

available at www.sciencedirect.comwww.compseconline.com/publications/prodclaw.htm

**Computer Law
&
Security Review**

Cursing the Cloud (or) Controlling the Cloud?

Noriswadi Ismail¹

MARA-SPC Scholar, HeiTech Padu Berhad, Malaysia

A B S T R A C T

Keywords:

Cloud computing
Cloud Compliant Strategy
Safe Harbor
Data protection
Cloud privacy
Binding Corporate Rules

Inspired by the cloud computing hypes, this paper responds to some of the hypes, but not to all. The hype in this paper refers to the level of the adequacy of data protection and privacy in a cloud computing (the Cloud) environment. Paradoxically, this paper proffers observational insights that surround the Cloud from the perspectives of data protection and privacy. It examines briefly the efforts of January 2010 led by Microsoft and anticipating “liability” scenarios. The liability rhetorically refers to the illegal access in the Cloud. This paper does not focus entirely on the technology sophistication; however, it analyses two scenarios of illegal access. To mitigate the liability, it suggests a “Cloud Compliant Strategy (CCS)” being a proposed model to control the Cloud. The observational insights of this paper have also intertwined with the adequacy of data protection from the lenses of the European Union (EU) Data Protection Directive 95/46/EC (DPD) and Safe Harbor provisions (SH).

© 2011 Noriswadi Ismail. Published by Elsevier Ltd. All rights reserved.

1. Introduction

When the first draft of this paper was being written, the London Olympic 2012 was just 515 days away. The BBC has mulled over the usage of cloud support for its London Olympic 2012 coverage (Summer, 2010). One of the headlines of the discussions, amongst others, is the security aspect of cloud service. In the EU, on 7 September 2010, the European Commission President Jose Manuel Barroso declared: “We will deliver a single digital market worth 4 percent of EU GDP by 2020” (Schultz, 2010). This is in line with the EU commitment to its Digital Agenda. The creation of integrating digital networks across the 27 Members States has enticed cloud providers to solicit and compete for potential cloud business. China, which has the second largest economy in the world, has embarked on an ambitious cloud computing project, which will enable the country to develop the first cloud computing system by the end of 2010. (Chinatechnews.com). The emergence of cloud computing is, however, fraught with risks. There is potential privacy risk in managing and retaining such data subjects’ data, which is parked within a mobile server.

Given the Cloud’s emergent progress across the globe, this paper aims to examine the level of adequacy of data

protection and privacy in the Cloud environment focussing on these two legal instruments: Data Protection Directive (DPD) and Safe Harbor (SH). Should the level of adequacy remains as based on the existing provisions? Or should there be supplemental guidelines or guidance that could be offered? Or should there be a specific or proposed laws and regulations that are bespoke for the Cloud?

2. Research methodology and limitations

The adopted research methodology is based on periodic review, analysis and observations of primary and secondary materials that are accessible from the period of December 2009 until February 2011. The cut off date of this research is as at February 2011, based on the observations, discussions and follow up research with numbers of subject matter experts and academics particularly in Queen Mary Cloud Computing Legal Research Project, London, United Kingdom, HeiTech Padu Berhad, Malaysia and leading Technology, Media and Telecommunications legal firms in London, United Kingdom. There are five main limitations that have been discovered:

¹ Academic Visitor (14 February 2011–4 April 2011), The Centre for Socio-Legal Studies, University of Oxford, UK. 0267-3649/\$ – see front matter © 2011 Noriswadi Ismail. Published by Elsevier Ltd. All rights reserved. doi:10.1016/j.clsr.2011.03.005

First, the subject matter concerned is very much newly debatable in legal discussions and discourse across the globe. Hence, different regions have different interpretations. Due to this, this paper does not address all of the hypes, but limits the discussion to the adequacy of data protection approaches in the Cloud environment. Second, as data protection and privacy laws suggest, the legal stance in each countries differ. As such, macro observations are only limited to the DPD and SH. Third, search of the most accurate cloud taxonomy remains technically taxing. Divergence of definitions has proven to be stimulating in the context of computing. Critically crucial, however, this paper opts for a taxonomy that leads to the birth of a diagrammatic illustration, pictured in Fig. 1 (below). Fourth, on 4 November 2010, the European Commission (2011) (EC) issued a public consultation paper on ‘A comprehensive approach on personal data protection in the European Union’, which aims to improve and simplify the current legal frameworks under the DPD. Fifth, the similar approach is also taken by the Council of Europe to modernise the data protection convention (Convention 108) in order to accommodate with globalisation and technology realities. Due to these ongoing developments, this paper will only take into cognisance prior to the EC and Council of Europe chief initiatives.

