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

ABSTRACT

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
0267-3649/© 2017 Pardis Moslemzadeh Tehrani, Johan Shamsuddin Bin Hj Sabaruddin, Dhiviya AP Ramanathan. Published by Elsevier Ltd. All rights reserved.

Keywords:
Cloud Computing
Controller
Processor
Accountability
Cloud service provider
Allocating responsibility
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 hosting to another customer on a pay as you go basis. Cloud computing allows users to focus less on how to manage the resource and more on their core business processes. 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.

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. 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. 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. 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. Nonetheless, the extensive usage of Cloud makes search and seizure much easier as it only requires a subpoena to be provided. Smith v Maryland and US v Miller 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’. 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), 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,

---

3. Ibid.
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.
8. Ibid 362.
storage, and applications that runs under minimal intervention from the service providers. In simpler terms, it is a storage service that merely requires a valid Internet connection.

Cloud Computing can be distributed into three forms, which are private cloud, public cloud and hybrid cloud. A private cloud is preserved within an organization and used solely for their internal purpose.\footnote{Abhirup Ghosh, Cloud Computing (M. Tech. Seminar Report, Department of Computer Science and Engineering Indian Institute of Technology) https://www.cse.iitb.ac.in/~abhirup09/Docs/cloud_computing_final_report.pdf accessed 28 December 2016.} Usually, such cloud is custom made according to the organization’s wants and needs. A private cloud is best for businesses, which have dynamic or unpredictable computing needs that require them to acquire direct control over their environments.\footnote{Alexa Huth and James Cebula, ‘The Basics of Cloud Computing’ (2011 Carnegie Mellon University) https://www.us-cert.gov/sites/default/files/publications/USCERT-CloudComputingHuthCebula.pdf 28 December 2016.} Such needs may not be fulfilled by a public cloud. Any subscriber with an Internet connection and access to the cloud space can access a public cloud.\footnote{Alexa Huth and James Cebula, ‘The Basics of Cloud Computing’ (2011 Carnegie Mellon University) https://www.us-cert.gov/sites/default/files/publications/USCERT-CloudComputingHuthCebula.pdf 28 December 2016.} This is the type of cloud that is accessed by most people and is governed by standard forms of regulation. A hybrid cloud, on the other hand, arises when an organization that was previously governed using an internal private cloud moves to a public cloud. It is a mixture of two types of cloud. By using a hybrid approach, companies can maintain control of the internally managed private cloud while also relying on the public cloud as needed.\footnote{Samantha Morris, ‘Cloud Types: Private, Public and Hybrid’ http://www.asiga.com/blog/cloud-types-private-public-and-hybrid accessed 28 December 2016.}

There are also three kinds of cloud computing providers namely Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). IaaS providers offer hardware and the bare minimum software for users to develop on e.g. virtual servers, hard disk space.\footnote{Cloud Computing Guidelines (ICT Qatar) http://www.motec.gov.qa/sites/default/files/publications/cloud_computing_ebook.pdf accessed 26 December 2016.} In this kind of Cloud Computing provider, users have broad control over the services offered by this provider and are able to customize it (configure the settings) based on their needs. This is said to be the most basic form of cloud computing provider. A PaaS provider has more control over the cloud computing thus reducing the control that the user has. This is because PaaS providers implement a software layer over the hardware they offer, forcing users to work with the providers’ software layer.\footnote{Ibid 9.} This is said to not be detrimental as having a ready made software layout reduces the technical expertise needed for the user to create their own web application.\footnote{Ibid 15.} Finally, SaaS providers basically offer software for users over the Internet through a web browser. SaaS makes it easier to have the same software on all of your devices at once by accessing it on the cloud.\footnote{Alexa Huth and James Cebula, ‘The Basics of Cloud Computing’ (2011 Carnegie Mellon University) https://www.us-cert.gov/sites/default/files/publications/USCERT-CloudComputingHuthCebula.pdf 28 December 2016.}

In comparison to the other two providers, users of an SaaS provider have the least control over their data.

