GSR 2012 Discussion Paper

The Cloud: Data Protection and Privacy

Whose Cloud is it Anyway?

Work in progress, for discussion purposes

Comments are welcome!

Please send your comments on this paper to: gsr@itu.int by 19 October 2012.

The views expressed in this paper are those of the author and do not necessarily reflect the opinions of Charles Russell LLP, ITU or its Membership.

TABLE OF CONTENTS

1 THE CLOUD: DATA PROTECTION AND PRIVACY WHOSE CLOUD IS IT ANYWAY?

Author: Stephanie Liston, Senior Counsel (Charles Russell LLP)[1]

INTRODUCTION

"To secure the public good and private rights, against the danger of … faction, and at the same time to preserve the spirit and form of popular government, is then the great object to which our enquiries are directed"[2]

Like James Madison and the Federalists, new technologies engendered by the advent, growth and development of the Internet pose challenges for policymakers and regulators. Technical innovation itself is breaking down traditional barriers and creating significant commercial opportunities for economic growth and wealth creation.

The object of this paper is to consider, in the cloud: how to protect an individual's privacy and personal data? To what extent regulation is required to protect privacy? And, how to apply effective, efficient, clear, balanced and proportionate regulation in relation to cloud services provided over the Internet – a global communications network with no stop lights or zebra crossings.

Cloud computing has been recognised as a technology "game changer".[3] European Commission (EC) Vice President Neelie Kroes included cloud services with e-Health and ConnectedTV as offering huge benefits for citizens and businesses, and an overall boost to the European economy.[4]

Cisco has produced a global cloud index. It has predicted:

- "Annual global Cloud IP traffic will reach 1.6 zettabytes by the end of 2015. In 2015 global Cloud IP traffic will reach 133 exabytes per month.
- Global Cloud IP traffic will increase twelvefold over the next 5 years. Overall, Cloud IP traffic will grow at a CAGR of 66 percent from 2010 to 2015.
- Global Cloud IP traffic will account for more than one-third (34 percent) of total data center traffic by 2015."[5]

In terms of revenue, the global cloud computing market is forecast to grow 22 percent annually to US$241 billion by 2020.[6]

This paper will briefly consider the definition of cloud services together with their economic and social benefits[7]; current privacy and data protection regulation as applied to cloud services; the effectiveness of current regulation and enforcement to preserve privacy; and consider a fit for purpose regulatory model that effectively balances commercial needs and opportunities, technological reality and a citizen's reasonable expectation of privacy in an international digital eco-system.

1 *THE CLOUD: WHAT IS IT?*

1.1 Consideration of the Definition of Cloud Computing

The definitions of the cloud are many and various. They range from a simplistic statement that it is the use of virtual servers available on the Internet to anything consumed outside a firewall, including conventional outsourcing. Cloud computing has been compared to the supply of utilities such as gas and electricity. "The shift from local software to Cloud computing has been compared to the switch from local electricity generation to electricity grids in the 20th Century."[8]

This definition captures the essence of cloud computing:

- Cloud computing provides flexible, location-independent access to computing resources that are quickly and seamlessly allocated or released in response to demand.
- Services (especially infrastructure) are abstracted and typically virtualised, generally being allocated from a pool shared as a fungible resource with other customers.
- Charging, where present, is commonly on an access basis, often in proportion to the resources used.[9]

Clouds, by any definition, do not respect international boundaries unless they have to. However, with the type of personal data they hold, uploaded by individuals, businesses and governments it is fundamental that clouds are trusted and accepted – perhaps as much or more than a tax haven.

There are three primary types of cloud computing service models:

- Infrastructure as a Service (***IaaS***):
  A cloud based virtual server providing networking and storage services and other infrastructure services. The customer does not manage or control the data centre but may have control over the data or operating systems placed into the infrastructure. For example, Amazon web service or AWS.

  The market was worth US$1 billion in 2011 and is estimated to be worth about US$7 billion by 2013.

- Platform as a Service (***PaaS***)
  Where a customer can use its own applications on the Cloud Service Provider (***CSP***)'s infrastructure. The customer can control the data, the applications and part of the hosting environment.

  The market was worth US$2 billion in 2011 and is estimated to be worth about US$8 billion by 2013.

- Software as a Service (***SaaS***)
  This is the most commonly used form of Cloud services. Customer access the CSP's applications through the Internet. Facebook, webmail and other social networking sites fall into this category.

  The market was worth US$15 billion in 2011 and is estimated to be worth about US$17.5 billion by 2013[10].

These services do not necessarily respect clear boundaries. They may be layered, stacked or intertwined to create a particular or bespoke service model. Existing models have been described as private cloud, community cloud, public cloud or hybrid cloud:

- Private cloud refers to infrastructure owned by or operated for the benefit of one (typically large) customer. It can be located on or off the customer's premises.
- Community cloud refers to infrastructure owned by or operated for, a number of organizations on a shared basis. It supports a specific limited group of users with specific common interests, such as governments.
- Public cloud refers to infrastructure shared among a variety of users with no particular set of interests. It is sometimes described as "multi-tenanted". The infrastructure is owned by the organization selling cloud services.
- Hybrid cloud refers to infrastructure and services that incorporate two or more of the above. An example would be a bank operating a private cloud for sensitive data and putting other data into the public cloud to lower costs and extend capacity.

1.2 **Economic Benefits**

The demand for data storage is expanding dramatically with the exponential growth in data production, digital stores, digital libraries, digital archives, usage and retention requirements. The use of cloud services by individuals (webmail, social networking sites, e-commerce) is now part of everyday life in developed countries. Cloud services are used for wholesale or trade purposes (which is the primary focus of this paper) as well as for personal or individual use.

E-commerce brings people and businesses together internationally and has the potential to drive dramatic economic growth.

Governments looking at ways to economise and provide optimal services to its citizens in e-learning and e-health, for example, have the opportunity to use this technology to bring enormous social benefits.

Though there are infrastructure challenges in the developing world, such as lack of broadband access as well as power shortages and outages, the potential to use cloud services to increase educational opportunities and spread health benefits is enormous.

Basic commercial advantages of cloud services include:

- Lower costs of IT services provision because companies can share resources in one place; users can avoid expenditure on hardware and software; consumption is billed as a utility with minimal upfront costs; typically low, fixed periodic service charges; applications are updated without expensive upgrades; and the cost per user of cloud computing decreases as the number of users increases.
- Customers have access to a wide and growing range of applications without having to download or install anything.
- Access to the cloud is available anytime and anywhere.
- The cloud provides flexibility to accommodate increasing and decreasing demand. The customer only pays for the services it takes.
- Green objectives: pooled resources enable use of centralized and more energy efficient data centres and efficient energy supply strategies[11].

1.3 **Cloud Economics, Freedom and Flexibility v Personal Privacy and Data Protection**

There is a significant tension between the financial benefits cloud services offer to governments, businesses, citizens and consumers and the risks such services may pose to an individual's privacy or personal data.

Different stakeholders in the Internet domain value privacy differently. A Policy Department of the European Parliament commissioned a study which articulated the diverse views this way:

"… policy makers have an appreciation of its (privacy's) value because of the role that privacy plays in delineating and characterising society and supporting the exercise of certain other interlinked fundamental rights. Businesses and economic agents value (or, more commonly do not) privacy for the way in which it may enable or deny access to personal data. Finally, individuals can hold competing and at the same time contradictory estimations of what 'privacy' is 'worth' to them: for example – in an abstract sense recognising its importance in contributing to liberal democracy on the one hand, but trading it economically for benefits on the other."[12]

Generational differences may influence individuals' attitudes to privacy and their use of the Internet. The active use of Facebook and other social media sites have made the Internet a place to gather. Freely putting personal information in the cloud, has perhaps desensitised or undervalued an individual's personal information from the individual's perspective. But is this correct? Do consumers have enough information and knowledge about how this data might be used and the possible risk to its security. Personal data is being referred to as "the new oil" from a commercial perspective. Should consumers have an economic right to benefit from trading this data? And if so, what is the intrinsic value of the data?

To what extent should policy makers, regulators (whether ICT or data protection) and business co-ordinate to promote "Cloud Literacy"? If a citizen gives away or trades data in the cloud – an effective regulator should facilitate education of citizens and consumers as to the risks to privacy and their personal data when using cloud services, as

part of its regulatory agenda. The choice, of course, belongs to the individual, but it ideally should be an informed choice.

To what extent should policy makers around the world play a role in protecting personal data if the individual has willingly and knowingly provided it and no longer has a reasonable expectation that the information will remain private? Just as fundamental as an individuals right to privacy of personal information is the individual freedom and privilege to waive that right.

It is clear that the Internet and cloud services are becoming an increasingly significant business tool. However, without clear cloud standards and consistent regulation, trust in electronic transactions will be reduced and the potential benefits will not be achieved. The challenges are to balance the interests of stakeholders, policy makers, governments, businesses, citizens and consumers to arrive at a pragmatic approach to regulation. To be effective, the approach must be consistent, clear and proportionate. It must also acknowledge the global - not geographically confined – nature of the Internet, as well as the pace of technological change.

The next section will consider examples of the patchwork of differing existing regulatory models.

2 *DATA PROTECTION AND PRIVACY REGULATION*

2.1 Background

89 countries have adopted privacy or data protection laws.[13] A critical element of many of these laws is how they regulate international data flows as a mechanism for protecting individual privacy and enforcing national policies.

The Organisation for Economic Co-operation and Development (***OECD***) adopted Guidelines on the Protection of Privacy and Transborder Flows of Personal Data in 1980. Data protection laws were passed in a number of European countries in the 1970s. At a regional level, Convention 108 of the Council of Europe was passed in 1981 and the original EU Data Protection Directive was enacted in 1995 (***European Directive***)[14]. The European Directive places significant emphasis on the location of data; restricting its transfer to countries that do not have similar privacy protections. In contrast, the Asia-Pacific Economic Co-operation (***APEC***) enacted its voluntary Privacy Framework, which provides protection for personal data on an accountability basis in 2004.

When the OECD Guidelines were adopted, the Internet had not emerged. Protecting privacy by restricting the geographic movement of personal information was possible. The data was typically in a physical form – whether it be written, tapes or other physical medium. This continued to be the case in 1995 when the European Directive was implemented.

Business, the economy and technology have fundamentally changed. The economy is increasingly international. Data processing is growing dramatically in importance due to increased data usage and the value of different forms of data. The global economy is currently undergoing an "information explosion" which can "unlock new sources of economic value, provide fresh insights into science and hold governments to account."[15] The advent of the Internet and now the proliferation and potential value of cloud services require a careful re-evaluation of whether the provisions of these guidelines and regulations for the protection of privacy need to be fundamentally re-evaluated, re-constructed and harmonised to be "fit for purpose" at a global level.

The following is a brief review of the existing privacy and data protection frameworks in the European Union, generally, and as implemented in the UK, France and Germany; the United States; Canada; Brazil; South Africa; Japan and India. Countries have been chosen to reflect a diverse group, including both developed and developing countries. Europe is the initial focus and the most extensive because many countries who have adopted or are considering the adoption of data protection regulation have followed the European model. The model is also useful to illustrate the problems presented to business and the economy by the lack of clear and consistent laws implemented seamlessly across international borders.

The focus is on the aspects of the frameworks that are relevant and particularly problematic in the cloud environment. The aspects of privacy and data protection legislation that fundamentally affect cloud computing are (i) the duties of the party controlling the relevant data; (ii) transborder data transfer restrictions; (iii) data security; and (iv) applicable law.

The recent Global Cloud Computing scorecard published by the Business Software Alliance (***BSA Scorecard***) surveyed 24 Countries to map their relative "cloud readiness".[16] The scorecard rated seven policy areas the BSA determined

to be beneficial to cloud services. The study found a sharp divide between developed and developing countries. The Republic of Korea and Japan were high on the list, where as Brazil and South Africa were at the bottom.

This is a recent map providing an indication of where data protection laws are in place or in the legislative process.

PLC : General Counsel briefing: privacy & data protection as at 23 February 2011

2.2 European Union

2.2.1 Privacy

The fundamental principle of privacy in the European Union (EU) is set out in Article 8 of the European Convention on Human Rights which states that "everyone has the right to respect for his private and family life, his home and his correspondence." This right to privacy is not absolute, however, and can be restricted under certain circumstances.

EU privacy law itself has a particular focus on the protection of this personal data and seeks to balance the privacy debate in an era where online content, especially personal data and access to it have developed exponentially. The International Data Corporation (IDC) predicts that the amount of information and content created and stored digitally will grow from 1.8 zettabytes (ZB) in 2011 to over 7 ZB by 2015.[17]

Cloud computing is just the latest technological development driven by this expansion and in turn it brings fresh challenges to the protection of personal data. Data in the cloud may be easy to access and to manipulate, but it is also harder to locate and maintain control over - which makes compliance with EU legislation and, indeed enforcement, particularly difficult.

The EU's e-Privacy Directive[18] is targeted at public communication network providers and states that personal data should only be accessed by authorised personnel for legally authorised purposes, that stored or transmitted personal data should be protected against accidental or unlawful destruction, accidental loss or alteration and unauthorised or unlawful storage processing, access or disclosure. Communication providers are required to implement a security policy for the processing of personal data and national authorities are granted rights to audit such policies. Notification requirements for personal data breaches are also imposed upon the providers.

This has particular and high profile significance in the context of cookies which can be used by operators to gather personal data without the knowledge of the individual user. The amended e-Privacy Directive,[19] which came into effect in 2009, states that Member States may only permit the use of cookies if the data subject has given their consent and has been provided with clear and comprehensive information, particularly in relation to the purposes of the processing. It is unclear to what extent the legislation will be enforceable from a practical perspective.

2.2.2 **Data Protection**

The current European Directive applies to the collection and processing of personal data within the EU. Personal data is defined broadly as "any information relating to an identified or identifiable natural person," whilst processing involves "any operation or set of operations which is performed upon personal data".