3. Taxonomic cloud

There are various definitions of cloud computing. Perhaps, the ideal definition of cloud computing is provided by Svantesson and Clarke (2010), where the author referred to the working definition of Vaquero and others (Vaquero et al., 2009). These definitions seek to define cloud from the technical perspectives that may be able to match the Cloud landscape. Vaquero and others have proposed the definition as:

“...a large pool of easily usable and accessible virtualized resources (such as hardware, development platforms and/or services). These resources can be dynamically re-configured to adjust to a variable load (scale), allowing also for an optimum resource utilisation. This pool of resources is typically exploited by a pay-per-use model in which guarantees are offered by the Infrastructure Provider by means of customized Service Level Agreements (SLAs)...” (p. 51).

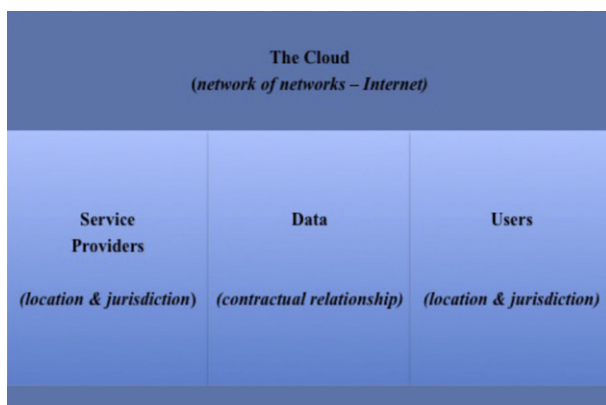


Fig. 1 – The Cloud inter-relationship.

By inferring to Vaquero and others’ definition, Roger Clarke provides a broader context by classifying five conditions that render cloud computing service (Svantesson and Clarke, 2010). They are: (1) the service is delivered over a telecommunications network (2) users rely on the service for access to and/or processing of data (3) the data are under the legal control of the user (4) some of the resources on which the service depends are “virtualised”, which means that the user has no technical need to be aware which server running on which host is delivering the service, nor where the hosting device is located and lastly, the service is acquired under a relatively flexible contractual arrangement, at least as regards to quantum used.

Whilst the above definitions are generally technical, most of the Cloud’s definitions possess the inter-relationship between the service providers, the data that are being transmitted via network of networks (the internet), users, geographical reach, location, jurisdiction and lastly, contractual relationship between and amongst the parties or actors who are involved. The inter-relationship is illustrated in Fig. 1 below:

Applying the above Fig. 1 within the context of the Cloud environment, it is observed that Clarke, Vaquero and others may apply the context of their definitions within the diagram. There are four actors in the diagram; the Internet, the service providers, the data and the users. These actors engage between each other through various terms of reference, liabilities and expectations from one end to the other end (Bradshaw et al., 2010). In other words, single actors in the above diagram are bound by their respective obligations (Bradshaw et al., 2010, p. 15–39). The respective obligations may also accrue to having the informational rights in the Cloud (Reed, 2009). It should be noted that the above diagram offers a lateral understanding, instead of any extended definition of the Cloud. The actors in this diagram may also be extendable to the third parties’ rights, obligations and liabilities (Reed, 2009). Of slight relevance, to the taxonomy, Jonathan Zittrain (2009) views that there are “tethered appliances” within the Cloud He cautions that such devices may be particularly insidious because the code and data may well remain near the user so they do not seem to be cloud computing devices. Such tethered appliances include the ubiquitous iPhone and Amazon’s Kindle reading device (OPC, 2010).

In the Clouds’ taxonomy, service providers have generally divided the offerings into Hardware as a Service (HaaS), Platform as a Service (PaaS) or Infrastructure as a Service (IaaS) and Software as a Service (SaaS). Bradshaw, Millard and Walden opined that there may be a combination of one service to another, and it may also come independently (Bradshaw et al., 2010, p. 8). In SaaS, software applications are run on a SaaS service provider’s system and retrieved by users through the Internet. The application is not run on the users’ Personal Computers (PC) or servers, but within the SaaS service provider’s facilities (Joint et al., 2009, p 270). In PaaS or IaaS, the service provider operates the whole computing and operating system for the users through the Internet. In a normal business case for service providers, PaaS or IaaS provides the operating systems, hosted software and data storage. These are bundled together with technical support and maintenance (Joint et al., 2009, p. 271). In SaaS, service

providers fix the price of applications based on usage and the terms of engagement with the users. The latter is, generally, a business case. Some service providers extend its offerings to Software as a Secure Service (SaSS), which includes security service, disaster recovery facility and other complimentary, or added value services (Padu*MOB HeiTech Padu Berhad, 2009).