The above is a brief definition of Cloud Computing and the types of Cloud Computing providers that exist. Cloud Computing is widely used around the globe because of its accessibility and many advantages. Cloud Computing provides a number of advantages which include reduced price, enhanced reliability, improved accessibility as well as the ease of access independent of a specific computer.\footnote{CHRISTOPHER SOGHOIAN, ‘CAUGHT IN THE CLOUD: PRIVACY, ENCRYPTION, AND GOVERNMENT BACK DOORS IN THE WEB 2.0 ERA’ [2010] <http://www.wjtl.org/content/articles/V812/TTHTLv812_Soghoian.PDF> assessed 20 November 2016.} Furthermore, many of the cloud-based services include a built revision control system, which enables a user to immediately access past versions of a document. It is also backed up in short intervals and stored in multiple servers around the world.\footnote{<https://www.google.com/drive/using-drive/> 24 November 2016.} It also increases the lifespan of the computer as the data will not be required to be processed and there will less resulting wear and tear.\footnote{CHRISTOPHER SOGHOIAN, ‘CAUGHT IN THE CLOUD: PRIVACY, ENCRYPTION, AND GOVERNMENT BACK DOORS IN THE WEB 2.0 ERA’ [2010] <http://www.wjtl.org/content/articles/V812/TTHTLv812_Soghoian.PDF> assessed 20.}

Since the Cloud Computing has proved to be beneficial, it is important for it to be governed by a proper system. However, that is not always the case in relation to Cloud Computing. One of the problems is distinguishing the roles an entity plays and allocating the appropriate responsibility. The following section will explain how the directive has distinguished the role of a particular entity in Cloud Computing.

2.1. The binary distinction in Cloud Computing in the Directive 95/46/EC

Before engaging in the study of how the roles of processor and controller are different, it is important to note the benefits of distinguishing these roles. This article will then address how to adopt a more pragmatic approach rather than following this binary distinction. Normally, an individual or an entity will avoid committing itself as a controller. This is because the person that bears the most liability is the controller and not the processor. The Information Commission Office\footnote{The UK’s independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals Information Commissioner’s Office <https://ico.org.uk/for-the-public/> assessed 22 November 2016.} (ICO), which is in charge of all forms of regulation. It also increases the control that the user has. This is because PaaS providers implement a software layer over the hardware they offer, forcing users to work with the providers’ software layer.\footnote{Information Commissioner’s Office, Data Controller and data processor: What the difference is and what governance implication are <https://ico.org.uk/media/1546/data-controllers-and-data-processors-dp-guidance.pdf> assessed 20 November.}

Since the Cloud Computing has proved to be beneficial, it is important for it to be governed by a proper system. However, that is not always the case in relation to Cloud Computing. One of the problems is distinguishing the roles an entity plays and allocating the appropriate responsibility. The following section will explain how the directive has distinguished the role of a particular entity in Cloud Computing.
The ICO encourages the distinction to be clearly set out in the contract rather than having a general wording that distinguishes both the controller and processor and the responsibility they have to bear.\textsuperscript{26} This guidance is in lieu of the new regulation that the EU has enacted. There was a need for enactment of a new regulation because the distinction was indistinct based on the rules followed in the directive. Such unclear lines give room for an organization to avoid liability because of the loophole that exists in the Act. General Data Protection Regulations encourage documentation of any arrangement and responsibility in the contract itself.\textsuperscript{27}

Opinion 1/2010 from the Working Party also records the similar point that having a distinction helps to regulate who is responsible for compliance with data protection and how data subjects can exercise their rights.\textsuperscript{28} It also mentions how such designation helps to apply national law and effectively exercise the supervisory task conferred on DPA. It mentions how it is important to know the precise meaning of the concept and the criteria are sufficiently clear among all Member States that adopted the directive.\textsuperscript{29}