The implementing law of an EU Member State is applied to the processing of personal data by an entity established within that state or by equipment situated within that Member State. Entities that determine the purpose and means of the processing of personal data are termed "data controllers", whilst entities that process the personal data on behalf of the data controller are called "data processors".

The European Directive specifies minimum measures to be implemented, leaving Member States the option of putting stricter requirements in place. This has resulted in significant variations in data protection laws across the EU, which cause complex and divergent compliance issues for businesses controlling or processing personal data in Europe, and in fact internationally (see section 2.3 below).

2.2.3 **Duties and Responsibilities of the Cloud Client and the Cloud Service Provider (*CSP*)**

Under the European Directive, data protection obligations are generally imposed upon data controllers, whilst data processors are only subject to specified security requirements. Differing Member State definitions and translations, along with the blurred categorisation of a CSP as a controller or processor make this ambiguity particularly significant.

The cloud client decides the purpose and organisation of any processing and thus, as a data controller, must accept responsibility for abiding by data protection obligations. The CSP will claim that simply hosting the service gives little control over the nature of any processing by the client and thus it cannot also be a controller. The lack of control means that the CSP will attempt to avoid liability for data quality, compliance with individual rights or the obtaining of any consents in relation to personal data and will often include provisions to reflect this within its terms and condition of service – which must be in writing.

The client is often responsible for the full burden of data protection obligations and compliance, despite having little control over the actions of the provider or movement of the data.

2.2.4 **Transborder Data Transfer Restrictions**

Under the European Directive, personal data must not be transferred to non EEA countries that are adjudged to have inadequate personal data protection measures in place. The European Commission (***Commission***) has deemed Andorra, Argentina, Canada[20], the Faroe Islands, Guernsey, the Isle of Man, Israel, Jersey and Switzerland to have adequate protection. The US Safe Harbor Scheme is also accepted as adequate for the purposes of transferring certain personal data, subject to some notable exceptions and now to specific due diligence.

Though there are some exceptions to the rule available, cloud computing is typically conducted without a stable location and providers are unlikely to be based only in the specified countries. The customer may not be able to ascertain the real time location of data that is being processed or stored. Of course, neither will regulators be obliged to enforce the restriction be able to ascertain this information.

The Independent Data Protection Working Party established under Article 29 of the European Directive (***Working Party***) has recently stated that the US Safe Harbor Certification alone may not be deemed adequate. Cloud providers should therefore obtain and retain evidence that certification is both up to date and their cloud provider is compliant with safe harbor requirements.[21]

If transfers need to be made to countries outside those that have "adequate" laws, Standard Contractual Clauses (***SCCs***) may be utilised. The SCCs contain non-negotiable provisions that set out transfer and security measures that have been deemed adequate by the Commission under Article 26(4) of the Directive. The benefit of using the provisions is reduced by registration and approval requirements that apply in some EU Member States. Registering or obtaining approval can be a very time consuming and bureaucratic process.

International businesses can adopt binding corporate rules (***BCR***) which require approval, for the regular transfer of data throughout their corporate networks.

2.2.5 **Data Security**

As data controllers, cloud clients have an obligation to take "appropriate technical and organisational measures to protect personal data"[22], thus data security forms an important aspect of the cloud computing contract.

The Working Party has put forward standardised data protection safeguards to be included in such contracts.[23] These safeguards include technical and organisational measures that aim to preserve the availability, confidentiality, integrity, ability to isolate, accountability, portability and individual rights to the personal data.

Accountability is particularly key to ensuring compliance and thus audit rights are becoming increasingly important to clients. However, the granting of these rights presents a practical problem for providers who use shared infrastructure for their clients. Granting access may itself compromise the confidentiality and security of data belonging to other clients.

Accountability can also be an issue in circumstances where sub-processors are used by the primary cloud provider. Most Member States leave the determination of appropriate technical and organisational measures to data controllers and processors. However, some Member States have prescribed onerous obligations - such as requiring data controllers to independently authorise each subcontractor and enter into direct contracts with all processors in the chain.

2.2.6 **Applicable Law**

The nature of cloud computing with shared resources, constantly moving data and multiple processors and subcontractors means that locating data and the processing of it is inherently difficult. The divergent implementation of the European Directive across the EU causes further problems when considering data protection compliance and which law or laws apply to its movement or processing.

2.2.7 **Compliance with Data Protection Requirements**

In a cloud service relationship, as outlined above, clients will typically bear the risk of data protection compliance despite the providers being responsible for the security and transferring of data. A controller must take appropriate technical and organisational measures to be confident of its compliance. Smaller businesses or individuals may have limited contractual power to negotiate the provider's terms.

Cloud clients are required to exercise due diligence with respect to choosing a provider who offers sufficient guarantees of reliability, competence and security safeguards for the client to be confident it is complying with relevant laws.

CSPs have an opportunity to differentiate their services and enhance business prospects by adopting terms of business and providing assurances to customers as to these processes and compliance. For example, Amazon has created a European Cloud to provide customers with confidence that data will not cross borders in breach of the European Directive. A number of self regulatory codes of practice are being established to address this issue (see section 3.3 below).

2.3 **Example of the Patchwork of Different Practises across the EU**

2.3.1 **United Kingdom**

In the UK, the Data Protection Act 1998 (the ***DPA***) forms the primary legislation that implements the Data Protection Directive. The DPA is regulated in the UK by the Information Commissioner's Office (***ICO***). The ICO's role is to provide guidance on data protection compliance, maintain a register of data controllers and investigate and sanction breaches of the DPA.

The UK Courts have narrowed the meaning of personal data in comparison to mainland Europe[24] so that for the data to be subject to the provisions of the DPA, the data must (i) be biographical in a significant sense; and (ii) "focus" on the individual, rather than some other person or transaction or event.

The ICO has wide ranging enforcement powers which include requiring the production of information; requiring a change of operating practices (a breach of which would be contempt of court); audit powers over central government departments, entry and inspection powers (with a court warrant) and monetary penalty notices of up to £500,000. Criminal sanctions are rare but remain available in certain circumstances, such as a failure to notify the ICO of a DPA breach.

Undertakings from a data controller's CEO are now also seen as a low cost method of enforcement. These undertakings state the failings of the company along with remedial steps that will be taken and are published on the ICO's website.

In the UK the Financial Services Authority is also able to enforce data protection breaches under its own regulatory regime under the Financial Services and Markets Act 2000 (***FSMA***). FSMA places wide obligations on financial services organisations including specific operational rules around data security and handling in its Systems and Controls Rules.

2.3.2 **France**

The implementing data protection legislation in France is the Data Processing, Data Files and Individual Liberties Act[25], as amended (the "DP Act"). This is regulated by the proactive National Commission on Computers and Liberties (***CNIL***).[26]

CNIL has published guidance on the legal processing of personal data which imposes notification and co-operation requirements on data controllers, as well as requirements to keep personal data secure and, in certain circumstances, to obtain CNIL approval prior to processing. Data subjects must also be kept informed of their rights.

There is no obligation to appoint an in-house or external data protection officer, although it is encouraged by the CNIL. Since 2005 more than 7,000 companies and a quarter of those listed on the Paris stock exchange have appointed a data protection officer.

The CNIL are active in regulating data processing and have powers to carry out audits and issue warnings or formal notifications to data controllers who do not comply with their obligations. Should the data controller fail to comply with the CNIL or breach the DP Act, the CNIL may impose an injunction preventing further processing or levy a fine proportional to the seriousness of the transgression. Fines for first breaches may not exceed €150'000, whilst a further breach within 5 years may be fined up to €300,000. Fraudulent or otherwise illegal data collection is governed by the Criminal Code and punishable by up to five years imprisonment and a €300'000 fine.

2.3.3 **Germany**

The use of personal data in Germany is primarily regulated by the Federal Data Protection Act of 1977 (*Bundesdatenschutzgesetz*) (***FDPA***) which has been amended so as to implement the Directive in 2001. Data protection regulations can also be found in the Social Act (*Sozialgesetzbuch*), the Telemedia Act (*Telemediengesetz*) and the Telecommunications Act (*Telekkommunikationsgesetz*).

The German national data protection authority is the Bundesbeauftragte Für den Datenschutz und die Informationsfreiheit (***BFDI***). Each of the federal states (*Lander*) also have their own regional data protection authorities. These regional authorities have recently been subject to scrutiny and restructuring to improve their independence following a European Court judgment in March 2010 which found that Germany had failed to implement the Directive correctly by placing the regional authorities under the state authority.

Personal data should be obtained directly from the data subject unless required by law for a genuine business purpose or if disproportionate effort would be required and there are no indications that the data subject's interests would be affected. Further, the FDPA puts particular emphasis on designing data protection systems to process as little personal data as possible such as through the anonymising or pseudonymising of the data subject. The data controller remains responsible for regulatory compliance and must have a written agreement with any data processor containing specific contractual requirements.

International data transfers are subject to the standard EU principles, save that since April 2010, German data exporters must check whether US data importers that have self-certified under the Safe Harbor scheme are actually compliant. The Working Party has recently endorsed this approach.

The BSA Scorecard points to Germany as an example of a country that threatens to undermine any advantage it may have had in being "cloud ready" by being overly restrictive in its interpretation of the EU Directive, requiring some data to be kept within national borders.

At least one German lawyer has noted that though the regulations are very strict in Germany, their enforcement is relatively lax[27].

Each regional authority can impose fines of up to €300,000 whilst non-compliance can be deemed a criminal offence with imprisonment of up to two years or fines possible. Fines should exceed the economic gain by the offender and may themselves exceed €300,000.

2.3.4 2012 EU Data Protection Proposals

On 25 January 2012, the Commission published its proposed reforms for data protection legislation within the EU.[28] The proposals contain a Regulation (for general and commercial data protection) and a Directive (for processing in the areas of police and criminal justice). The draft Regulation will replace the European Directive which is seen as out of date following numerous technological developments.

The proposals aim to increase an individual's online privacy rights and introduce new obligations on organisations. Contained within a Regulation, the changes will be directly applicable within the Member States in an attempt to harmonise the current "fragmented and outdated" data protection legislative framework. Co-operation between Member States is encouraged with the view that a single data protection regime should reduce red tape whilst ensuring that individuals and organisations are clear on their respective rights and obligations. It is also intended to make compliance more straight forward and consistent.

The key changes that have been proposed include:

- National regulatory authorities will have the power to take action against organizations in other Member States in certain circumstances and may issue fines of up to €1million or 2% of a company's annual turnover in some cases.
- An expanded definition of personal data that captures any information relating to a data subject and a requirement that an individual's consent must be explicit.
- The draft Regulation will have a wider application and include non-EU entities that process personal data that relates to EU citizens.
- Organizations will be required to report data breaches without undue delay and, if feasible, within 24 hours of the breach.
- There will also be requirements on data controllers to carry out data protection impact assessments, appoint data protection officers and inform third parties of any breaches.
- Individuals will be given a new "right to be forgotten" under certain circumstances and will no longer be subject to a fee for subject access requests.
- Finally, international data transfers will be subject to a more detailed regulatory framework requiring safeguards to be in place and authorities to undertake prior checks, whilst the derogations available to data controllers will be more restrictive.

The proposals were announced at the start of 2012. Their controversial nature has and will attract significant lobbying and debate which could mean long delays before implementation. Indeed, the UK Government is already reported to have stated that Member States should have more flexibility over the implementation of the reforms and has questioned the £3billion value of benefits projected by the Commission.

2.4 United States Privacy and Data Protection

US Legislation changed dramatically following the terrorist attacks of 11 September 2001 with the introduction of the US Patriot Act.[29] The US Patriot Act permitted the sharing of personal data of anybody suspected of involvement with terrorism or money laundering activities and introduced a requirement for financial institutions to implement anti-money laundering systems. This combination, in conjunction with multi-chain processes, has resulted in the

possibility of broad access and sharing of personal information. The US Patriot Act has been viewed by Europe as a significant risk to data privacy and has put the Safe Harbor scheme in jeopardy.

The right to privacy has been recognised by the US Supreme Court based on the US Constitution, despite there being no explicit constitutional right contained within it.[30] Many states have privacy protections within their own constitutions. Only California has extended the protection of data from government interference into an obligation on the private sector.[31]

The United States has spawned a wide range of narrowly applicable federal and state laws relating to the use of personal data. This patchwork, similar to the lack of harmony in Member State implementation of the European Directive, is incompatible with the nature of cloud computing. However, businesses and government are working to establish and implement credible self-regulation and guidelines.

Nationally, the Federal Trade Commission Act[32] (***FTC***) prohibits unfair practices. This has been applied to online and offline privacy as well as data security policies. The FTC also monitors and enforces any breach of the Safe Harbor Rules. However, doubts have been raised about the FTC's enforcement effort with respect to the Safe Harbor Rules. The FTC's first action for breach of the Safe Harbor principles was only in 2011 – against Google regarding its Buzz service, for not giving notice or choice to users when it used information collected through Gmail for different purposes.

The Financial Services Modernisation Act (***FCMA***) and Health Insurance Portability and Accountability Act (***HIPAA***) regulate the collection and use of financial and medical information, respectively. Among the range of federal legislation, there are specific acts that regulate, for example, the collection and use of email addresses[33] and telephone numbers[34].

At state level, there are many laws relating to data protection and most states have enacted some form of privacy legislation. Forty-six states have enacted laws requiring notification of security breaches involving personal data. California leads the way with a developed framework that includes an established Office of Privacy Protection and laws comparable to those in Europe. These include requirements for companies to maintain reasonable security measures to protect personal data[35] and to disclose details of third parties with whom they have shared the personal information[36].

There has also been a move toward a more European approach at federal level with the issuing of a Consumer Privacy Bill of Rights in February 2012. This is the first comprehensive privacy bill introduced to the Senate in over a decade. The bill sets out fundamental principles that companies should observe, namely that individuals should control the use of their data whilst maintaining access and correction rights; data use should be secure, transparent and consistent with the context of collection; there should be reasonable limits on what data is collected and retained and companies must remain compliant and accountable. There are also proposals for a national security breach notification law[37] and a requirement for reasonable security policies and procedures to protect computerised personal data.[38] These proposals signal dramatic change to American privacy laws. However, they are yet to gain the requisite support in Congress.