4. Microsoft initiative

4.1. Calling for Cloud confidence

Microsoft published an eight-page document dated January 2010 entitled 'A Proposal for Industry and Government Action to Advance Cloud Computing' (Microsoft, 2010; Kang, 2010). There are four central calls. Firstly, Microsoft proposes a call for responsible government action in strengthening the privacy regime in the Cloud. The software giant elucidates that related laws on the usage of cloud technologies and its future laws should be considered. Secondly, it proposes enhancement of security for the purpose of strengthening criminal and civil enforcement mechanisms against malicious hacking of cloud services. Thirdly, a call for transparency in security enhancement and fourthly, promoting user confidence in the Cloud via common approaches to jurisdiction. These calls have also proposed the US Congress to amend the Computer Fraud and Abuse Act (CFAA), as a measure to combat unauthorised access to data stored in the cloud and on a similar vein, to amend the Electronic Communications Privacy Act (ECPA). This paper will not do this, however, paraphrasing the rationales of each call. Instead, it will offer macro observations on ECPA and CFAA respectively (Microsoft, 2010, p. 7–8).

Privacy, in the United States of America (US), is a constitutional right under the Fourth Amendment of the Federal Constitution. The ECPA, in particular, was enacted in 1986 with the legislative aim to provide a comprehensive privacy framework for data shared or stored in various types of telecommunications services. ECPA, based on Microsoft's call, lacks the application to keep abreast with technological innovations as the legislation was drafted based on pre-Web foundation (Microsoft, 2010, p. 3). Basic definitional terms on electronic communications and remote computing services are, arguably, no longer intelligible and sensible within the context of the Cloud (especially the service providers). Due to this definitional lag, the courts and law enforcements face arduous tasks in determining the applicable definitions. Microsoft argues that the ECPA has been overridden by technological change and the needs to strike the balance between consumers' privacy interest and the government's legitimate needs are valiantly crucial (Microsoft, 2010, p. 4; Smith, 2010). The need to reform and modernise ECPA, as observed by Microsoft, can create users' privacy concerns in the Cloud, and thus impact upon confidence in the cloud.

Digital crime, is Microsoft's concern in the Cloud. The CFAA, is the legislation that combats such attempts by thieves, fraudsters and malicious hackers. Two proposed amendments of CFAA are called for. Firstly, the establishment of presumed losses attributable to unauthorised access to accounts hosted online. For the purpose of establishing thresholds for related felony penalties, the proposed quantifiable value that exceeds

USD 5,000 under § 1030(c)(2)(B), and information that is obtained via fraud over under § 1030(a)(4). Microsoft proposes that the prosecution can establish the value by multiplying a specified statutory amount by the number of offences and violations through separate unauthorised accessed account (Microsoft, 2011, p. 5). Secondly, Microsoft proposes different quantification criteria in relation to the penalties for malicious hackers that hack into a single cloud datacenter that corresponds to the number of user accounts illegally accessed. The present provision of the CFFA is currently USD 250,000, based on a single Personal Computer (PC). Due to the Cloud environment, violation may occur by users (whether individual or business) and such violations should be quantifiably based on a per user account instead of a single PC. The key rationale for the Microsoft's call to amend the penalty provision is to enable the prosecution to secure larger penalties for hackers that illegally access the Cloud (Microsoft, 2011, p. 5).

Civil action against digital criminals is also an indispensable agenda for the CFAA reformation. To effectuate such agenda, Microsoft proposes the amendment of CFAA's civil action provision that the cloud service providers possess a private right of action against those who illegally access their datacenters or secure unauthorised access of their customers' accounts. This proposed cause of action shall bring the bearing rights to the cloud service providers to combat digital criminals on behalf of their customers (Microsoft, 2011, p. 5). The call continues by proposing meaningful statutory damages for successful civil actions instead of requiring plaintiffs to prove economic damages.

4.2. Observation

Based on the Microsoft proposal, the US legislative regime attempts to tackle privacy concern vis-à-vis the Cloud through ECPA and CFAA respectively. It does not, however, aim to tackle privacy from the perspective of SH. Ideally a rethinking on this concern is relevant. The nature of the Cloud does not only involve the US jurisdiction, but also extendable to other jurisdictions. Due to that, it should be painstakingly observed that the cross border effect of such digital crimes in the Cloud might attract the Congress' attention. The Cloud environment is not creating legal chaos in the legal sphere. However, it creates the platform for existing US legislation to reform and to suit with its technology and infrastructure. The objective of fact, as opined by Chris Reed (Reed and Angel, 2007) and the circumstantial context of a particular fact as propounded by Edwards and Waelde (2009, p. 447–451) should be fundamentally appraised prior to reforming such existing data protection or sector specific laws and legislation. This, in effect, will rigorously render a good law making, in contrast to a bad law making (Reed, 2010). In addition, whilst this paper was in preparation, a preliminary Federal Trade Commission Staff Report titled 'A Proposed Framework for Businesses and Policymakers' was issued. The proposed framework is to be applied to all commercial entities that collect or use consumer data that can be reasonably linked to a specific consumer, computer or other device (FTC, 2011). It will be particularly interesting to gauge the feedback from the participating stakeholders once the FTC has reviewed and finalised its stance, particularly from the cloud computing perspective.