Furthermore, accountability is essential in the regulatory framework that governs Data Protection. The doctrine of accountability is connected with the issue of distinguishing of the role of controller and processor. This is because without the distinction, it will not be possible to determine which entity/person will be accountable for the breach of privacy. There are three main goals for establishing an accountability framework in Cloud Computing. Firstly, individual users fear that their privacy is not respected.\textsuperscript{30} At times, the business client will doubt the security in regards to sensitive data and will be reluctant to be a data controller. Secondly, the international nature of the industry has already confronted businesses with a multitude of legal and regulatory regimes, which are constantly developing further and as a whole. Lastly, all these problems are amplified due to the fact that Cloud Computing is relatively new and is a ‘complex and dynamic business development’.\textsuperscript{31} The application of the doctrine of accountability reduces the fear of privacy abuse. It also further reinforces the importance of distinction, as accountability will cease without proper allocation of responsibility.

Based on the discussion above, it can be noted that distinguishing between the controller and processor is important and in order to discuss the contingency in the distinction one has to look at the meaning of both the controller and processor. Article 2(d) of the Directive\textsuperscript{32} 95/46/EC states that controller ‘is a natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purpose and means of processing of personal data, where the purpose and means of processing are determined by natural or community law or regulations the controller or the specific criteria for his nomination may be designated by national or community law’.\textsuperscript{33} This definition was derived primarily from Convention 108\textsuperscript{34} which aimed to extend the safeguards for anyone’s rights and fundamental freedoms, and in particular the right to privacy, taking into account at that time the increasing flow across frontiers of personal data undergoing automatic processing.\textsuperscript{35} In the convention, a controller was called the controller of file because during the enactment of Convention 108, there were more state objects, which were handed over. However, cloud computing reflects the life cycle of the information which starts from the initiation until the destruction of the particular information.\textsuperscript{36} Such scenarios are wider in comparison to holding the file, which is referred to in Convention 108. Thus a broader notion was taken which stated in Article 2(b) of the directive that ‘any operation or set of operations which is performed upon personal data’. This is method is taken to expand the scope from what was stated in the Convention.

Furthermore, the directive has also introduced the possibility of pluralistic control. As mentioned above, Convention 108 involves a state object, which does not need a pluralistic concept for the holding of the file as is usually done by an individual. There are also a few other differences between the definition of controller and controller of file and an important one being, the introduction of the concept of processor which was omitted in Convention 108 since during the enactment of this convention, there was only minimal processing in comparison to what cloud computing entails.

The Working Party, in their article,\textsuperscript{37} have provided a detailed analysis of the definition which was subdivided into three separate sections which are namely ‘the natural or legal person, public authority, agency or any other body’, ‘which alone or jointly with others’ and ‘determining the purposes and means of processing of personal data’. The most important of all the three elements and that which helps in distinguishing the controller from the processor is the third element. The Working Party’s article (WP169) has placed considerable emphasis on the third element in comparison to the element, which is merely a personal aspect of the definition and the pluralistic nature of the controller. For showing the distinction between the controller and processor, this article will consider in detail the analysis provided in the third element, which is the most crucial element in the WP169 as well as the guidance set by the ICO.\textsuperscript{38}

The first thing that WP169 has delivered in the third element is the notion of who determines. This is pursuant to Convention 108, which explains the controller of file is the one that

\textsuperscript{26} Ibid 16,17.
\textsuperscript{27} General Data Protection Regulation 2016 (EU).
\textsuperscript{29} Ibid.
\textsuperscript{30} Ibid.
\textsuperscript{31} Ibid.
\textsuperscript{32} Ibid.
\textsuperscript{33} European Data Protection Directive 95/46/EC [1998], Article 2(d).
\textsuperscript{34} Convention 108 Protection of Individuals with regard to Automatic Processing of Personal Data. Reference, ETS No. 108.
\textsuperscript{35} Convention 108 Protection of Individuals with regard to Automatic Processing of Personal Data. Reference, ETS No. 108.
\textsuperscript{37} European Data Protection Directive 95/46/EC [1998].
The directive clearly stresses that having the authority to determine is a crucial trait of a controller. For example, during a decision making situation, the one who determines the decision needs to be taken is the controller whereas the others that merely follow and facilitate the decision cannot be regarded of having control over the situation. The ideology of controller in regards to ‘determining’ is grounded in such simple logic. Thus, determining the identity of a controller must be based on factual circumstances that indicate how an entity has chosen to process personal data for its own purpose. A formal criterion that involves the entity to carry out the role of controller will not solely hold the organization as a controller.

