COMPUTER LAW & SECURITY REVIEW ■■ (2017) ■■–■■

Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

The problem of binary distinction in cloud computing and the necessity for a different approach: Positions of the European Union and Canada

Pardis Moslemzadeh Tehrani *, *Johan Shamsuddin Bin Hj Sabaruddin*, *Dhiviya A.P. Ramanathan*

Faculty of Law, University of Malaya, Malaysia

Keywords:
Cloud Computing
Controller
Processor
Accountability
Cloud service provider
Allocating responsibility

A B S T R A C T

The development of Cloud Computing is an undisputable fact that is present in this modern era. It is a widely used system, which consists of users from ordinary individuals to multinational companies. However, despite its benefits, there is a problem of accountability in Cloud Computing. Accountability is vital for the allocation of responsibility to ensure the non-existence of threats concerning privacy and security of personal data stored in a Cloud. Both these issues are interconnected because one will not be able to exercise the principle of accountability by omitting the allocation of responsibility. Due to the complexity of the Cloud Computing infrastructure, the line in the distinguishing the role of controller and processor is blurred. This article serves to provide a better understanding of the role of Cloud Computing as well as to configure the need for either a modified or a completely different approach. Furthermore, this article will discuss the different approaches whilst providing a detailed analysis of the roles of the controller and processor. Clear and unambiguous roles and responsibilities will help to reinforce the principle of accountability. This article will compare the positions of Canada and the European Union, because the Canadian approach provides a different outlook since they do not follow the same binary distinction concept in allocating responsibility for controller and processor. This discussion hopes to bring awareness for the discrepancies in the current system and attempts to recommend a possible outcome to curb the problems relevant to this issue.

* *Corresponding author.* Faculty of Law, University of Malaya, Jalan Universiti, 50603 Kuala Lumpur, Wilayah Persekutuan Kuala Lumpur, Malaysia.

E-mail address: pardismoslemzadeh@um.edu.my (P.M. Tehrani)

http://dx.doi.org/10.1016/j.clsr.2017.03.014

Please cite this article in press as: Pardis Moslemzadeh Tehrani, Johan Shamsuddin Bin Hj Sabaruddin, Dhiviya A.P. Ramanathan, The problem of binary distinction in cloud computing and the necessity for a different approach: Positions of the European Union and Canada, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.03.014

1. Introduction

Cloud, also known as a visible mass of condensed water vapour floating in the atmosphere, is typically known for being high above the ground. We often symbolize cloud in mind maps as the top of the chart followed by subsequent details. In such a mind map, the column with the cloud is the largest fact and all that falls below it are merely subsections of what follows the cloud. Cloud Computing is also derived from a similar concept. Cloud Computing is an Internet based system where virtual software provides software, infrastructure, platform devices and other resources and hosting to another customer on a pay as you go basis.[1] Cloud computing allows users to focus less on how to manage the resource and more on their core business processes.[2] To explain, the managing and monitoring aspects of data storage are handled within the cloud computing by the cloud service providers themselves. Cloud Computing reduces costs and has the potential to transform a data center from a capital-intensive set up to a variable priced environment.[3]

Nevertheless, the Cloud Infrastructure is diverse in nature, ranges from lucrative, and mission critical business functions to sensitive information and expressive content. Because of the nature of data that is being dealt with, there is a considerable amount of potential dispute that can arise. One concern is the privacy of the end user. This is of paramount importance because Cloud Computing infrastructure contains sensitive data of the end user, which requires heightened security. One example is where the government wiretaps the personal data in Cloud for surveillance. There are instances where the service provider provides the FBI wholesale access to its network, enabling agents to tap customers' data at will without obtaining permission of the person in charge.[4] This is a clear breach in the general expectation of privacy of the individual who stored their personal data in the cloud services because there is room for illegal wiretapping.[5] Babak Pasdar, current CEO of New York-based Bat Blue, has said that it is alarming how this carrier ended up essentially allowing a third party outside their organization to have unfettered access to their environment.[6] Before the wide-ranging usage of Cloud, if the government wanted access to potentially incriminating evidence from a home computer, the investigator had to obtain a search warrant for each account.[7] Nonetheless, the extensive usage of Cloud makes search and seizure much easier as it only requires a subpoena to be provided.[8] *Smith v Maryland*[9] and *US v Miller*[10] made it challenging to prove breach of privacy under the Fourth Amendment of the US Constitution because they held that the obtaining of information from third party sharing does not give rise to a breach of privacy even though 'the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed'.[11] Hence the data stored in third party servers, such as Cloud, fall under the description stated above. However, it is difficult to perceive as to why such a technicality applies when the sole purpose of storing data in the Cloud, is to use the Cloud as a substitute to storing data on the desktop, and not with the intention to share with a third party. It also should be emphasized that this analysis, which subjects the third party to criticism for breaches of privacy, overlooks the reason that the data user uses the cloud. This will eventually discourage the data users from using the cloud system due to its inability to hold liable the wrongdoer merely because it technically falls under the third party doctrine.