5. Cursing the Cloud

5.1. Illegal access

The Cloud opens the doors to many users: it is flexible, cost effective and susceptible to criminal behaviours. Violations in technology crimes are very challenging and it gets alarming if the users are not able to comprehend its taxonomy. Digital crime in the Cloud is a prevalent one. Two scenarios are hypothetically outlined: firstly, illegal access in the Cloud by the service providers and secondly, illegal access in the Cloud by the users. There are, of course, potentially many scenarios of illegal access in the Cloud that may take place. Nevertheless, this paper focuses on these two scenarios.

First scenario: This assumes that Service Provider X is a multinational based in an Asian jurisdiction, which does not have a data protection and privacy law. It has investment outreach in countries where data protection and privacy laws are still premature. Besides the Main Outsourcing Agreement, in its cloud computing service, Service Provider X adopts contractual arrangement via Service Level Agreements (SLAs) that incorporate controls and measures in retaining, controlling and deleting data for its customers (which consist banks, insurance companies and governmental departments). In other words, the SLAs provide provisions that are adopted from the respective customers' regulatory and compliance requirements of sector specific laws). But, the SLAs lack terms and conditions that relate to criminal provisions that are attributed by the Service Provider X, the customers and the third parties who are directly dealing with the SLAs. If a disaster occurs in a data centre due to illegal access or unauthorised access, who should be liable?

In the above scenario, in the absence of such specific terms in relation to criminal penalties, it is argued that every party may be collectively liable. The nature of SLAs should be able to outline back-to-back terms, which include liabilities and damages that are jointly and severally applicable and liable. Existing cloud service providers should be able to specify detailed terms and conditions of their cloud offerings not only limited to the agreements, but also other supplemental terms and conditions (Bradshaw et al., 2010, p. 8). The illegal access or unauthorised access in this context is one of the digital crimes that may potentially occur. The difficulty in this arrangement is to quantify the damages that may occur due to the illegal access. In addition, to authenticate or to pursue such a digital investigation takes a herculean process especially within a complex application or system (Walden, 2007, p. 205–213). Thus, it requires careful examination and to a certain extent involving specialised forensic investigation. Arguably, one may consider instituting an action against Service Provider X due to lack of controls in its project management. However, the objectivity of such an action should be justifiably proven based on the cause of action and the parties involved, directly and indirectly to such an illegal access. In this context, the objective of fact applies (Reed and Angel, 2007).

Second scenario: Assuming user Y is an ex-employee of Service Provider X who is technically competent and involved in the cloud computing service. User Y creates a pseudonym purportedly being one of the users through identity theft. User Y hacks the cloud applications of Service Provider X's customer (a bank). Who should be liable?

In this second scenario, it does not only involve potential criminal conviction against Y, but also potentially cross-examining the terms and conditions that are related to Y's resignation from Service Provider X.

This scenario is critically crucial to determine the next cause of action; whether the confidentiality of security must be maintained at the utmost level or whether the knowledge that Y has gained from the previous employment in Service Provider X, shall be a justifiable cause of action to institute a suit. In this scenario, employee's mobility in technology projects is a norm. The mobility, on the one hand, provides advantage to a competitor to leverage the know-how and on the other, provides disadvantage to the ex-employer. In this scenario, the purported action of identity theft by Y has to be substantiated into a different context. Two possible examinations must be made. Firstly, whether Y's action is based on his own criminal intention (*mens rea*) or secondly, whether it is motivated or solicited by other corroborative parties. In this regard, Y could be liable if the intention proves to be malicious. However, arguably, Service Provider X may also be subjected to investigation depending upon the terms and conditions of contractual arrangement between Service Provider X and Y.

5.2. Observation

The two scenarios above have 2 different faces in a mirror. One face mirrors the Service Provider X obligations, terms and conditions and liabilities and the other face mirrors Y, the ex-employee of Service Provider X, who acts maliciously via identity theft. There is a co-existence and inter-relationship from the latter and the former. In other words, criminal liabilities are accruable. Arguably, cursing the Cloud does not mean that the technology imposes more hardship and difficulties. Nevertheless, cursing the Cloud means pre-emptively examining every possible criminal scenario that may attribute by criminals of digital crime.

One may argue that it is almost impossible to list down all potential crimes within the context of digital crime in the Cloud. However, there are cloud service providers, which have extended future terms to control and regulate such behaviours (Bradshaw et al., 2010, p. 8). In these scenarios, the Cloud does not only attract contractual issues on the SLAs. However, in the digital crimes context, it also extends to these acts of crime: extortion, fraud, information acquisition, information supply, phishing and money laundering (Walden, 2007, p. 66–67). As the above scenarios do not include any specific jurisdictions, it is observed that they may potentially occur in any jurisdiction. Microsoft, in its call to promote user confidence in the Cloud through common approaches to jurisdiction, succinctly points out that:

“...there are, however, no universally agreed upon rules governing such access by law enforcement. The result is that service providers are increasingly subject to divergent, and at times conflicting, rules governing jurisdiction over user content and data. Further complicating the problem is the fact that the jurisdictions also have different laws regarding privacy rights and data retention...” (Microsoft, 2011, p. 7).