The above can be seen in the case of SWIFT, which showed that factual influence is what determines whether the entity is a controller or processor. In this case, the DPA of Belgium found that the SWIFT is in breach of Belgian Law concerning the protection of privacy concerning data processing of personal data. This was the holding despite the fact that the contract stated that SWIFT is a processor. Hence, it can be seen that the factual circumstances of the situation was looked into and formalities are not decisive in determining who is liable as a controller. This factual approach is not only a concept suggested by WP169 but was also established in the directive itself as it states that the controller is the one who ‘determines’ rather than ‘lawfully determines’.

However, deciding who is the party that ‘determines’ can at times require an in-depth and lengthy investigation. In order to ensure predictability, a pragmatic approach is taken with a view to ensure predictability concerning control. This requires an interpretation of the determining body to be clearly identified by reference to those legal and/or factual circumstances from which factual influence can be inferred, unless other elements indicate the contrary.

WP169 also has classified it into three classes, the first being the control stemming from explicit legal competence. This is a situation where the law has clearly appointed the controller or has explained the duties and responsibility that indicates that the party is indeed the controller. Secondly, this is where the control stems from implicit competence. This is the situation where it is not explicitly laid down by law, nor by the direct consequence of explicit legal provision, but still stems from a legal provision. An example of this can be seen in Recital 41 of the Directive, which provides that a telecom operator who assists in the transmission of personal data through their service will not be deemed controller of the personal data. Nevertheless, those offering such service will normally be considered as controller in respect of the processing of the additional personal data necessary for the operation of the service. Thus, the provider telecommunication service can be considered controller only for traffic and billing data and not for any data transmitted.

Lastly is the control that stems from factual influence. This is a scenario where the control is determined by the factual circumstances that occur in a situation. There can be two circumstances, one being the situation that is explicitly elucidated in a cloud contract itself and the other being the necessity to extrapolate based on the factual situation. However, it should be noted that the factual situation prevails over what is stated in the contract. This can be seen in the above-mentioned case involving SWIFT. This category is particularly important since it allows the addressing and allocation of responsibility in those cases of unlawful conduct, where the actual processing activities may even be carried out against the interest and the willingness of the parties. This is the most complex category in comparison to the others that were stated before. The later stages of this article that involve the service provider will look at this category and analyse the factual influence surrounding the issue.

Furthermore, the third element also contains the concept of purpose and means of processing which is significant in distinguishing the controller from the processor. When it comes to assessing the determination of the purposes and the means with a view to attribute the role of data controller, the crucial question is which level of details somebody should share in determining the purpose and means in order to be deemed a controller. A pragmatic approach is needed, to know which entity holds the most discretion.

Means should be construed based on the original proposal of the directive, which includes four elements, namely purposes/objective, personal data, operation and access. This is however not as evident as determining purpose as most of the time the determination of the means is something the data processor will deal with, due to the data processor’s technical expertise. In such circumstances where the data controller expertise is limited, the means that are taken have to be communicated to the controller by the processor. WP169 provided an example where it showed how a processor deciding the means by himself and not informing the controller can make him liable as a controller. If one chooses to decide on a particular action, one has to assume the responsibility. This approach is based on the principle of accountability, which was discussed earlier in this section. By making the person liable and allocating responsibility shows that one is accountable for his own actions. Thus, based on the discussion above, it can be seen that this element is the most important element in deciding whether one is a controller or processor. The determination of purpose is reserved for the controller. The determination of the means on the other hand can be delegated to the processor as far as the technical and organization questions are concerned.