2.5 Data Protection in Canada

The Canadian Charter of Rights and Freedoms contains a right "to be secure from unreasonable search or seizure"[39] which the courts have extended to protect an individual's "reasonable expectation of privacy".[40] Recent case law from the Court of Appeal in Ontario has also introduced a common law tort of invasion of privacy or, specifically, "intrusion upon seclusion".[41.]

At federal level, privacy is regulated by the Privacy Act 1985 and the Personal Information Protection and Electronic Documents Act 2000 (***PIPEDA***). The PIPEDA applies to all regulated activities except where the federal government has determined that provincial law is substantially similar to it. Although the applicable legislation may differ, the relevant provisions will be similar. Provincial legislation that has been found adequate includes the Act Respecting the Protection of Personal Information in the Private Sector 1993 in Québec and the Personal Information Protection Acts 2003 of both Alberta and British Columbia.

Responsibility for personal information falls to the Office of the Privacy Commissioner of Canada at federal level, whilst certain provinces also have their own authorities. Standard exceptions to the application of the legislation apply, but in Alberta and British Columbia, personal information may also be transferred in certain business transactions (such as share sales) without consent, provided the parties comply with certain specified requirements. Consent in Canada may be express, implied or even deemed, depending on a narrowing set of circumstances. The

same sliding scale applies to the level of security requirements which will depend on the sensitivity and amount of information along with the method of its storage.

Canadian laws do not restrict international transfers of personal data. Any transfer remains the responsibility of the disclosing party who must ensure that appropriate protections are in place and the third party will abide by these protections. One aspect that may be considered is the location where the data may be held. Consent to the transfer must be obtained from the data subject, although this may be implied via consent to general terms and conditions. Provinces tend to impose additional requirements upon disclosing parties such as developing specific policies and taking reasonable steps to ensure security measures are maintained. There is also no approval procedure for data transfer agreements in Canada and, indeed, no standard form agreements have been approved by the national authorities.

2.6 Brazil's Data Protection Regime

Brazil is yet to implement specific data protection legislation although its Constitution does set out fundamental rights to both privacy and secrecy of correspondence.[42] The Civil Code also provides (i) that an individual may request relief from any threat to personality rights,[43] and (ii) that the private life of an individual is inviolable and judges may be asked to take steps to prevent actions contrary to it.[44]

There are also broad protections within the Consumer Protection Code.[45] These include consumer rights of access and correction to any recorded personal data, requirements for such records to be clear and objective with the recording of negative information limited to five years and a requirement for inaccurate data to be promptly corrected with the correction conveyed to any possible addressee within five business days. The Pubic Prosecutor's Office can enforce privacy rights whilst government authorities, such as the Bureau of Consumer Protection, can impose administrative fines of up to $1.7million if consumer rights are involved.

The current lack of legislation gives no reference or certainty to companies that process personal data and this, along with varying case law, potentially makes operating cloud services in or to Brazil unattractive. As a result, the BSA Scorecard has put Brazil at the bottom of the list of "cloud ready" countries.

A specific Brazilian Data Protection bill is now in the pipeline and Congress is soon to vote on the first reading of a bill that sets out a general legal framework for the Internet, the "Marco Civil da Internet" (***MCdI)***.

The MCdI is heavily based upon European legislation and covers Internet access, network neutrality, the liability of Internet services providers, data retention and the necessity of a judicial order for law enforcement authorities to obtain users' personal data. It places limits on collection and usage of personal data, with an individual's consent required for any processing, whilst companies would also have to notify a newly established "National Data Protection Council" (***NDPC***) in the event of a data security breach. This central authority would publish compulsory compliance recommendations and have powers including suspensions, prohibitions and media announcements. The MCdI also obligates personal data processing companies of more than 200 employees to appoint a data protection officer who would have to report directly to the NDPC and be responsible for all of the company's personal data processing.

2.7 South Africa's Data Protection Regime

South Africa currently has no specific data protection legislation but a right to privacy is set out within its Constitution. There are also relevant personal information provisions contained within the Consumer Protection Act 2008 (***CPA***) and the Electronic Communications and Transactions Act 2002 (***ECT***). Compliance with the latter is voluntary and any adherence must be recorded in an agreement with the data subject.

There is, however, a new Protection of Personal Information Bill (***POPI***) which is making its way through the South African Parliament. The POPI's aim is to regulate the processing of personal data and in doing so establish an Information Protection Regulator to oversee its administration. The final provisions of the POPI are subject to change, but personal information carries a broad definition, covering information relating to an identifiable juristic person, which includes corporate entities and trusts. Correspondence that is implicitly or explicitly confidential is also covered by the definition.

The POPI imposes eight mandatory information protection conditions upon data controllers: accountability; processing limitation; purpose specification; further processing limitation; information quality; openness; security safeguards and data subject participation.

Similar to the European Directive, the current draft bill prevents the international transfer of personal information unless specific provisions are met.[46] Such transfers are only permitted by a "responsible party" and subject to specific requirements. These include consent from the data subject; the international recipient being subject to laws or contracts containing comparable levels of protection to the POPI; the transfer being necessary for the performance of a contract to which the data subject is a party or that benefits him, or the transfer benefiting the data subject and it being not reasonably practicable to obtain consent (but if it were the data subject would be likely to give such consent).

A South African data protection regulator will not be established until the implementation of the POPI. Future failures to comply with notices under the POPI or obstructing the regulator will be punishable by a fine of up to ZAR10million or imprisonment of up to ten years.

2.8 Data Protection in the Kingdom of Saudi Arabia

The Kingdom of Saudi Arabia currently has no specific data protection legislation, although a right to privacy is established in a number of different Saudi Arabia laws. Saudi Arabia's Basic Law of Governance sets out the overriding principle that all correspondence and communications between parties should be kept strictly confidential and should not be disclosed. This overriding principle is supported by provisions contained in other legislation, including the Saudi Arabia Telecommunications Act issued under the Council of Ministers Resolution no. 74 (2001) (**Telecommunications Act**) and the Saudi Arabia Anti-Cyber Crime Law 2007 issued by Royal Decree no. M/17 (**Anti-Cyber Crime Law**). There are also particular laws and regulations in Saudi Arabia which provide for the protection of data and confidential information held by various entities, including financial and insurance institutions, hospitals and the majority of Government entities.

The Telecommunications Act regulates internet service providers and telecommunication companies in Saudi Arabia. It prohibits internet service providers and telecommunication companies from, amongst other things, disclosing any information relating to their subscribers and customers and from intercepting telephone calls or data carried on the public telecommunications network (Article 38.7). It also prohibits internet service providers and telecommunication companies from intentionally disclosing the information or contents of any message intercepted in the course of its transmission, other than in the course of duty (Article 38.13).

If no relevant legislation containing specific data protection and privacy provisions can be applied to the facts in question, the Saudi Arabia courts will apply Shari'ah or Islamic law. The Shari'ah principles establish a tort claim for damages for the wrongful disclosure of a person's personal information where that disclosure results in loss or harm to the individual. The degree of liability and penalties for breaching Shari'ah law relating to the protection of personal information will be determined on a case by case basis, although severe penalties may be imposed.

As indicated above, Saudi Arabia has no data protection authority or national regulator. However, the Telecommunications Act imposes a fine up to Saudi Riyals (SAR) 5,000,000 for failure to comply with the provisions thereof.

The Anti-Cyber Crime Law also imposes a number of civil and criminal sanctions relating to the breach of the privacy and data protection restrictions/ obligations contained therein, including:

- A fine of SAR 500,000 and/ or up to one year's imprisonment for the interception of data transmitted through an information network without legitimate authorisation;
- A fine of SAR 2,000,000 and/ or up to three years' imprisonment for the illegal access of bank data, credit information or information relating to the ownership of securities; and
- A fine of SAR 3,000,000 and/ or up to four years' imprisonment for unlawfully accessing computers to modify, delete, damage or redistribute personal information.
- A fine of SAR 3,000,000 and/ or up to four years' imprisonment for unlawfully accessing computers to modify, delete, damage or redistribute personal information.

2.9 **Data Protection in the United Arab of Emirates**

The United Arab of Emirates (**UAE**), a federation of seven entities each of which is subject to federal and local laws, currently does not have any specific data protection legislation, although a right to privacy is set out within its Constitution and in various UAE laws.

The UAE Constitution states that an individual enjoys "freedom of communication by post, telegraph or other means of communication and the secrecy thereof shall be guaranteed in accordance with the law." (Article 31).

In addition, the Penal Code (Federal Law 3 of 1987 as amended) establishes certain rights of privacy and the protection of personal data. These include the prohibition of the publication of news, pictures or comments pertaining to the secrets of people's private or family life, even if it is true (Article 378); the prohibition of the interception and/ or disclosure of correspondence or a telephone conversation without the consent of the relevant individuals (Article 380); and the prohibition of any person who because of his profession, craft, situation or art is entrusted with a secret from disclosing or using that secret for his/ her own or someone else's benefit without the consent of the person to whom the secret relates unless otherwise permitted by law (Article 379).

The protection of an individuals personal data and rights to privacy are also established in other legislation and regulations in the UAE, including:

- The UAE Labour Law (Federal Law 8 of 1980) which imposes record-keeping obligations on employers in relation to information pertaining to its employees;
- The UAE Cyber Crimes Law (Federal Law 2 of 2006) which prohibits "hacking";
- The UAE Commercial Transactions Law (Federal Law 18 of 1993) and The Electronic Transactions and Commerce Law (Federal Law 1 of 2006) which imposes record-keeping obligations on banks and commercial traders;
- The UAE Telecommunications Regulatory Authority Privacy of Consumer Information Policy which enshrines the right to the protection of personal information relating to subscribers/ customers by telecommunication service providers; and
- The UAE Medical Liability Law (Federal Law 10 of 2008) which provides for the protection of confidential patient information.

These UAE federal laws are often supported by emirate-level laws, particularly in relation to banks/ financial institutions and telecommunication companies and internet service providers.

It should be noted that there are a number of Free Zones established in the UAE, each of which is subject to its own specific regulations and procedures (including, in certain cases, in relation to data protection and privacy). By way of example, the Dubai International Financial Centre (**DIFC**) enacted the Data Protection Law No.1 of 2007 (**DPL 2007**) which governs the collection and use of personal data in the DIFC. It requires the data to be processed accurately, securely and lawfully and particular care should be taken when processing 'sensitive' personal data.

The UAE has no national data protection regulator or authority responsible for monitoring compliance with the data protection laws. It should however be noted that failure to comply with the data protection laws can lead to both criminal penalties (including imprisonment and/ or fines) and civil remedies.

In the DIFC, the laws and regulations contained within the DPL 2007 are administered and overseen by the Commissioner of Data Protection (**CDP**) (Article 7(1) and 21(2)). The DPL 2007 states that the CDP will need to conduct reasonable and necessary inspections and investigations before notifying a data controller that it has breached or is breaching the DPL 2007 (Article 32). If the laws and regulations have been breached, the CDP may issue a direction to the data controller to do or refrain from doing any act or thing (Article 32(1)); or to refrain from processing any specified personal data or to refrain from processing personal data for a specified purpose or in a specified manner (Article 32(2)).

In addition, the DIFC Court may issue orders which include remedies for damages, penalties or compensation if it thinks it is just and appropriate in the circumstances.

2.10 **Data Protection in India**

There is no specific constitutional right to privacy in India, although the Supreme Court has established that privacy should be included within the Right to Life and Personal Liberty.[47]

The collection and processing of personal data in India is regulated under the Information Technology Act 2000 (***IT Act***). The IT Act states that companies must maintain reasonable security practices whilst processing personal data[48] and if obtained under a contract, such data must not be disclosed in breach of that contract without the data subject's consent.[49] Consequently, international transfers are only subject to consent when data is obtained under contract. The IT Act does not provide a definition of a data controller nor does it include a specific requirement for the form or content of consent.

The Indian Government sought to clarify the IT Act by issuing guidance in April 2011[50] (***2011 Rules***) which stated, among other obligations, that written consent is required for the collection of sensitive personal data and that the processor of any such data must publish a privacy policy on its website. Parties must also comply with internationally recognised reasonable security practices.[51]

A Personal Data Protection Bill was proposed at the end of 2006 with the intention of harmonising data protection regulations within the country, establishing a data protection authority and creating a formal right to privacy. Commentators have said that clauses such as the protection of an individual's "honour and good name" make the protections too broad.[52] It is no surprise that the bill is yet to make it through Parliament.

In the absence of a dedicated Indian data protection authority, breaches of the IT Act are adjudicated by each state's Secretary of the Ministry of Information Technology who is granted sanctioning powers that include imprisonment of up to three years and a fine of up to INR500,000.[53]

2.11 **Japanese Data Protection**

Japan is a member of APEC and as such subscribes to its approach to privacy. The Act on Protection of Personal Information (***PPI Act***)[54] regulates the collection and use of personal data in Japan. Any form of data handling is covered, but the PPI Act only applies to situations involving the personal information of 5,000 or more individuals.

The PPI Act imposes common obligations of consent, security and providing information, alongside additional requirements to supervise employees and third parties who handle the personal data.[55] Consent is not defined, although it can be implied. Specific exceptions from the application of the PPI Act are also outlined. These include the handling of personal information for reporting the news, literary works, academic studies, religion or political related activities.

There is no specific provision within the PPI Act restricting the international transfer of personal information. Similar to the Canadian accountability approach, Japan puts the burden of compliance on the party having prime responsibility for the data. All transfers to third parties carry an obligation to supervise and, should the third party be using the data, consent from the data subject is also required.

The BSA Scorecard indicated that Japan would be an excellent model for those interested in advancing cloud computing. Japan's set of laws "support and facilitate the digital economy and cloud computing – from comprehensive privacy legislation that avoids burdens on data transfers and data controllers …".[56] Japan also leads in the development of international cloud computing standards.