The latter reflects the dilemma in scenario 1 and the Cloud which requires possible controls at this stage to be considered.

6. Controlling the Cloud

6.1. Is adequacy level of SH sufficiently safeguarded?

The context in which laws apply in the Cloud attracts service providers and users. This discussion does not attempt to argue nor does it opt which laws should take precedence. Neither does it purports to analyse the strength, weakness, opportunity and threat that these may pose.

As observed in Section 4.2, Microsoft’s call for cloud confidence does not suggest strengthening the Safe Harbor – a self-regulation instrument – that is shaped by commercial and consumer preferences based on market share. Joep Ruiter and Martijn Warnier (2009) and Strauss and Rogerson (2002) opined that Safe harbor (SH) is a result of consumer preferences that determine the market share, and that a higher market share leads to higher profit. In the Cloud environment the subject matter of adequate levels of protection of data remains questionable. Taking the example of *first scenario* in Section 5.1 above, if Service Provider X outsources part of its application functions to a US based cloud service provider, the chief concern is to determine whether SH will be able to address the adequacy of data protection in the Cloud? If yes, is the SH agreement suffice or if not, do supplemental terms and conditions need to be bundled together? Alternatively, other sector specific laws related to privacy may apply. Moreover, should SH extend its commitment to digital crime not only within the US, but also globally?

In addressing these concerns, SH, arguably, benefits only EU businesses as all 27 Member States will be bound by the EU Commission’s finding of adequacy (Morgenthaler et al., 2010, p. 25). As the nature of SH agreement with the EU Member States are regulated with the US, European citizens can institute claims against such US cloud service providers in the US contour. However, if one is to apply the SH, being the only legal instrument addressing these concerns beyond the EU, the level of adequacy of data protection is arguably lower. To the contrary, the level of adequacy may be acceptable by the DPD standard if supplemental terms and conditions are bundled together based on the customised sector specific laws relating to privacy. The question as to whether SH should extend its coverage to digital crime is considerably beyond than the scope of SH as the ECPA and CFAA are able to address and accommodate such potential issues that may arise. On the contrary, the reality of SH is that it is a manifestation of commercial incentive, and hence, the self-regulatory approach only binds parties who are certified under the SH agreement.

6.2. Is adequacy level of DPD sufficiently safeguarded?

The EU Data Protection Directive’s (DPD) approach in determining the level of data protection adequacy is painstakingly vigorous. Applying the DPD principles vis-à-vis the *first scenario* in Section 5.1, if Service Provider X outsources part of its application functions to an EU based cloud service provider, the questions to be substantiated are whether consent has been sought from the data subject (in this context, Service Provider X’s customers), whether there is a contract with the data subject? Or whether a legal obligation has been formalised? Or whether such special regulations apply? If all of these questions are in the affirmative, the processing of data in the Cloud complies with the DPD, and thus, the level of adequacy is generally acceptable (DPD, Article 25/6). Service Provider X, based on the DPD definition, is the controller (DPD, Article 2 (d)). Service Provider X has to ensure that the rights of data subject and the controller’s own legal obligations are covered which includes notification, provision of information, correction, erasure or blocking. However, if the answers to these questions are in the opposite, the level of adequacy of the data is critically questionable.

There are specific conditions, wherein the DPD allows the transfer of personal data to countries outside the EU. Taking Service Provider X, as a repeated example, the EU based cloud service provider may realise the adequacy level through contractual terms and conditions and a code of conduct concerning data protection globally (Morgenthaler et al., 2010, p. 23). In the Cloud environment, data transfer may be possible subject to the consent of Service Provider X’s customers; the performance of contract in the interest of Service Provider X’s customers; Service Provider X and the EU based cloud service provider; and the consent of governing data protection regulators or Information Commissioner if Service Provider X demonstrates adequate safeguards in its contractual arrangement (DPD, Article 25/6).

6.3. Observation

Safeguarding the adequacy level of data protection in the Cloud is axiomatically lucid if Service Provider X tailors the obligations concurrently consistent with the parties involved. The questions of adequacy between SH and DPD are equally applicable within the context of the objective of fact and the circumstances of the Cloud arrangements. In SH, there are seven requirements that Service Provider X should self-regulate: notification; choice; access; security; data integrity; onward transfer and enforcement (Safe Harbor, US–EU Safe Harbor). In such agreements relating to SH, Service Provider X may be able to detail down its commitment to self-regulate these requirements. The DPD, in addition to what has been discussed in Section 6.1 above, also offers the Binding Corporate Rules (BCR) approach that Service Provider X may consider to opt into. Admittedly, the Cloud, in the context of safeguarding data is still very much regulated through contractual arrangement which carries supplemental terms and conditions that are bundled with additional protection. Service Provider X may have two options to consider whether SH or DPD. It is possible, however, to consider an alternative model that this paper proffers in Section 7 – the CCS. As a prologue,

this model does not suggest overriding precedence to either the SH or DPD, but, suggesting a model for jurisdictions that may not be able to comply and safeguard the adequacy of data protection in the Cloud.