The working party in describing the degree of discretion that a controller must exercise to determine the purpose of the

---

40 Convention 108 Protection of Individuals with regard to Automatic Processing of Personal Data. Reference, ETS No. 108, Article 2.
46 Ibid 9.
processing activity has resorted to a general phase such as the level of the influence and margin of maneuver.\textsuperscript{46} On the other hand, ICO have also provided some guidance on whether one is a controller or a processor. Based on the ICO, to determine whether you are a data controller, you need to ascertain which organization decides:

- To collect the personal data in the first place and the legal basis for doing so; Data controllers and data processors
- Which items of personal data to collect, i.e. the content of the data;
- The purpose or purposes the data are to be used for;
- Which individuals collect data;
- Whether to disclose the data, and if so, to whom;
- Whether subject access and other individuals’ rights apply i.e. the application of exemptions; and
- How long to retain the data or whether to make non-routine amendments to the data.

The guidance is similar to that of WP169 which described how to determine the purpose and means. The only shortcoming in regards to ICO guidance is the fact that it is less detailed in nature in contrast to WP169.

On the other hand, the processor is defined as ‘a natural person or a legal person, public authority, agency or any other body which processes personal data on behalf of the controller’.\textsuperscript{49} The Data Protection Directive provides a non-exhaustive list of what constitutes processing. Thus, “processing” is a very broad term and includes the following: collection, recording, storage, organization, alteration or adaptation, use, disclosure, retrieval, alignment, combination, blocking, erasure, or dissemination or otherwise making data available.\textsuperscript{50} The processor plays an important role in the context of confidentiality and security in processing grounded in Articles 16 and 17.

Article 16 identifies the responsibility of those who are more closely involved in the processing of personal data, either under direct authority of the controller or elsewhere on his behalf.\textsuperscript{51} This concept was first presented in the commission of the proposal, which ultimately led to the concept of the proposal being introduced. The existence of the processor is wholly dependent on the controller. The Data Protection Directive provides six legal grounds for processing. Consequently, processing is lawful in the following instances:

- Where the data subject has granted its unambiguous consent
- To perform a contract in which one of the parties is the data subject
- To enable the controller to comply with a legal obligation
- To protect the vital interests of the data subject
- To perform a task for the public interest or in the exercise of an official authority vested in the controller
- To pursue legitimate interests by the controller or third parties who have become privy to such data, unless the protected interests of the data subject override those of the controller or third parties.\textsuperscript{52}

Based on the working party there are two basic conditions for qualifying as a processor. It has to be a separate legal entity and it has to process personal data on behalf of the controller. This is basically the legal concept of delegation which is contemporaneous in the cloud computing. However, this still licenses a certain level of discretion in deciding how to best satisfy the controller.\textsuperscript{53} Moreover, there are instances, where there are data to be delegated to other sub-contractors. Nevertheless, all of them have to abide by the instruction of the data controller in carrying out the data processing. WP169 opines that it is not necessary for a detailed explanation of processing, but it is necessary for the processor to inform the processing structure. Due to the fact of the complexity of the processing operation, often the margin of maneuver gives attention to distinguishing the role. An example of company XYZ was given by WP169 which involved a sponsor and a trial center of a draft trial who were both regarded as a joint controller.

However, it will be interpreted differently if the sponsor has chosen to determine the purpose, the essential elements, and the means in a trial center and left very little margin to maneuver. Moreover, EU Article 29 Working Party issued the “Working document 01/2014 on Draft Ad hoc contractual clauses ‘EU data processor for non-EU sub-processor. The Working Party decided to propose a new set of contractual clauses dedicated to the international transfers of personal data from an EU data processor (to a non-EU data sub-processor and subsequent sub-processors).\textsuperscript{54} In this Opinion Paper, it was said in regards to sub-processing that the data importer is not permitted to subcontract any of its processing operations performed on behalf of the data controller under the Draft Contractual Clauses without prior written authorization of the data controller or of the data exporter given on behalf and according to the instructions of the data controller. Depending on the provisions of the Framework Contract, the data controller may have decided that its general prior written authorization is sufficient. Otherwise, prior written authorization needs to be given on a case-by-case basis.\textsuperscript{55} This emphasizes the power of the controller and how the processor is merely a follower of the controller’s instruction.
Based on this, one can roughly get an idea of the role of controller and processor, despite the difficulty in differentiating the controller and processor due to the complexity of the cloud computing infrastructure. It should be noted that although the working party has provided a comprehensive account of both roles, it is not directly binding on the national supervisory authority. In reality, the opinion of the working party is highly respected because of the composition of the working party, mainly consisting of national supervisory authority explicitly tasked with contributing to the uniform application of the directive within the European Union.