Japan has no data protection authority, but the Consumer Affairs Agency has overall responsibility for deciding basic policy along with limited sanctioning powers such as making recommendations and, if necessary, ordering corrective measures to be taken. Enforcement falls to government departments which regulate data protection within their own sector. Failure to comply with the data protection laws can lead to sanctions from the relevant minister who can impose fines of up to JPY300,000 and six months imprisonment. Guidelines are also frequently issued, with the system relies heavily on self regulation and adherence to these recommendations.

2.12 **The Tension between Freedom and Regulation: Is the Current Patchwork of Regulation Fit for Purpose in the Cloud?**

The short answer is no. National regulation with respect to privacy and data protection was built 20 to 30 years ago. The advent in many countries of a global digital eco-system built on dramatic changes to technology was not foreseen by policy makers or regulators. It is now fundamentally outdated.

The development and deployment of services over the Internet and in the cloud typically cross national boundaries – it is not the exception! To restrict international data flows in the interest of protecting privacy rights is no longer an effective or efficient tool. The diverse set of rules across EU countries, for example, illustrates the complexity created for CSPs and their business customers (i.e. the data controller) to comply with the laws of each jurisdiction in which it operates. The effect is to slow down the growth of cloud services in Europe.[57] If there is not a shift in policy and regulation in Europe, and other countries followings its model, they will not be competitive in areas which should be a major source of economic growth.

The inherent difficulty of enforcing European and other similar transborder data flow restrictions gives rise to a lack of effectiveness in protecting personal data.[58] Policy makers need to address this problem by establishing frameworks which are cloud ready and provide efficient, clear and proportionate protections.

There is increasing confusion as to who has the duty to protect personal data. Clear lines of responsibility need to be established to allow stakeholders to understand and comply with requirements. One party in the chain of cloud activity must take responsibility and be accountable. Regulation should clarify rather than confuse the accountability issue. Individuals must have the absolute privilege to waive their right to privacy.

It is also unclear, in a global eco-system, which jurisdiction has authority to deal with a complaint. Consumers are left wondering who to complain to about services received in the UK, for example, but delivered from abroad. Businesses and CSPs face an equally daunting task of trying to discover exactly with which laws they are required to comply.

Significant security issues surround the development of cloud services. The person accountable for preserving personal data must have and take responsibility for ensuring they take steps to identify exactly how data processing will be managed and effectively protected. A risk assessment will need to be made taking into account practical physical storage concerns, location, technology that may be used to protect data and the ability to move data from one provider to another, as well as the right and ability to have data removed in accordance with applicable data protection regulations.

For cloud services to develop, CSPs need both freedom to innovate and clear direction. The advances being made in self-regulation[59] and the development of privacy enhancing technologies[60] present practical and effective solutions to protect privacy and enhance the security of cloud based services.

Section 5 below describes some best practice policies and recommendations for future data protection and privacy laws that reflect the reality of the international digital economy and promote economic growth while consistently and effectively protecting the privacy of personal information.

2.13 **The Opportunity Cost of Regulation**

Fundamental changes are needed to privacy and data protection legislation and governance to ensure they are fit for purpose over the next 10 to 20 years. Regulation is required to incentivise stakeholders to craft and provide their cloud services without unduly compromising the privacy rights of individuals whose personal data they hold and process.

Regulation in the national and regional patchwork form as found today, presents a muddy environment in which individuals, businesses and CSPs are trying to find their way. This confusion has at least delayed the take up of cloud services. Governments are carefully evaluating the use of cloud services – which could bring huge benefits in both cost savings and exciting developments in services such as e-health, e-learning etc. The Commission's initiative on government procurement - bringing regulators and stakeholders together - is a welcome step in advancing the contracting process and potential use of cloud services by Governments. The initiative may provide sufficient clarity and best practice to be adopted by the private sector.

The costs of compliance with diverse laws in multiple jurisdictions, however, seem unacceptably high. One report suggested that businesses comply with the most stringent EU Member State requirements and then could be relatively sure of complying with most other data protection laws.[61]

A balance also needs to be crafted between regulation for privacy and regulation for security. Moving personal information across borders will expose that data to possible interception by foreign law enforcement.

In many cases law enforcement requests may conflict with data protection laws, including in those of countries where the data originated or where it is stored. Such requests may also violate commitments made by companies to customers or employees, leading to potential legal liability and a loss of reputation. Political tensions may also arise between countries when authorities in one country request companies to disclose personal data stored in another one. The attendant legal and political issues, not to mention uncertainty, may discourage companies from investing in certain countries and may limit the free movement of data.[62]

These conflicts are particularly acute in the cloud – with increased cross border data flows and the expansion of illegal activity on the Internet.

Harmonisation of international data protection rules and co-operation between governments where rules are inconsistent would be the best solution.[63] The International Chamber of Commerce (***ICC***) has made a number of recommendations to governments and law enforcement authorities, including (i) taking into account the possibility that law enforcement requests may violate foreign data protection laws; (ii) making formal and specific written requests including the legal basis for the request; (iii) making cross-border requests for data stored abroad through mutual legal assistance treaties; (iv) giving companies the opportunity to evaluate the legitimacy of the request; (v) avoiding the requirement for companies to enter into supposedly "voluntary" agreements to deliver information and under threat of penalties and (vi) allowing companies to limit potential liability, by anonymysing or shielding personal data of parties that are not being investigated.[64]

The current conflicts and confusion in privacy and data protection regulation are having a significant negative effect on global trade and the take up of cloud services. Though many of the regulations are severe and cumbersome, the enforcement of regulations has generally been *ad hoc*. There are obvious difficulties in identifying the occurrence of a breach and proving same.

2.14 **The Role and Importance of International Co-operation**

Cloud services, whether provided to individuals through social networking or webmail or to businesses of any size or governments, are by their nature global. Governance models must take account of the international nature of the cloud. Technology is moving quickly towards further international expansion. For example, Google had patented floating data centres. Might they sport an EU Member State flag?

There are a number of initiatives underway that are fostering international co-operation. In 2009, data protection authorities from 50 countries approved the "Madrid Resolution" on international privacy standards.[65]

The standards proposed were international minimums. The principles were put forward in an attempt to achieve the greatest international consensus, with a view to influencing the development of legal and institutional structures for those countries yet to adopt a framework for data protection.

In particular, the resolution defined a number of principles and rights to guarantee the effective protection of privacy at an international level as well as ease the international flow of personal data essential in a cloud environment. The basic principles of lawfulness and fairness, purpose specification, proportionality, data quality, transparency and accountability were widely accepted. It is interesting to note that transborder data flow is not included in "basic principles", but set out in a different section. The proposal also expressed the need for supervisory authorities and co-operation and co-ordination of activities by different states, better compliance with applicable laws, limited international transfers of data – subject to consistent legal protections based upon relevant laws or contractual protections and offering awareness, education and training programmes.

A number of large companies welcomed the initiative and signed a declaration in support.[66]

The upcoming ITU World Conference on International Telecommunications in December 2012 will be a major treaty writing conference. The 1988 International Telecommunications Regulations (***ITRs***) will be reviewed and renegotiated. Some Member States would like to see a substantial increase in the scope of the Treaty. This could potentially include Internet and privacy issues.

In January 2012, Vice President Neelie Kroes proposed that public authorities and industry, cloud buyers and suppliers come together in a "European Cloud Partnership". The Cloud Partnership will propose common requirements for cloud procurement by looking at standards, security and ensuring competition rather than lock-in. At the second phase, the Partnership is to deliver "proof of concept resolutions" for the common requirements. In the third phase, reference implementations will be built. The Commission is investing €10million in the project. The project is directed at government Cloud procurement, but is expected to influence procurements by the private sector.[67]

As yet there is no universally binding privacy legislation covering all countries of the world. In Europe, as described in section 2.2 above, Member States have implemented the European Directive differently causing difficulty in compliance and significant administrative costs for operators. Though current proposals are intended to harmonise the approach, they do not go far enough to take account of the global nature of cloud services. The current US approach is also fragmented, with a variety of state and federal laws, mixed with self-regulation.

The ITU-T Technology Watch Report on Privacy in cloud computing[68] provides additional examples of privacy principles in other organisations and countries.[69] These include a description of the Odense Municipality case, a review of the EU Data Protection Directive; a definition of privacy by design and the use of PETs to implement privacy by design. Privacy by design generally refers to technical design of the processing system to integrate and implement effective privacy protection.

The Report identifies the three main privacy challenges in cloud computing as (i) complexity of risk assessment in a cloud environment, (ii) the emergence of new business models and their implications for consumer privacy and (iii) achieving regulatory compliance.

The Report also outlines the current work of the ITU-T SG 17 on cloud computing security. The ITU also set up a focus group on cloud computing security in 2010.

These steps are welcome as the lack of consistent and coherent domestic and international policies and regulation is having an unjustified chilling effect on the uptake of global cloud services. Policy makers, regulators and commercial stakeholders need to work together to develop standards, working practices, new technologies and educational tools which are "fit for purpose" in the changing global environment.

Section 5 outlines the options for future co-ordination and co-operation in the development of frameworks for the protection of privacy and data protection in a cloud world.

3 *ENFORCEMENT OF DATA PROTECTION AND PRIVACY LAWS IN THE CLOUD*

3.1 The Regulator's Role and Ability to Enforce Data Protection and Privacy laws in the Cloud

With the international nature of cloud services and the inconsistent international regulatory environment, the national regulators (both the ICT regulator and the specialized privacy/data protection agency), have a significant challenge. First – how are breaches of relevant laws to be discovered in the cloud? If discovered, will the national regulator have jurisdiction to effectively address the breach if it occurs outside its borders?

There are numerous laws following the European Directive restriction on transborder data flows. It is difficult, if not impossible, to know how well such a regulation can be enforced. There are still relatively few enforcement actions. "The fact that some of the largest economies in the world (such as China and Japan) have not been the subject of a formal EU adequacy decision means that there must be substantial non—compliance at least with regards to data flows from the EU to those countries."[70]

There is also a balance to be achieved between protection of personal data and national security risk that may give government a legitimate interest in having access to personal data. Particular concern has been expressed across Europe about the breadth of the US Patriot Act. To monitor the extent and potential threat of foreign governments having access to personal data, Google maintains a register of the requests it receives from governments. The most requests are received from the US, followed by India and Brazil.[71]

It is critical that individuals as well as businesses and other private and public bodies know which data protection rules regulate the protection and processing of data.

The Working Party adopted an opinion on applicable law (WP179) "to improve legal certainty, clarify Member States' responsibility … and ultimately provide for the same degree of protection of EU data subjects, regardless of the geographic location of the data controller."[72]

Data controllers, regardless of location, may be subject to data protection laws of one or more Member States depending on the activities undertaken.

It may be challenging for businesses to assess which laws it should comply with. If a business operates globally, a clear understanding of the European Directive will be important and the adoption of BCRs may be appropriate. The European Directive continues to be influential in the development of data protection laws globally, including in Hong Kong (China), Dubai and developing countries – such as South Africa.

The draft European Regulation includes ambitious territorial scope, both within the EU (with regulators permitted to levy cross-border fines) as well as provisions requiring compliance by non-EU based organisations. It also includes mandatory notification of data breaches within 24 hours. It is unclear how these provisions will be enforced in practice.

These practical challenges raise once again the need for international co-operation and harmonization if cloud computing is to have the opportunity to grow as promised and to provide a significant catalyst to global growth.

3.2 Recent Examples of Enforcement Directives

3.2.1 UK[73]

- **ACS:Law**

  In May 2011, the ICO concluded its investigation into the law firm ACS:Law which had been involved in one of the UK's most high profile data breaches, involving some 6,000 data subjects.

  ACS:Law had acted on behalf of copyright holders within the music and adult film industries in pursuing illegal filesharers. In the process of doing so, the firm became the target of Internet activists and, due to inadequate I.T. systems, the details of the 6000 individuals and the names of the works they were accused of sharing were published on the Internet.

  The leaked information was a gross invasion of the individual's privacy and the ICO's investigation found that no one at the data controller had any IT qualifications, the IT system in use was not intended for business use and cost £5.99 a month, and there were no proper firewalls or access controls in place.

The ICO concluded that in the ordinary course of sanctioning, a monetary penalty of £200,000 would have been imposed. However, because ACS:Law was the trading name for a sole practitioner of limited means, the fine was reduced to £1,000. This reduction attracted strong criticism and even the theoretical level of fine was seen as particularly low in light of such a serious breach.

- **Torquay Care Trust**

  On the 6 August 2012 a health trust in Torquay was issued an ICO penalty of £175,000 after sensitive details of 1,373 employees were accidentally published on the Trust's website and remained there for 19 weeks. The ICO found that the Trust had no guidance for staff on what information should or should not be published online and had inadequate checks in place to identify potential problems.

- **Google Inc.**

  In November 2010, Google Inc. was required by the ICO to sign and publish an undertaking following the collection of payload data via its Street View mapping service.

  In collecting data for the service via publically available wi-fi signals, Google had also captured data from private individuals such as emails, URLs and passwords without their consent.

  The ICO chose not to impose a sanction and Google undertook to implement improved training measures on security awareness and data protection issues for its employees. Furthermore, any future project that involves significant personal data processing must have a compliance document from the outset and any data collected in breach would also have to be deleted.

  This name and shame approach was relatively soft in comparison to the sanctions imposed on Google for the same transgression in France, Spain and Italy.

3.2.2 **France**

- **Google Inc.**

  On 17 March 2011, CNIL issued a fine of €100,000 to Google following the same data collection issues encountered in the United Kingdom. In this instance the fine was for Google's failure to respond in a timely manner to CNIL's formal request in May 2010 that the company rectify its procedures. Google had undertaken to stop collecting the data and delete any data that it had collected by mistake. However, CNIL found that Google had failed to stop making use of the data and, although it had stopped collecting through its "Google cars", it had in fact continued to collect data through users' mobile phones.