7. CCS

7.1. What constitutes CCS?

Some jurisdictions are still grappling with data protection and privacy laws. Privacy International has updated its data protection laws map, as pictured in Fig. 2 below: -

As of May 2010, the countries in blue denote comprehensive enacted data protection laws. Countries in red denote pending efforts to enact law and the countries in white denote no laws at all (Privacy International, 2010). Appropriately, the US should not be under the category of no laws as the effort that reflects through SH agreement with the EU is strongly prevalent as analysed in Section 5.1 above. From this map, the world of data protection law is divergently divided based on its regional and continental economic spheres and technological outreach. From the economic perspective, these regions have a strong incentive to join the 'network effects' which involve consumers, companies and the network of networks (*The Economist*, 2010). In the context of the Cloud, Service Provider X may establish its cloud business arrangement with any countries subject to its expansion and future demands. If the latter may possibly happen, the proposed and coined – *Cloud Compliant Strategy* – may be adopted as a bespoke model. The CCS constitutes four fundamental cloud compliant tiers. Tier 1 classifies cloud contractual arrangements with jurisdictions which have data protection and privacy laws. Tier 2 classifies the jurisdictions which have its law, but fall short in terms of the maturity of laws in addressing technological innovation

TIERS	Applications
TIER 1	Horizontal
TIER 2	Vertical
TIER 3	Vertical
TIER 4	Horizontal

Fig. 3 – The Cloud compliant strategy model.

and advancement. Tier 3 classifies the jurisdictions which have piecemeal sector specific laws and Tier 4 classifies the jurisdictions that do not have such data protection and privacy laws at all. These classifications are prevalent so that the relationships of actors in the Cloud are compliantly intact (Fig. 1). There are two applications to adopt the CCS; horizontal and vertical. Horizontal refers to the bundling of terms and conditions besides complying with the existing data protection and privacy laws, whilst vertical refers to non-bundling terms and conditions based on sector specific laws. The vertical and horizontal applications may also be extendable to civil and criminal suits that relate to the Cloud. Fig. 3 illustrates:

7.2. Justifiable hypothesis of CCS

Whilst awaiting the next decade of such legislative reform in the advent of technological progress with the Cloud, it is submitted that this proposed CCS model is able to offer Service Provider X a potential temporary option. This is based on the assumption that governments and legislatures will take considerable time to suggest pathways to firmly legalising and regulating the Cloud. This sentiment is perhaps, a cliché, not only in the Cloud context, but also in respect of

Data Protection Laws Around the World

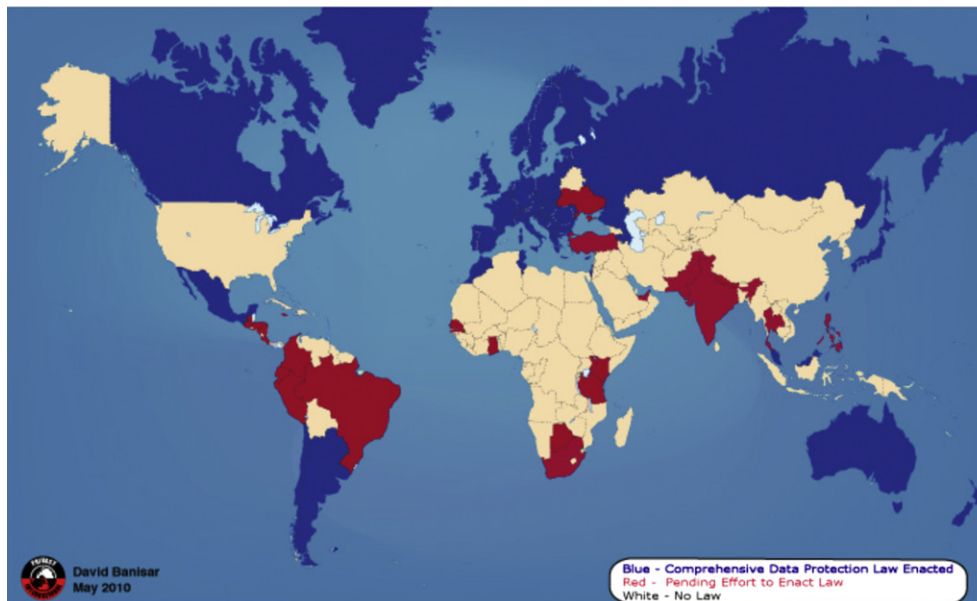


Fig. 2 – The Laws as of May 2010.

other technology-based related matters that are expeditious to the laws and regulations. As Ian Walden succinctly noted:

“...law reform is a generally slow process, requiring parliamentary time, political enthusiasm and external lobbying. Sometimes, the length of process is reflected in the product, a compromise of interests and issues, while the world has often moved on...” (Walden, 2007, p. 59).

