessed 18 January 2016].

WIPO Copyright Treaty. (Adopted in Geneva on December 20, 1996) WIPO Int. http://www.wipo.int/treaties/en/text.jsp?file_id=295166%20.#P78_9739 [Accessed 17 January 2016].

WIPO. (1996) Agreed statements concerning the WIPO Copyright Treaty. WIPO Int. http://www.wipo.int/treaties/en/text.jsp?file_id=295456 [Accessed 26 February 2016].

WIPO. (2014) *Director Gurry Speaks on Naming New Cabinet, Future of WIPO.* IP watch. http://www.ip-watch.org/2014/05/08/wipo-director-gurry-speaks-on-naming-new-cabinet-future-of-wipo/ [Accessed 21 April 2016].

WIPO Performances and Phonograms Treaty (WPPT) (adopted in Geneva on December 20, 1996), WIPO. *http://www.wipo.int/edocs/lexdocs/treaties/en/wppt/trt_wppt_001en.pdf* [Accessed 12 April 2016].

WIPO. (2013) Main provisions and benefits of the Marrakesh Treaty (2013). WIPO. *http://www.wipo.int/edocs/pubdocs/en/wipo_pub_marrakesh_flyer.pdf* [Accessed 12 April 2016].

WISEMAN, L. (2012) *Copyright and the challenge of the new*. Wolters Kluwer Information Law Series. 25. Netherlands.

WHITTAKER, Z. (2014) *Dropbox under fire for 'DMCA takedown' of personal folders, but fears are vastly overblown.* ZDnet. *http://www.zdnet.com/article/dropbox-under-fire-for-dmca-takedown-of-personal-folders-but-fears-are-vastly-overblown*. [Accessed 14 April 2016].

World Intellectual Property Organization. (n.d.) *WIPO*. *Internet Treaties.* WIPO. http://www.wipo.int/copyright/en/activities/internet_treaties.html [Accessed 14 April 2016].

World Intellectual Property Organization. (n.d.) *Internet Treaties*, WIPO. http://www.wipo.int/copyright/en/activities/internet_treaties.html [Accessed 12 January 2015].

Y

YU, P.K. (2012) Region codes and the territorial mess. *Cardozo Arts and Entertainment Law Journal*. *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2026737* [Accessed 4 April 2016].

Z

ZUCKERBERG, M. (2007) *Thoughts on Beacon.* Facebook. *https://www.facebook.com/notes/facebook/thoughts-on-beacon/7584397130/* [Accessed 5 April 2016].

Index