  CNIL was invited by the Working Party to take the lead in the analysis of the new privacy policy that Google had undertaken to implement. In May 2012 CNIL announced that Google's answers to its questions were incomplete or approximate, that it was impossible to know Google's processing of personal data and that the obligation to inform data subjects was being ignored.[74]

3.2.3 **Germany**

Significant fines have been imposed by the German authorities in recent years. In 2009, **Deutche Bahn** was fined €1.1million for several breaches including illegal screening of employees' personal data.[75]

- **Google Inc.**

  Germany took a similarly soft approach to the UK in its treatment of Google and German residents were granted the opportunity to "opt-out" of the Street View system.[76]

3.2.4 **USA**

The FTC is the primary enforcer of national privacy laws alongside other national agencies that enforce privacy laws within their respective sector. The FTC Act provides for penalties of up to $16,000 for each offence along with imprisonment of up to ten years. The state laws of California are enforced by the California Attorney General and district attorneys.

Settlements are common in the United States and offenders may be issued onerous reporting, audit and monitoring requirements alongside monetary fines. Google may have escaped sanction from the FTC for Streetview but has recently received a record fine of $22.5 million by way of settlement for the placing of cookies on Internet browsers and misleading users who were led to believe they had opted out[77].

3.2.5 Canada

There are a wide range of enforcement methods contained within the various Canadian privacy statutes. At federal level, the Federal Privacy Commissioner has fairly limited investigatory powers and can make recommendations following violations of the PIPEDA. Provincial privacy commissioners tend to have increased powers including the ability issue fines and make binding orders.

The sanctioning of Google in May 2011 provides a good example of the limited powers of the Federal Privacy Commissioner. In comparison to sanctions for the same offences elsewhere in the world, Google was issued with recommendations including improved training of staff, adoption of a privacy governance model and deletion of the illegally collected data.[78]

3.3 The Value and Effectiveness of Self Regulation, Regulation of Commercial Relationships and Technology Solutions

It is critical to keep in mind the core value of personal privacy and data that relevant laws are trying to address and protect. In the current international data culture, the solution must be both practical and effective. The combination of cloud providers (i) establishing self-regulatory measures that address the data customer's concerns, (ii) crafting best practice contractual provisions; and (iii) creating and using security technologies to address security concerns; may well provide the best practical way forward to achieve the fundamental goal.

3.3.1 Progress in Self Regulation

There are three key reasons to increasingly rely on self-regulation with respect to on-line privacy and data protection:

- Self-regulation by CSPs who are most familiar with the technical aspects of cloud computing and the practicality of the delivery of cloud services facilitates global best practices. By integrating national and international privacy frameworks into a unified programme or code, CSPs and their customers will be in a better position to satisfy regulatory requirements and implement practical best business practices globally.
- Self-regulation evolves with technology. On-line privacy frameworks must be dynamic, like the technology they regulate. Conventional regulation is typically years behind, as discussed above.
- Self-regulation can provide strong incentives for compliance. They provide safe harbors to foster growth and promotion of best practices, which is in turn critical to the success of self-regulation.

A variety of voluntary and private sector mechanisms have been put in place in an attempt to comply with relevant regulations and provide the party accountable for the data with necessary assurances.

The US-EU Safe Harbor framework is a hybrid example of self-regulation. Companies can choose whether to adopt the framework. By self-certifying their compliance with the seven Safe Harbor principles,[79] US companies can assure EU organisations that the company provides "adequate" privacy protection for purposes of compliance. A company who self-certifies is then legally bound to comply. It is a hybrid regime because the FTC has the power of enforcement in the event of a breach of the certification. Perhaps this hybrid model of voluntary adoption of self regulatory codes coupled with enforceability by the appropriate national or indeed international regulator could be explored and considered for adoption as best practice.

Other codes of practice and standards have been implemented in Canada and Singapore. The International Organization for Standardization (***ISO***) is also working on privacy standards.

Cloud service providers have also taken measures to establish codes of practice to address the concerns of the data controller or accountable party. The Cloud Industry Forum (***CIF***) launched its Code of Practice in November of 2010. Following an extensive period of public consultation the CIF Code of Practice is intended to create a credible and certifiable code of practice that provides transparency of cloud services to allow customers to have clarity and confidence in the services, security and process used by the cloud provider.[80] It does not, however, have any legally binding effect.

The Cloud Security Alliance (CSA) is also promoting a code of best practice for providing security assurance in cloud computing and Cloud Audit is developing an application to automate the audit of cloud services[81].

In 2011, the American Institute of Certified Public Accountants (***AICPA***) established a Service Organization Controls (***SOC***) reporting framework to be applied to CSPs. One of the areas covered is privacy. The audit will examine whether personal information is collected, used, retained, disclosed and destroyed in conformity with the commitments of the company's privacy notice and relevant accounting standards (ex Generally Accepted Accounting Principals (GAAP)).[82]

CSPs should be encouraged by policy makers and regulators to adopt clear accepted industry standards and best practice on technical, security and other critical issues relating to the services provided. Trustworthy and consistently applied certifications will go some way to address confusion.

The positive effect of the implementation of these codes and standard can be seen in the take-up by cloud providers. Autonomy (now an HP company) indicates on the first page of its Cloud Solutions marketing page that it "adheres to global certification standards, including PCI DSS, US DOD5015.02, UK TNA2002 and Australia's VERS." It also indicates that "its people, processes and technologies operate in compliance with Statement of Accounting Standard number 70 Type II (SAS70) and undergo annual SAS70 audits."[83]

The challenge for CSPs is to be able to demonstrate to business customers that their services will fulfil compliance standards the customer requires to be confident in trusting the service provider and being confident that the customer is complying with its responsibility as a data controller or accountable party.

In implementing such measures, the CSP will have to analyse the cost versus the benefits. The additional requirements could increase the cost of the cloud solution to the point that it is no longer a good business decision for either party.

In addition to self regulation and certification, the customer should, to the extent possible, look to establish clear contractual terms with the CSP. Of course, the customers' ability to negotiate the terms will depend on the customers' position and bargaining power.

3.3.2 Contractual Solutions

The contract entered into between CSPs and their customers should, to the extent possible, present a clear set of rights and relative responsibilities of the parties.

The European Directive has used private contracts as a critical tool in allowing transborder data flows. International business can adopt Binding Corporate Rules and standard approved clauses may be included in contacts between the CSP and data controller to assure compliance with relevant data protection laws. This is an interesting and effective regulatory tool.

The most challenging area for CSPs and customers is when SaaS is chosen as the cloud service. Typically SaaS vendors will have many contracts globally. They are typically for off the shelf solutions and used by individuals or small and medium sized business. The terms are typically published on the CSP's website, are very supplier centric and may be accepted electronically. They exclude all but the most limited warranties and any liability for data loss, corruption or service failure. Cloud customers who are data controllers must try to choose CSPs that will guarantee or assure their compliance with applicable law through due diligence. The introduction of self regulation and certification processes will assist in this process.

The best customer solution is to seek negotiated terms which would include service levels, service credits, data back up to preserve data from loss and agreement by the CSP to take data out of its system. Of course, this increases the cost of the service and may not be practical for smaller businesses.

The Working Party has recently provided recommendations for businesses and government administration wishing to use cloud computing services.[84] The Working Party recommends the data controller conduct comprehensive due diligence and risk analysis of the proposed service. Due diligence

with respect to cross-border transfers must be particularly robust. The process will require knowledge and action by the purchaser as well as co-operation from the CSP.

The opinion also provides guidance on the contractual arrangements that govern the commercial relationship between the customer and CSP with respect to privacy and security.

The contract shall provide for:

- appropriate transparency regarding data handling processes;
- isolation of personal data so that the personal data may be amended or deleted by the data subject;
- appropriate security measures to ensure availability, integrity and confidentiality.

Specific contractual safe guards have also been proposed, including sufficient guarantees of technical security and organisational measures, detail the customers instructions including time frame, subject and SLAs, limitation of people who have access to the data, when disclosure to third parties is permitted and on what terms, obligations for the CSP to co-operate with its client regarding monitoring and facilitating the rights of data subjects, guarantee of lawfulness of cross border transfers, definition of the logging and auditing of the data processing and identifying and delineating appropriate technical and organisational measures to manage the risk of lack of control.

In addition to these specific requirements, the contract must include the controller's instructions to the processor, obligations with respect to security measures, specifications of the conditions for destroying or returning data and obligation to provide a list of locations where data may be processed, as well as measures facilitating accountability, such as third-party audit and certification.

Helpfully, the Working Party endorses third-party certification as an acceptable means of proving compliance. This will obviously help to streamline and cut the cost of the customer's due diligence.

In addition to self-regulation and certification and carefully considered contractual terms, a third and critical form of effective protection of personal data can be found in the growth and development of privacy enhancing technologies (***PETs***).

3.3.3 Technology Solutions

The number of PETs have been increasing. The use of these technologies will potentially provide the data controller or accountable person with practical and effective means of being confident of its compliance. Examples of PETs include a variety of encryption models, technologies hiding the correlation between input and output data, private authentication protocols and anonymisation techniques to name a few[85].

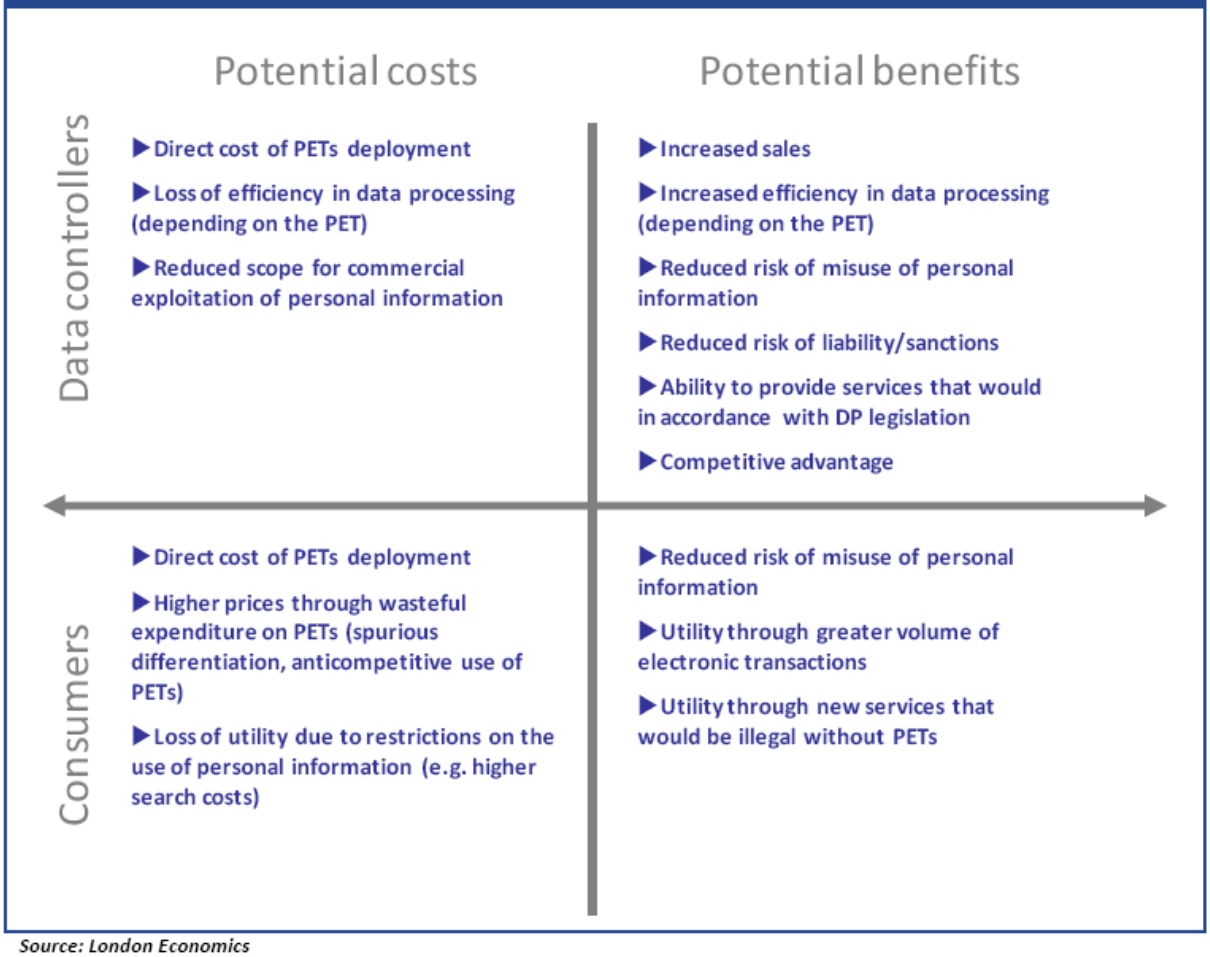
Companies like TRUSTe are rolling out new technologies and platforms that offer privacy solutions. For example, it has developed an EU Cookie Audit, which detects and reports on all first and third party tracking mechanisms present on a website.

New businesses are springing up as "cloud access security brokers". Perspec Sys, for example, provides a gateway allowing the customer to select its data protection policies, such as encryption or tokenization in a single platform. The platform is vendor-agnostic and supports multiple clouds. Consequently, concerns about vendor lock-in are addressed technically.[86]

The challenge, of course, is to increase awareness and take up of PETs. London Economics has indicated that "Market imperfections, which can include asymmetric information, externalities, lack of information sharing about privacy risks and co-ordination failures, mean that the individually rational decisions of data controllers do not necessarily lead to the optimal level of PETs deployment."[87] This essentially indicates current market failure. There is clearly a role for policy makers and regulators to overcome these barriers.

London Economics has analysed the costs and benefits of PETs deployment as follows:

Figure 1: Potential costs and benefits of PETs deployment



Source: London Economics

88

4 ARE THE ISSUES DIFFERENT IN THE DEVELOPED V. DEVELOPING WORLD?

4.1 The Infrastructure Challenge

While developed countries debate the best practice privacy and data protection regulations to meet in the cloud, most developing countries are struggling – to differing degrees – with more basic obstacles to the development of cloud services. The three key market segments of mobile, Internet and broadband are critical to delivering cloud computing. Obstacles in many developing countries (and particularly in Africa) centre on lack of infrastructure and government policy. In addition, the combination of power shortages and inefficiencies generally stall development. Mobile penetration is significant, but broadband penetration tends to be low.