Another derived assumption is based on the level of data protection and privacy awareness of a specific jurisdiction within the Cloud environment. The nature of the Cloud is arguably akin to the birth of the Internet which opens a box of legal issues (Lessig, 2006, p. 53–58).

Interestingly, a possible criticism of this CCS model is that one may argue that Tier 4’s application tends to strictly impose a compliant culture instead of imposing one-sided terms and conditions. One may argue that unfair contract terms may occur in Tier 4 due to its one sided and loop sided application. To debunk, it is submitted that SH agreement requirements and the DPD’s Binding Corporate Rules (BCR) may offer shielded and safeguarded protection. In addition, this CCS may also be adopted within the context of the Cloud of Clouds. This means that the underlying fundamental characteristic of this model is hybridly flexible. The Cloud of Clouds refers to a collection of connectivity of other clouds that are potentially integrated. For instance, the EU commitment to produce a single digital market anticipates an integration of clouds (Globalpost, Schultz). The situation will be more complicated and sophisticated especially when it comes to interoperability and standards. Both of these, however, are not the central discussion.

7.3. Observation

The Code 2.0 as elucidated by Lessig is the grounded theory that leads to the hypothesis of CCS. This is also in consonant with Reidenberg’s theory of *Lex Informatica* which appreciates the role of technology that regulates the users’ behaviours (JR, 1998, p. 558). These two authoritative theories have persuaded such a CCS model to be introduced. The CCS aims to address the scenarios of different jurisdictional approaches and styles in the Cloud environment. It does not only apply to service providers, which are based in a jurisdiction that does not have data protection and privacy laws, but also, the others. It is observed that the CCS model can be aimed to safeguard the adequacy of data protection in the Cloud that is holistically hybrid. What hybrid means is that the application of the CCS model is able to match the uncertain gap that may arise between the service providers and users.

A related observation on the CCS model is that its application is based on contractual arrangement between and amongst the service providers and users. CCS, however, is considerably a macro model, instead of a micro model. It is observed to be a model of “soft-law” mechanism, which targets to reduce the need for governmental intervention and provides a flexible and responsive regulatory regime, particularly appropriate in the Cloud environment (Ashworth, 2003, p. 195). The chief limitation appears if digital crime in the Cloud emerges within the CCS applications. To mitigate this

limitation, as in the case of Service Provider X, and the *second scenario* in Section 5.1 above, a separate set of supplemental enforcement and penalties terms may be incorporated. Such classifications of digital crimes in the contractual arrangement – whether through horizontal and vertical applications – may, arguably, complement the limitation of this model. This is based on the assumption that the jurisdictions under each Tiers of the CCS model have had legislation passed dealing with cyber crime and computer crimes.

8. Concluding remarks

From the outset of this paper, the calling for confidence in the Cloud by Microsoft represents a private-public policy making approach. From the inset, the proposed ECPA and CFAA reformation by Microsoft is regarded as a convincing move to lobby the Congress to accept such calls. The liability and control that may derive from the Cloud is not limited to the given scenarios, but also extends to other modes of digital crime. This article has discussed the adequacy of data protection that SF and DPD may offer to cloud service providers and the actors. The two examined scenario analyses are hypothetical and may potentially be used as a basis or a platform for further discussion and debate. Two correlated links have emerged throughout this article: pragmatism of the CCS model and maturity of the CCS model. The former concerns the level of effectiveness in practice, especially to the service providers.

If this model is to be taken into the test bed and proves to be workable the author will engage in future constructive criticism and dialogue to enhance such existing gaps. The latter concerns the maturity of the model – whether it remains just a theoretical model to impress – or, whether it remains a potential model to be adopted by commercial interests – or, whether it remains a potential model for future legal, regulatory and policy guidance. *Apropos*, the suggested CCS model is relatively just a possible option, which is unlikely to inhibit control of the Cloud, and is likely to offer substantial enhancement. It is hoped that this article will contribute to such future guidance in the Cloud. Controlling the Cloud is necessarily cumbersome; condemning the Cloud is simply unproductive.