There are many reasons and factors that lead to the privacy concerns related to the easy access to Cloud Computing, the digital interference by the government related to the blurred concept of who bears responsibility and how a Cloud Service provider is able to negate liability through this gap in the law. This article will consist of a three-part discussion, which explains the distinction of the controller and processor and the position of a Cloud Service Provider in detail. Firstly, the discussion will encompass a study of cloud computing in general and how the directive deals with distinguishing the roles of each entity. The second part, on the other hand, will address the position of the Cloud Service Provider both in the directive as well as the new regulation in the European Union. The final part of this article evaluates the Canadian Data Protection Act, which takes a different approach in allocating responsibility compared to the European Union. This article ends with a recommendation that could be drawn from this study.

2. Cloud Computing

The National Institutes of Standards & Technology (NIST),[12] which has formulated a universally adopted definition, describes cloud computing as a platform that allows easy, on-demand network access to resources such as networks, servers,

[1] Erric Griffith, 'What is Cloud Computing?' (PC MAG Asia 2015) <http://sea.pcmag.com/networking-communications-software/2919/feature/what-is-cloud-computing> assessed 18 November 2016.

[2] Ben Kepes, 'Cloudonomics: Economics of Cloud Computing' <https://support.rackspace.com/white-paper/cloudonomics-the-economics-of-cloud-computing/> assessed 18 November 2016.

[3] Ibid.

[4] CHRISTOPHER SOGHOIAN, 'CAUGHT IN THE CLOUD: PRIVACY, ENCRYPTION, AND GOVERNMENT BACKDOORS IN THE WEB 2.0 ERA' [2010] <http://www.jthtl.org/content/articles/V8I2/JTHTLv8i2_Soghoian.PDF> assessed 20 November 2016.

[5] Ibid 388. It is stated by the author that the telecommunication companies often act as a form of oversight for surveillance requests – primarily due to their fear of being sued for assisting with illegal wiretapping.

[6] Babak Pasdar spoke to THREAT LEVEL; source taken from Kevin Poulsen, 'Whistle-Blower: Feds Have a Backdoor Into Wireless Carrier – Congress Reacts' https://www.wired.com/2008/03/whistleblower-f/ accessed 10 February 2017.

[7] CHRISTOPHER SOGHOIAN, 'CAUGHT IN THE CLOUD: PRIVACY, ENCRYPTION, AND GOVERNMENT BACKDOORS IN THE WEB 2.0 ERA' [2010] <http://www.jthtl.org/content/articles/V8I2/JTHTLv8i2_Soghoian.PDF> assessed 20 November 2016, p 386.

[8] Ibid 362.

[9] Smith v. Maryland, 442 U.S. 735 (1979).

[10] United States v. Miller, 307 U.S. 174 (1939).

[11] United States v. Miller, 307 U.S. 174 (1939).

[12] Peter Mell, Timothy Grance, 'The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology' http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf accessed 26 December 2016, p2.

Please cite this article in press as: Pardis Moslemzadeh Tehrani, Johan Shamsuddin Bin Hj Sabaruddin, Dhiviya A.P. Ramanathan, The problem of binary distinction in cloud computing and the necessity for a different approach: Positions of the European Union and Canada, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.03.014