4.2 The Opportunity

The ITU, the World Bank, the EBRD and other development agencies are keenly interested in ICT for Development. Cloud computing is potentially at the centre of this opportunity. Critical assistance can be provided in e-education, e-health, e-commerce, e-governance and e-environment and telecommunicating. The cloud may also provide an opportunity for business to by-pass traditional trade bottlenecks, corruption and inefficient bureaucracy. To deliver these benefits in the developing world, pieces of equipment and software must come down in price and governments must have access to financial resources and education to run their IT systems.[89]

Laverty uses the development of mobile applications as a current example of the enormous opportunity to create links between the developed and developing world that were "unimaginable before cloud computing". "A developer in Rwanda can use web based applications to create and test an app for the iPhone and then publish their completed work to Apples' App Store where any iPhone user in the world can purchase the app and download it".

4.3 Lack of Privacy Protection

Privacy International has expressed concern about the lack of adequate legal and institutional frameworks and safeguards. Without them, both corporations and governments can collect and share personal data in the name of development.

"In many developing countries the framework for the protection of personal information are either at a nascent stage, are not implemented or enforced, or simply do not exist at all".[90] Concern was expressed about the collection and storage of biometric information and the use of ID cards. The use of such information could range from identity theft, social sorting and criminal investigations.

It is critical at this stage in the development and rollout of cloud services that as part of the international ICT development agenda, practical and effective privacy regulation be an integral part of the process of investment and enhancement of services that are delivered in developing countries.

A balance must be struck between advancing development through the use of ICT, particularly cloud services, and the need for education regarding the risks and benefits of the services as well as regulation to preserve this fundamental human right of privacy.

As the cloud is evolving in developed nations – developing nations must not be left behind. The implementation of appropriate policies that both encourage investment, while protecting personal rights will be critical.

If a coherent and consistent international approach can be established to privacy in the cloud, the appropriate international organisation would be in a position to propose model laws which would move the process of take up a major step forward.

Government, policy makers and regulators need to look to the future and particularly the fundamental role and importance of international co-operation. They need to focus on the development of best practice privacy and data protection policy that preserves an individuals' rights while avoiding confusion, lack of clarity and a "heavy hand". A balance must be struck between all stakeholders that does not have a chilling effect on innovation or freedom of the Internet and cloud computing.

5 *THE FUTURE: HOW CAN DATA PROTECTION AND PRIVACY REGULATION KEEP PACE WITH TECHNOLOGY AND BE BOTH EFFICIENT AND EFFECTIVE IN THE INTERNATIONAL CLOUD CULTURE*

5.1 Best Practice Policy in the Development of Data Protection and Privacy Laws in the Cloud Eco-system

The challenge for policy makers is to balance the commercial need and individual desire for free flow of information with informed knowledge and effective control by individuals of their personal information. Clear and consistent policies need to be developed based upon current and prospective technologies. The opportunities for growth and development should not be hindered by unnecessary regulatory barriers, administrative burdens or choice of law or applicable jurisdiction issues.

The first and most important hurdle is to raise the opportunities and challenges presented by international transfers of data to the top of the agenda of national, regional and international policy makers. As the "new oil", "ministers and government officials should grant international data flows the same attention as they do international flows of capital and international trade. . . These topics are in many ways inseparable, since the ability to transfer personal data internationally is a vital component of the globalized economy."[91]

CSPs and businesses should be actively consulted and involved in the development of policies relevant to the provision of cloud services. Businesses should consider implementing research and effective cloud protection plans. Investors should consider where best to locate their cloud business. If we compare the cloud to a shared office building – what terms and conditions should be implemented? With CSPs delivering the digital economy, governments and regulators should consider offering cloud friendly investment policies while ensuring an effective framework for privacy and protection of personal, business and government data is in place.

In an effort to demystify privacy and data protection issues in the cloud, studies have been commissioned and information is being gathered on various subjects including, for example, best practice government procurement[92] and PETs[93] and the European Parliament's 2011 study "Does it help or hinder? Promotion of Innovation on the Internet and Citizens Right to Privacy."

In addition, individual attitudes must be explored and taken into account. After all, whose personal data are we trying to protect? What responsibility should individuals take for disclosure of their personal information. Individual attitudes are typically measured and identified by way of opinion polls. The 2011 Special Eurobarometer report contained interesting perspectives on individual attitudes to privacy. 74% of survey respondents considered on-line disclosure of information an increasing part of daily life; a majority expressed concerns over recording of their behaviour by way of mobile phones, payment cards and mobile Internet; and 58% did not believe there was any alternative to disclosure of personal information to obtain the benefit of desired products and services.[94]

Consumer groups tend to take a more active role in trying to protect the consumer's personal information than individual consumers do.[95] The key to analysing the real value of personal information to the consumer is obviously education and the advancement of "Cloud Literacy". A fundamental role for national ICT and data protection regulators is the facilitation of Cloud Literacy.

5.2 Recommendations for Future Data Protection and Privacy Laws

The four key areas of data protection laws that apply to cloud services are:

- Who is responsible for the protection of personal data in its possession?
- What restrictions, if any, should be placed upon the transborder flow of data?
- What security obligations should be imposed upon the party responsible for the relevant personal data?
- What law should apply in the cloud?

5.2.1 Who is responsible?

As discussed above, the current European Directive imposes primary responsibility for the protection of personal data on the "data controller".[96]

The definition applies to and imposes primary responsibility on the cloud business customer. In the case of cloud services provided to individuals, Facebook, or another provider, of social networking services or webmail would be the data controller. It does, however, also envisage the possibility of more than one "controller". When the cloud customer chooses a CSP, it is appointing that entity to process personal data on its behalf. The controller or customer has significant responsibilities to ensure that the CSP provides "sufficient guarantees" with respect to technical and organisational security measures and takes steps to ensure the CSP complies with those measures. In addition, the arrangements must be evidenced by a written contract requiring the CSP to act only on the customers' instructions and comply with obligations "equivalent" to certain security measures imposed on the customer. Processors are not typically directly subject to the European Directive.

The position regarding sub-processors is complex. If sub-processors are used they must also be obliged to act in accordance with the direction of the controller. Realistically, the efficient provision of cloud services could involve a number of sub-processors. Some member states have added the burden of requiring the customer to enter into direct contracts with each sub-processor.

With the ever increasing complexity of data processing and the involvement of multiple parties in the delivery of cloud services, the Working Party has issued guidance on the definition.[97]

Rather than clarifying the position, the Working Party further confuses stakeholders by indicating that factual functional control matters most in determining controller status. Though contractual provisions will be relevant, they will not be determinative.

These distinctions are unclear and out dated. They are unlikely to be enforceable in accordance with their terms in a cloud environment. CSPs and their customers are in the unhappy position of guessing what law might be applied and how it will be applied in a particular situation.

A different approach is taken by APEC, Canada and a number of other jurisdictions. The principle of "accountability" is increasingly being adopted internationally and advocated in Europe.[98] The accountability approach puts end-to-end responsibility on the controller of the relevant personal data. The accountability model appears to be the most effective means of clearly allocating responsibility in a cloud environment. For example, PIPEDA places no prohibition on transborder data transfers. The accountable party remains responsible for the personal data wherever it is held. This reflects a pragmatic, technically savvy and best practice approach to effectively protecting personal data.

5.2.2 Transborder Data Flows[99]

There are two schools of thought and attendant regulation relating to the international transfer of data. Harmonising and clarifying these approaches will be essential to promoting the growth and proliferation of cloud services – with their attendant economic benefits.

The European approach is based on geography. It is intended to protect against risks by the country or location to which data is transferred. The critical question is whether the importing country has "adequate" legal protections of personal data. In addition to the EU, Argentina, Morocco and Russia have adopted this approach. South Africa and other countries currently preparing data protection legislation may also adopt the geographically-based approach.

The geographic-based approach may also be questionable going forward under the General Agreement on Trade in Services (***GATS***)[100]. Data protection legislation is exempt from scrutiny under the GATS, but only so long as it is not a disguised restriction on trade.[101]

The Canadian PIPEDA and the APEC Privacy Framework imposes the obligation on the data exporting organisation to ensure the continued protection of personal data for which it is accountable. The geographic location is irrelevant. Though there is some overlap in the two legal approaches,[102] the best approach to provide clarity would be to try to internationally harmonise the two diverse principles.

It is now questionable whether, in light of the growing international digital environment and the prospective economic benefit cloud services present, whether the geographic restrictions imposed by current laws present not very well disguised restriction on international trade. Consider the fact that CSPs are now creating separate geographic clouds to accommodate EU style laws. This is particularly of concern in light of the other alternative,

i.e. the accountability principle. This principle presents a modern and clear approach to who is responsible and to what extent the restriction of international data flows are important to the effective protection of privacy.

The European Commission now has the opportunity to amend its geographically-based approach in its proposed reform of European Data Protection legislation and adopt the accountability model – reflecting international best practice. The reforms are intended to resolve disharmony between Member States and make compliance more straight forward.

The international digital eco-system calls for new ways of effectively protecting personal data. The Commission could seize this moment to lead the way toward an efficient internationally harmonised approach by adopting the accountability principle in its approach to who is responsible for personal data and where that data is held.

5.2.3 Security Obligations

Data security is one of the technical and organisational measures put in place to protect personal data. Security obligations on the "controller", "processor" and "accountable party" are common and defensible across international data protection regulations.

The accountability principle puts the obligation squarely on that party to take steps to assure the practical security of personal data that it will have processed by a third party.

Based upon the current uncertain technical environment, the safest option for the accountable party is to refrain from putting personal data in its control into the cloud environment. This is not, however, a position that will promote global economic connectivity and growth.

A number of opportunities are being created by new businesses offering security, encryption, auditing and other privacy enhancing technical solutions to provide comfort to the accountable party. CSPs have a role to play in putting in place reasonable commercial terms with customers and advancing self-regulation.

A significant tension may occur between the accountable party's obligations and potential interests by some foreign governments in personal data held in their country. International policy makers and bilateral arrangements between governments should play a role in providing clarity and consistency. Though with diverse interest across the globe – harmonisation may be out of reach for the moment.

5.2.4 Applicable Law

The process of determining which country's law applies to a breach of privacy is very complicated. It is challenging within the EU itself. Again, the EU is used as an example here because its data protection structure has been in place for some time and is forming the basis for legislation in many other parts of the world.

The current position within the EU has left room for considerable uncertainty in relation to the applicable law, not just in relation to data protection, but cloud computing in general. The European Directive envisaged data processing being limited to a small number of fixed locations under the control of one organisation, but the evolution of cloud computing has left this framework outdated and redundant.

That reform in this area would be welcome, if not necessary, is clear from the responses to the recent European Consultation.[103] It is essential that a clear framework is implemented to allow both providers and customers to gain a degree of certainty and it remains to be seen how the European Commission proposals for data protection will address these concerns.

There is also a need to address the relationship between the Rome I and Rome II conventions (that govern the law applicable to contract and tort in the EU) and cloud computing. The test for the applicable law, absent choice, is not suited to the development in modern technology, particularly in relation to cloud computing. Rome II, for example, provides that notwithstanding where the events giving rise to the damage occurred, the applicable law is the law of the country in which the damage occurs. Where cloud computing is concerned, this could reasonably be any number of jurisdictions. The potential for fragmented litigation is enormous. A wholesale failure by a provider could, as things stand, result in years of unpredictable proceedings.

The matter is further complicated where multiple jurisdictions are involved. Conflicts of laws is an extremely complex topic, again one that is not suited to the evolving nature of cloud computing. As matters stand, it would

be almost impossible for a provider with customers scattered around the globe to manage its legal exposure with any real certainty. However, as the use of cloud computing continues to grow, so will the political will to implement an international framework to govern its provision and use with clarity and certainty.

5.3 Recommendations to Policy Makers and Regulators

Having established the existing and potential value of cloud services, considered current data protection and privacy regulations, reviewed the challenges to enforcement of these regulations in the cloud, differences in issues between the developed and developing economies, the need for international co-operation and set out some recommendations for future international harmonisation of laws. What are the recommendations to policy makers and regulators to address the critical challenges raised by the cloud eco-system? This agenda must include clarity with respect to applicable law.

- ***Facilitate Knowledge***: Regulators have the opportunity to advance and facilitate "Cloud Literacy". This will assist consumers and citizens to make informed choices about what personal information they put in the Cloud, advance their understanding of who to complain to if their information is misused and enhance their understanding of the value to businesses of their personal data and how it might be used.
- ***Develop Expertise***: Policy makers and regulators must ensure they take account of current technical and social developments in the Cloud, its usage and potential. They must also keep current by taking soundings from all stakeholders to be in a position to develop, evolve and enforce relevant laws.
- ***Adopt Fit for Purpose Laws***: We are at a cross-road where international and national policy makers must work together to develop efficient, effective, proportionate and enforceable laws to protect an individual's reasonable expectation of privacy. Responsibility should also be devolved to stakeholders developing self regulation.
- ***Clearly Allocate Responsibility***: Regulations should ensure that responsibility for compliance is effectively and efficiently allocated to the party who is in the best position to ensure compliance. Responsibility and enforcement powers should be clearly allocated between national and international regulators as well as between domestic ITC and data protection regulators.
- ***Understand and Use Technology***: Cloud technology has evolved extraordinarily quickly. Policy makers and regulators now have the opportunity to take account of the development of new PeTs, and other practical means of protecting individual privacy and enhancing security systems.
- ***Review Existing Laws***: Policy makers internationally need to review existing laws to facilitate the national and international use of cloud services. The development of common standards and interoperability requirements will facilitate information flows with appropriate security and privacy protections. The elimination of restrictions on the transborder flow of data is critical to the growth of the cloud eco-system.
- ***Raise Awareness and Promote Uptake by the Public Sector***: Cloud services and the opportunities and savings they make available to governments around the world should be actively pursued and promoted. Particularly in the developing world. Bringing awareness and opportunities will lift the economic opportunities and provide great value to citizens, consumers and businesses.
- ***Encourage Clarity and Transparency in Cloud Contracting***: Confusion caused by the inconsistent patchwork of current laws may be assisted by clear contractual arrangements. Governments and stakeholders should establish a continuing dialogue to define best practice contractual terms.
- ***Enforcement***: Because some current legislation restricts behaviour that is virtually impossible to monitor in the cloud, regulators need to establish a means of identifying breaches to ensure they are able to respond effectively. This may be effected through self regulatory mechanisms, CSPs notifying the appropriate regulator of breaches of security and ideally changes to those aspects of data protection legislation which are impossible to monitor and hence unenforceable in practice.