Noriswadi Ismail (noriswadi@gmail.com). MARA-SPC Scholar, HeiTech Padu Berhad, Malaysia

REFERENCES

- Ashworth A. Principles of Criminal Law. 4th ed. Oxford: University of Oxford Publication; 2003.
- Bradshaw S, Millard C, Walden I. Contract for clouds: comparison and analysis of the terms and conditions of cloud computing services, QMUL cloud legal project 2009. Retrieved February 28, 2011, from, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1662374; 2010.
- Chinatechnews. Chinatechnews. Retrieved: <http://www.chinatechnews.com/2010/09/07/12490-chinas-inspur-to-launch-cloud-computing-operating-system-this-year>; 2010.
- Edwards L, Waelde C, editors. Edwards and Waelde: Law and the Internet. Oxford, Portland & Oregon: Hart Publishing; 2009.

- European Commission Justice. Retrieved February 28, 2011 from http://ec.europa.eu/justice/policies/privacy/news/docs/pr_16_12_10_en.pdf.
- European Commission Justice. Retrieved January 1, 2010–September 20, 2010 from http://ec.europa.eu/justice/policies/privacy/index_en.htm.
- Federal Trade Commission. Retrieved 28 February 2011 from <http://www.ftc.gov/os/2010/12/101201privacyreport.pdf>.
- HeiTech Padu Berhad. HeiTech Padu Berhad products and services. Retrieved September 1, 2010, from, <http://www.heitech.com.my>; 2010.
- Joint A, Baker E, Eccles E. Computer Law and Security Review 2009;25:270–4.
- Jr R. The formulation of information policy rules through technology. *Texas Law Review* Volume 1998;76:558.
- Kang C. The Washington Post. Microsoft calls for regulations over cloud computing. Retrieved August 1, 2010, from, http://voices.washingtonpost.com/posttech/2010/01/microsoft_calls_for_regulation.html; 2010.
- Lessig L. Code version 2.0. Perseus Books Group; 2006.
- Microsoft. Building confidence in cloud computing. Retrieved January 20 2010, from, <http://www.microsoft.com/presspass/presskits/cloudpolicy/>; 2010.
- Microsoft. Microsoft urges government and industry to work together to build confidence in the cloud. Retrieved 18 March 2011, from, <http://www.microsoft.com/presspass/press/2010/jan10/1%E2%80%9320brookingspr.mspx>; 2011.
- Modernisation of Convention 108: give us your opinion!. Retrieved March 18, 2011 from, http://www.coe.int/t/dghl/standardsetting/dataprotection/Consultation_Modernisation_Convention_108_EN.pdf; 2011.
- Morgenthaler, M., Ulmer, H., Wiedemann, M. Data Protection and Privacy United States vs. EMEA. Retrieved September 20, 2010, from, <http://www.sdn.sap.com/irj/sdn/go/portal/prtroot/docs/library/uuid/001bcd72-7930-2d10-5083-893516af4308?QuickLink=index&overridelayout=true>.
- Office of the Privacy Commissioner of Canada. Retrieved September 23, 2010 from, http://www.priv.gc.ca/information/pub/cc_201003_e.cfm; 2010.
- Privacy International. Retrieved September 20, 2010 from, <http://www.privacyinternational.org/survey/dpmap.jpg>.
- Reed C, Angel J, editors. Computer Law. Oxford: University of Oxford Publication; 2007.
- Reed C. Information rights in the cloud. Retrieved September 1 2010, from, <http://www.box.net/shared/51a7rqa0y7>; 2009.
- Ruiter, J., Warnier, M. (unpublished). Privacy Regulations for Cloud Computing Compliance and Implementation in Theory and Practice. Retrieved September 20, 2010 from <http://www.cpdpcconferences.org/Resources/Ruiter.pdf>.
- Safe Harbor. Retrieved January 1, 2010–September 20, 2010 from, <http://www.export.gov/safeharbor/>.
- Schultz. Globalpost. Retrieved September 1, 2010, from, <http://www.globalpost.com/dispatch/europe/100915/cloud-computing-eu-europe-commerce-digital>; 2010.
- Smith B. The Huffington Post. Retrieved September 15, 2010, from, http://www.huffingtonpost.com/brad-smith/cloud-computing-for-busin_b_429466.html; 2010.
- Strauss J, Rogerson K. Policies for online privacy in the United States and the European Union. *Telematics and Informatics* 2002;19(2):173–92.
- Summer. Computing.co.uk. Retrieved September 1, 2010, from, <http://www.computing.co.uk/computing/news/2267619/bbc-considering-cloud-olympic>; 2010.
- Svantesson D, Clarke R. Privacy and consumer risks in cloud computing. *Computer Law and Security Review* 2010;26:391–7.
- Technology Quarterly. *The Economist*. (2010).
- Vaquero LM, Merino RL, Caceres J, Lindler Maik L. *ACM SIGCOMM. Computer Communication Review* 2009;39(1):50–5.
- Walden I. *Computer Crimes and Digital Investigation*. Oxford: University of Oxford Publication; 2007.
- Zittrain J. Lost in the cloud. *The New York Times*. Retrieved September 23, 2010 from, <http://www.nytimes.com/2009/07/20/opinion/20zittrain.html>; 2009.