available at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Cursing the Cloud (or) Controlling the Cloud?

Noriswadi Ismail [1]

MARA-SPC Scholar, HeiTech Padu Berhad, Malaysia

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

ABSTRACT

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).

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).*

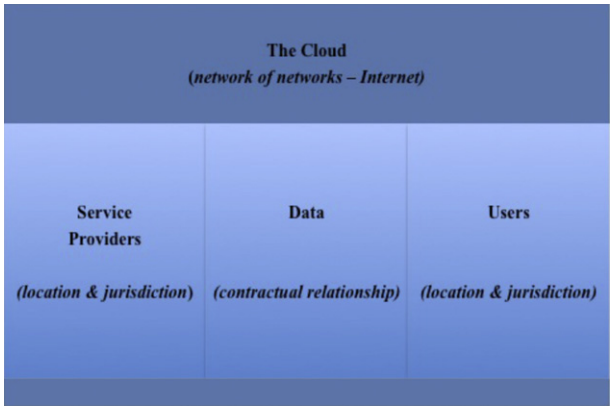

Fig. 1 – The Cloud inter-relationship.

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 hosing 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