6 CONCLUSION

> "***It was a thing hardly to be expected that in a popular revolution the minds of men should stop at that happy mean which marks the salutary boundary between power and privilege, and combines the energy of government with the security of private rights. A failure in this delicate and important point is the great source of the inconveniences we experience, and if we are not cautious to avoid a repetition of the error in our future attempts to rectify and ameliorate our system we may travel from one chimerical project to another; we may try change after change; but we shall never be likely to make any material change for the better."***[104]

Hamilton's concerns in the 18th Century upon forming the US Federal Constitution, could equally apply today. Now is the time to consider the present governance approach as a group of countries (rather than states) who face a global rather than federal future.

We need now to combine the energy of governments with the security of private rights to take a clear, consistent, pragmatic and "internationalist" approach to a fundamentally global digital eco-system.

Domestic and international policy makers need to come together to address the issues and opportunities presented by cloud services.

A patchwork of inconsistent and largely unenforceable national and regional regulations will neither harness the opportunities presented by cloud services or secure an individuals' private rights and information. An internationally harmonised approach to the practical protection of privacy and personal data is the best way forward. We as citizens, consumers, businesses, policy makers and governments need to act together – perhaps under a new banner to move the effective protection of privacy in a global digital eco-system to the top of the international agenda.

Dedication: For my daughter Genevieve who is a digital native.

Acknowledgements:

Thanks to Charles Russell LLP for its continuing support; in particular to Oliver Price and Louise Tomlinson, new data protection experts; to Vanessa Barnett, a seasoned data protection expert; to Tom Briggs for Middle Eastern Expertise; to Zani Polson, Phillis Thompson and Alison Gaffney;

Special thanks to Dr Mike Short CBE, Peter Ingram and Campbell Cowie for their insightful comments.

References

- Association of Corporate Counsel - Article 29 Working Party issues opinion on cloud computing - McDermott Will & Emery - 8 August 2012
- Autonomy – Cloud Solutions – Autonomy Systems Limited
- Autonomy – How to Measure the ROI of Cloud Data Protection – Autonomy Systems Limited
- Autonomy – Social Media and the Shifting Information Compliance Landscape – Autonomy Systems Limited – [Undated]
- Autonomy – The Next Generation of Archiving – Autonomy Systems Limited – [Undated]
- Autonomy – Why Cloud and How to Choose a Cloud Vendor – Autonomy Systems Limited
- BroadGroup - Competing in the clouds: Emerging strategies for enterprise data centres – BroadGroup - May 2010
- BSA Global Cloud Computing Scorecard - A Blueprint for Economic Opportunity - BSA (Business Software Alliance)
- Business Computing World - Cloud Industry Forum - Launches Code of Practice - Andy Burton - 22 November 2010
- Business Computing World – Is The Cloud Safe? Kate Craig-Wood – 21 May 2012
- CabinetOffice.gov.uk – The Queen's Speech 2012 – Her Majesty's Most Gracious Speech to both Houses of Parliament – HRH Queen Elizabeth II – 9 May 2012
- Cio.co.uk – Perchance to dream… Are dreams just the brain's way of digesting the day's information into a manageable searchable package? Mike Lynch – 22 February 2011
- Cisco – Cisco Global Cloud Index: Forecast and Methodology, 2010-2015
- Cloud Industry Forum - Code of Practice for Cloud Service Providers
- Cloud Security - [Unknown] - Michael Davis - 16 August 2012
- Computer World UK: Cloud computing and EU data protection law: Part Two - On international transfers of personal data - W Kuan Hon and Christopher Millard - 23 April 2012
- Computer World UK: EU data protection regulation and cookie law - Are you ready? Thor Olavsrud - 24 May 2012
- Computer World UK: US Patriot Act - Can UK cloud customers use US cloud providers? W Kuan Hon - 29 May 2012
- Computer World UK: Who's responsible for personal data in cloud computing? W Kuan Hon - 23 May 2011
- Data Centre Management Security in the CLOUD - Nick Coleman - July/August 2012
- DataCentres.com: Cloud computing will cause 'horrible problems in the next five years' - DataCentres.com - 7 August 2012
- European Data Protection Commissioners (Spring Conference 2012) Resolution on the European data protection reform - 3-4 May 2012
- European Data Protection Supervisor – ACTA measures to enforce IP rights in the digital environment could threaten privacy and data protection if not properly implemented - [Unknown] – 25 January 2012
- European Data Protection Supervisor – EDPS general survey shows that EU institutions and bodies have different levels of data protection compliance - [Unknown] – 30 January 2012
- European Data Protection Supervisor – EDPS welcomes a "huge step forward for data protection in Europe", but regrets inadequate rules for the police and justice area - [Unknown] – 25 January 2012
- European Network and Information Security Agency – Benefits, risks and recommendation for information security - November 2009
- European Parliament - Directorate-General for Internal Policies, Policy Department Economic and Scientific Policy A - Does it help or hinder? Promotion of Innovation on the Internet and Citizens' Right to Privacy - 2011
- European Privacy Association - Ofcom Traffic Management and 'net neutrality' Consultation
- European Union - Article 29 Chairman of the Article 29 Working Party: Proposals a chance for better protection – Jacob Kohnstamm – 25 January 2012
- European Union - Article 29 Data Protection Working Party European Data Protection Authorities adopt opinion on cloud computing (WP 196) - 1 July 2012
- European Union - Article 29 Data Protection Working Party Opinion - The Future of Privacy – [Unknown] - 1 December 2009
- European Union - Article 29 Data Protection Working Party Opinion - 01/2010 on the concepts of "controller" and "processor" - 16 February 2010
- European Union - Article 29 Data Protection Working Party Opinion - 08/2010 on applicable law - [Unknown] - 16 December 2010

- European Union - Article 29 Data Protection Working Party Opinion - 11/2011 on the level of protection of personal data in New Zealand - 4 April 2011
- European Union - Article 29 Data Protection Working Party Opinion - 14/2011 on data protection issues related to the prevention of money laundering and terrorist financing – 13 June 2011
- European Union - Article 29 Data Protection Working Party Opinion - 04/2012 on Cookie Consent Exemption - [Unknown] - 7 June 2012
- European Union - Article 29 Data Protection Working Party Opinion - 05/2012 on Cloud Computing - 1 July 2012
- European Union – Reform of the data protection legal framework
- European Union – Setting up the European Cloud Partnership – Neelie Kroes – 26 January 2012
- European Union – The clear role of public authorities in cloud computing – Neelie Kroes – 25 March 2011
- Federal Ministry of Economics and Technology (Germany) - The Standardisation Environment for Cloud Computing Federal Ministry of Economics and Technology (Berlin) - February 2012
- G-Cloud c1 - Cloud Legal Project's Analysis - W Kuan Hon, Prof Christopher Millard and Prof Ian Walden - 23 April 2012
- Gigaom.com - Will using Dropbox put your CEO in jail? Janko Roettgers - 21 June 2012
- Giving bite to the EU-U.S. data privacy safe harbour - model solutions for effective enforcement - Daniel R. Leathers - 1 January 2009
- HM Government - G-Cloud Information Assurance Requirements and Guidance - [Unknown] - 10 May 2012
- IBM Global Business Services – IBM Institute for Business Value – The power of cloud, driving business model innovation – Saul Berman, Lynn Kesterson-Townes, Anthony Marshall and Rohini Srivathsa – February 2012
- Industry Recommendations to Vice President - Neelie Kroes on the Orientation of a European Cloud Computing Strategy - [Dr. Eugene Sweeney, Iambic Innovation Ltd] - November 2011
- Information Commissioner's Office (ICO) – Personal information online code of practice – July 2010
- Information Commissioner's Office (ICO) – Privacy by design
- Intel - Security in the Cloud - [Unknown]
- International Chamber of Commerce - The Digital Economy - Cross-border law enforcement access to company data – current issues under data protection and privacy law - International Chamber of Commerce - 7 February 2012
- International Conference of Data Protection and Privacy Commissioners – International Standards on the Protection of Personal Data and Privacy (The Madrid Resolution) – 5 November 2009
- International Data Privacy Law – Oxford Journals - Who is responsible for 'personal data' in cloud computing? – The cloud of unknowing, Part 2 - W Kuan Hon, Christopher Millard and Ian Walden - 6 December 2011
- ITU - ICT Regulation Toolkit – 2.4 What is the Role of Regulators? – 2012
- ITU - ICT Regulation Toolkit – Module 6. Legal and Institutional Framework – [Unknown] – [Undated]
- ITU-T Technology Watch Report - Privacy in Cloud Computing - Stephane Guilloteau and Venkatesen Mauree - March 2012
- Kuppinger Cole - 10 Rules for Securing the Cloud - Martin Kuppinger - 7 March 2011
- Kuppinger Cole - Data Protection and the Cloud - Martin Kuppinger - 14 February 2012
- Kuppinger Cole – Is cloud computing worth the hassle? 17 November 2011
- Kuppinger Cole – Top Trends 2012-2013 – Martin Kuppinger – April 2012
- Loeb & Loeb LLP - Data Protection - United States - Ieun Jolly - 1 March 2012
- London Economics – Study on the economic benefit of privacy-enhancing technologies (PETs)
- Mondaq – European Union: New Data Protection Regulation – How Will It Affect Your Business? John Menton, Rob Corbet, Caroline O'Gorman, Chris Bollard, Colin Rooney and Olivia Mullooly – 28 February 2012
- Mondaq – European Union: Reform Of Data Protection Laws - Colin Rooney – 23 April 2012
- Mondaq – Germany: German Data Protection Authorities Broaden Application Of German Data Protection Law To Foreign Social Networks And Attack The Use of Social Plugins And Fanpages – Fabian Niemann – 17 April 2012
- Mondaq – Germany: New EU Data Protection Regime Will Bring Significant Changes – Jurgen Hartung and Dr Marc Hilber, LL.M. – 2 March 2012
- Mondaq – Netherlands: Personal Data Protection Act Amended Jacqueline Van Essen – 20 February 2012
- Mondaq – United Kingdom: Draft Data Protection Regulation – Alan Meneghetti, Andrew Horrocks and Manoj Vaghela – 22 May 2012
- Mondaq – United States: Data Protection: Frequently Asked Questions – Goodwin Procter LLP – 13 January 2009

- Mondaq – United States: The USA Patriot Act and the Privacy of Data Stored in the Cloud – Alex C. Lakastos – 24 January 2012
- National Institute of Standards and Technology - Guidelines on Security and Privacy in Public Cloud Computing - Wayne Jansen and Timothy Grance - December 2011
- OECD – OECD Guidelines for the Security of Information Systems and Networks – Towards a culture of security
- OECD – OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data
- Oppenhoff & Partner Rechtsanwalte - Germany: Employees Off Into The Cloud? Dr Marc Hilber, LL.M. and Gilbert Wurth - 16 May 2012
- Oppenhoff & Partner Rechtsanwalte - Germany: German Data Protection Authority Forbids Certain Facebook Features - Jurgen Hartung - 29 August 2011
- Oxera (Agenda – Advancing economics in business) - Global-local: European telecoms regulation in the 2020s - Richard Feasey - July 2012
- PerspecSyS - Cloud Security Issues – [Undated]
- PerspecSyS - Gartner Highlights the Growing Importance of Cloud Security Brokers to Protect Sensitive Information in the Cloud - David Canellos - 7 August 2012
- PerspecSyS -Information and Privacy Commissioner Ontario, Canada – Ann Cavoukian
- PLC - Software as a service (SaaS) - Roger Bickerstaff, Barry Jennings of Bird & Bird - 13 March 2009
- PLC & Baker & Mackenzie LLP – Overview of EU data protection regime – Robbie Downing
- PLC & Bird & Bird – What is cloud computing - Roger Bickerstaff, Barry Jennings, Tessa Finlayson
- PLC IPIT & Communications – Article 29 Working Party adopts opinion on applicable law
- PLC IPIT & Communications – Cross-border transfers of personal data
- PLC IPIT & Communications – EU data protection regime proposals: analysis and noter-up
- PLC IPIT & Communications – European Commission proposes new data protection framework
- PLC IPIT & Communications - General counsel briefing: privacy and data protection
- PLC IPIT & Communications – ICO analysis of new EU data protection proposals
- PLC IPIT & Communications & Baker & McKenzie LLP – Data protection and the internet - Robbie Downing - [Undated]
- PLC IPIT & Communications & Baker & McKenzie LLP – Overview of UK data protection regime - Robbie Downing - [Undated]
- PLC Media - Cloud computing and EU data protection laws: a work in progress - [Unknown] - 25 May 2012
- Privacy Identity Innovation.com – Videos – PII 2012 Conference – [Undated]
- Privacy International - Privacy in the developing world: a global research agenda - Carly Nyst - 14 July 2012
- Public Service Europe – Can we trust cloud computing, ISPs and social networks? – Ross MacDonald – 2 April 2012
- Public Service Europe – Cyber-space now seen as 'fifth dimension of warfare' – Chris Hardy – 9 February 2012
- Public Service Europe – Getting to grips with the EU data directive – David Gibson – 18 April 2012
- Public Service Europe – New EU laws to protect data in the cloud – Daniel Mason – 7 December 2011
- Rundfunk & Telekom Regulierungs – GmbH: European regulators face new challenges - Regulation 2.0 - Georg Serentschy - 9 August 2012
- Scripted - Data Export in Cloud Computing - How can Personal Data be Transferred Outside the EEA? The Cloud of Unknowing, Part 4 - W Kuan Hon and Christopher Millard - 15 April 2012
- SearchCloudSecurity.TechTarget.com – Article 29 Working Party cloud computing opinion: Blow to Safe Harbor?
- Society for Computers & Law – G-Cloud v1: Cloud Legal Project's Analysis – [Undated]
- Society for Computers & Law - In Defence of the Cloud - Eduardo Ustaran - 22 May 2012
- Society for Computers & Law - The 12 Cs of Cloud Computing: A Culinary Confection - W Kuan Hon - 16 April 2012
- Taylor Wessing - Why the Clouds of Suspicion? Data Protection and Cloud Computing - January 2011
- Telegraph.co.uk – Facebook's Mark Zuckerberg says privacy is no longer a 'social norm' – Emma Barnett, Technology and Digital Media Correspondent – 11 January 2010
- The African File - The Cloud and Africa Indicators for Growth of Cloud Computing - Alex Laverty - 18 May 2011
- The New York Times - New European Guidelines to Address Cloud Computing - Kevin J. O'Brien - 1 July 2012
- Thomson Reuters – An Overview of Cloud Computing and its Legal Implications in India – Naqeeb Ahmed Kazia – Issue 2, 2012
- TILT (Tilburg Institute for Law, Technology, and Society) - Law & Technology Working Paper Series Regulation of Transborder Data Flows under Data Protection - and Privacy Law: Past, Present, and Future - Christopher Kuner - October 2010

- TRUSTe - TRUSTe CEO Testifies Before Congress - John Gamble - 19 June 2012
- U.S. * EU Safe Harbor Framework - Guide to Self-Certification - March 2009
- West Law - Computer and Telecommunications Law Review 2010 – China's personal data protection on the internet – Hong Xue
- West Law - Computer and Telecommunications Law Review 2010 – Collecting data online: what is best practice? Oliver Bray and Paul Joseph
- West Law - Computer and Telecommunications Law Review 2010 – EU applicable law: clarification on some practical issues relating to data protection – from Article 29 Working Party's Opinion 8/2010 – Pierre-Andre Dubois
- West Law - Computer and Telecommunications Law Review 2010 – United States: electronic commerce – ethics
- Who's Who Legal – Cloud Computing and Data Protection - Dr Ursula Widmer, Dr Widmer & Partners – July 2009

[1] This paper and the comments herein are of a general nature, not to be relied upon in connection with any specific circumstances and no liability is accepted by the author, Charles Russell LLP or the ITU.

[2] James Madison, The Federalist, no 10, 1787. James Madison, Jr was an American statesman and political theorist. He is credited as being the "Father of the US Constitution" for being critical to the drafting of the Constitution and author of the US Bill of Rights. He was also the fourth president of the United States. The Federalists were the first American political party who fashioned a strong new government and approach to drawing the individual states together in the late 18th Century. The Federalist Papers are a series of essays promoting the adoption of the US Constitution.

[3] The power of Cloud: Driving business model innovation, IBM Global Business Services by Saul Berman, Lynn Kesterson-Townes, Anthony Marshall and Robini Srivathsa.

[4] Enhancing the broadband investment environment – policy statement by Vice President Kroes, Brussels, 12 July 2012.

[5] Cisco Global Cloud Index: Forecast and Methadology, 2010-2015.

[6] The power of Cloud: Driving business model innovation, IBM Global Business Services by Saul Berman, Lynn Kesterson-Townes, Anthony Marshall and Robini Srivathsa.

[7] See further the GSR paper on "Demystifying Regulations in the Cloud: Opportunities and Challenges for Cloud Computing."

[8] Computer and Telecommunications Law review 2010, Cloud Computing, Mark Taylor and Matko Matteucci, CTLR 2010, 1692), 57-59.

[9] WK Hon and C Millard, "Data Export Cloud Computing – How can Personal Data be Transferred Outside the EEA? The Cloud of Unknowing, Part 4", (2012) 9:1 SCRIPTed 25. http://script-ed.org.

[10] The power of Cloud: Driving business model innovation, IBM Global Business Services by Saul Berman, Lynn Kesterson-Townes, Anthony Marshall and Robini Srivathsa.

[11] See the GSR paper on "Demystifying Regulations in the Cloud: Opportunities and Challenges for Cloud Computing" for an in-depth discussion of cloud computing.

[12] Cave, Robinson, Schindler, Bodia, Kool van Lieshout; "Does it help or hinder? Promotion of Innovation on the Internet and Citizen's Right to Privacy: European Parliament: Directorate-General for Internal Policies; Policy Department A; December 2011. http://www.europarl.europa.eu/committees/en/studies.html

[13] Global Data Privacy Laws: 89 Countries, and Accelerating; Social Science Research Network; 6 February 2012.

[14] EU Directive 95/46/EC.

[15] 'Data, data everywhere, A special report on managing information', The Economist, 27 February 2010, at 3.'.

[16] BSA,"Global Cloud Computing Scorecard": A Blueprint for Economic Opportunity, 2012.

[17] ITU, "Privacy in Cloud Computing," ITU-T Technology Watch Report, March 2012, http://www.itu.int/en/ITU-T/techwatch/Pages/cloud-computing-privacy.aspx

[18] 2002/58/EC.

[19] Article 5(3).

[20] Subject to the application of the Personal Information Protection and Electronic Documents Act.

[21] Article 29 Working Party WP196 on Cloud Computing, 1 July 2012.

[22] Article 17(1), Data Protection Directive.

[23] Article 29 Data Protection Working Party Opinion 05/12.

[24] Court of Appeal – Michael John Durant v Financial Services Authority [2003] EWCA.

[25] Act 78-17, 6 January 1978.

[26] Commission nationale de l'informatique et des libertes.

[27] Jorg – Alexander Paul, Bird & Bird, as quoted by Kevin J O'Brien, "New European Guidelines to Address Cloud Computing", July 1, 2012.

[28] European Commissions: Commission proposes a comprehensive reform of the data protection rules, 25 January 2012.

[29] Uniting and strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (2001), Public Law 107-58 (***US Patriot Act***).

[30] See for example, Katz v. United States, 389 U.S. 347 (1967).

[31] PLC, Data Protection, USA.

[32] 15 U.S.C.

[33] Controlling the Assault of Non-Solicited Pornography and Marketing Act.

[34] Telephone Consumer Protection Act.

[35] California A.B. 1980 Data Security Law.

[36] California 5.B. 27 "Shine the Light" Law.

[37] SAFE Data Act, H.R. 2577.

[38] Data Accountability and Trust Act of 2011, H.R. 1841.

[39] S.8.

[40] See, Hunter v Southam (1984) 2 SCR 145 (CA).

[41] Jones v Tsige (2012) ONCA 32 (CA).

[42] Article 5, X and XII.

[43] Article 12, Law 10 406/2002.

[44] Article 21, Law 10, 406/2002.

[45] Under Article 43.

[46] S.69.

[47] Article 21 of the Constitution, see Kharaj Singh v State of UP (Air 1963 SC 1296).

[48] S.43.

[49] S.72-A.

[50] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011.

[51] Specifically, the International Standard IS/ISO/IEC 27001 on "Information Technology – Security Techniques – Information Security Management System – Requirements".

[52] See Economist, Private data, public rules, 28 January 2012.

[53] PLC, Data Protection – Japan, Brazil, South Africa and India.

[54] Act No. 57 of 2003.

[55] Articles 21 and 22.

[56] BSA Scorecard, pg 3.

[57] Gartner has indicated Europe is two years behind the US in adopting cloud services because of the confusion and concerns over privacy.

[58] See section 3.

[59] See section 3.1.

[60] See section 3.3.3; and London Economics; "Study on the economic benefits of privacy – enhancing technologies (PETs); Financial Report to The European Commission, D G Justice, Freedom and Security.

[61] Practice Note: PLC General Counsel briefing: privacy and data protection.

[62] International Chamber of Commerce; "Cross-border law enforcement access to company data – current issues under data protection and privacy law; Document NO. 373/507 – (7 February 2012).

[63] See Section 5.

[64] ICC (as above).

[65] International Conference of Data Protection and Privacy Commissioners, "International Standards on the Protection of Personal Data and Privacy: The Madrid Resolution", 5 November 2009.

[66] Oracle, IBM, Hewlett-Packard, Walt Disney, Microsoft, Accenture, Google, Intel, Proctor & Gamble and General Electric.

[67] Speech/12/38; 26/01/2012 Neelic Kroes, Vice President of the European Commission responsible for the Digital Agenda; "Setting up the European Cloud Partnership".

[68] ITU, "Privacy in Cloud Computing," ITU-T Technology Watch Report, March 2012, http://www.itu.int/en/ITU-T/techwatch/Pages/cloud-computing-privacy.aspx

[69] Some examples of other privacy principles: OECD (Privacy Principles 1980), Generally Accepted Privacy Principles (GAPP) from AICPA, FTC Fair Information Practice Principles (FIPPs) (ref: United States Privacy Act of 1974), Consumer Privacy Protection Principles (CPPPS), Asi-a Pacific Economic Cooperation (APEC) Privacy Framework – Information Privacy Principles (2005) and International Security, Trust & Privacy Alliance (ISTPA) Privacy Principles.

[70] Kuhn, (2011), "Regulation of Transborder Data Flows under Data Protection and Privacy Law – Past, Present and Future", OECD Digital Economy Papers, No. 187, OECD Publishing.

[71] Google Transparency Report, August 2012.

[72] WP179.

[73] UK Information Commissioner's Office.

[74] CNIL, 32nd Annual Activity Report 2011.

[75] Data Protection and Privacy, Jurisdictional Compensations 2012.

[76] BFDI, Annual Activity Report 2009/2010.

[77] August 2012, http://mashable.com/2012/08/09/ftc-google-22-5-million/

[78] Office of the Privacy Commissioner of Canada.

[79] The seven principles include commitments as to Notice, Choice, Onward Transfer of data, Security, Data Integrity, Access and Enforcement. "US-EU Safe Harbour Framework", Guide to Self-Certification, March 2009.

[80] Burton, A, "Cloud Industry Forum launches Code of Practice", Business Computing World, 22 November 2010. Members of the CIF include UK PLC, APMG-International, Channel Cloud, Citrix, Claranet, Concorde Databarracles, Dell, etc. For a full list of members and more information see www.cloudindustryforum.org.

[81] The CSA members include ASTRI, US Dept of Defense, Ericsson, Adobe, Accenture etc. For a full list of members and more information, see www.cloudsecurityalliance.org.

[82] Schellman, C. "SOC 2 For Cloud Computing", October 10, 2011.

[83] Autonomy Cloud Solutions – Product Brief.

[84] WP 196.

[85] Privacy Enhancing Technologies : A Review; Yun Shen & Siani Pearson, HP Laboratories; HPL-2011-113.

[86] Other examples of PETs can be found at Stanford's Center for Internet and Society. http://cyberlaw.stanford.edu/wiki/index.php/PET

[87] London Economics; Study on the economic benefit of privacy-enhancing technologies, pg xi.

[88] Ibid.

[89] Laverty, A; "The Cloud and Africa – Indicators for growth in Cloud Computing; The Africa File"; 18 May 2011.

[90] Nyst, C: "Privacy in the developing world: a global research agenda"; Privacy International, 14 July 2012.

[91] Kuner, C. (2011), "Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future", OECD Digital Economy Papers, No. 187, OECD Publishing.

[92] European Commission.

[93] London Economics; "Study on the economic benefits of privacy-enhancing technologies (PeTs)"; Final Report to The European Commission D G Justice, Freedom and Security; July 2010.

[94] Special Eurobarometer 359/Wave 74.3 – TNS Opinion and Social : Attitudes on Data Protection and Electronic Identity in the European Union (July 2011). The Eurobarometer research also reported that six in ten Internet users usually read privacy statements (68%) and that majority (70%) that did so adapted their online behaviour. Levels of trust in companies active on the Internet was reported to be low: less that one-third (32%) trust (mobile) phone companies or Internet Service Providers and just over one fifth (22%) trust other Internet companies like search engines, social networking sites and e-mail services. The research further discovered that 70% are concerned that their personal data held by companies may be used for a purpose other than that for which it was collected. A majority (75%) wanted to delete personal information on a website whenever they decide to do so.

[95] London Economics.

[96] "The natural person, public authority, agency or any other body which alone or jointly with others determines the purposes and means the processing of personal data" – European Directive, Art. 2 (d).

[97] Working Party (WP169).

[98] Examples include OECD Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data (1980); APEC Privacy Framework (APEX Secretariat, 2005); and The Madrid Resolution (2009).

[99] Christopher Kuner has considered these issues thoughtfully and in detail. See: Kuner, C. (2011), "Regulation of Transborder Data Flows under Data Protection and Privacy Laws: Past, Present and Future", OECD Digital Economy Papers, No. 187, OECD Publishing; and for more detail – Kuner, C. "Regulation of Transborder Data Flows under Data Protection and Privacy Laws: Past, Present and Future"; TILT Law & Technology Working Paper No. 016/2010 and Tilburg University Legal Studies Working Paper No. 016/2010.

[100] a World Trade Organisation treaty that came into force in 1995

[101] GATS Article XIV (c)(ii).

[102] For example, the PIPEDA expects the accountable person to have received some assurance that personal data transferred will continue to receive protection; and the EU recognises exceptions if binding corporate rules or standard EU contractual clauses are put in place.

[103] European Consultation: Cloud Computing – Public Consultation Report dated 5 December 2011.

[104] Alexander Hamilton, The Federalist, no. 26, 1787. Like James Madison, Alexander Hamilton was a "founding father" of the United States. He was a soldier, economist, political philosopher, as well as the first US Secretary of the Treasury.