The problem usually arises because of the enormous role that a processor plays that raises doubt as to whether they still fall under the cluster of processor. ICO has pointed out accurately that the data processor has its own data controller responsibility for personal data, which is not being processed on behalf of its data controller client. Thus, it is important to look at the particulars of the situation in order to conclude whether it is processing on behalf of the controller or for its own accord. One such processor that falls under this category is the cloud service provider in cloud computing because of its unlimited access to personal data. A cloud service provider is often known as a processor; however, ambiguity continues to surround the role of the service provider. The later section will discuss the cloud service provider’s role and its responsibilities.

2.2. Cloud service provider

Before discussing the role of the Cloud Service Provider, it is important to define a cloud service provider and who falls under the cloud service provider cluster. Mitigating the risks associated with using cloud services is a responsibility shared between the organization and the Cloud Service Provider, including their subcontractors. However, organizations are responsible in providing proper protection for their data and ensuring its confidentiality, integrity and availability. The burden is borne by the organization and not the cloud service provider. A cloud provider is a company that offers components of cloud computing, typically Infrastructure as a Service (IaaS), Software as a Service (SaaS) or Platform as a Service (PaaS) to other businesses or individuals. These different types of cloud computing mandate different types of services accordingly.

Each of the services involves different responsibilities. For example, a PAAS provider’s goals are to be able to quickly and efficiently design and deploy applications and make them function reliably. The providers in the IaaS, on the other hand, decide whether an IAAS service is appropriate. Finally, SAAS is where the cloud computing has extended from IaaS into business systems and user programs. The provider of SAAS has a broader scope in comparison to the previous two types of cloud computing. The SAAS has a broader scope which starts from productivity applications and CRM app’s suites to software programs which manage cloud applications and deployments and even enable the creation of hybrid clouds.

Based on the above, it can be seen that cloud service providers are major role players in any type of cloud computing. They are basically in charge of managing and dealing with technicalities involved in cloud computing that frees the data user from worrying about such matters. Having a cloud service provider does not only prove advantageous for a data user, but also for the cloud service providers themselves. The following section will list a few advantages of acting as a cloud service provider.

2.3. Advantages of Cloud Computing to service providers

As mentioned in the first part of the article, Cloud Computing has many advantages. This is the reason for its widespread usage across the globe. However, most people are unaware that Cloud Computing does not only serve the data user but also the service provider. This is because it appears that Cloud Computing advantages are primarily focused on the data users that enjoy the service of cloud computing rather than those providing the service to the data user. Below are a few benefits that the service provider enjoys because of Cloud Computing.

Firstly, the problem of unauthorized copying is close to nonexistent when the software is delivered via the web. This is because much of the computation occurs on the software provider’s own servers that contain a code that even the data user is not provided with. Hence, it almost impossible for illegal data sharing to occur in cloud service in comparison to other servers, which have thousands of users illegally sharing, copies. Furthermore, Cloud Computing provides the ability for the service provider to terminate any services, which they find, are against their principles or terms and conditions. The service provider is able to maintain such control due to the individual account given to each individual, which has a specific username and password. If the company wishes to terminate the services with a particular data user, it can simply do so by suspending their account.

Besides that, cloud services also allow software vendors to easily embed advertisements into their offerings, and to use sophisticated data mining algorithms to display advertisements related to the users’ private data held within the cloud. This advertisement provides them with a lucrative amount of

---

59 Ibid 133.
60 Ibid 134.
61 Ibid 134.
63 Ibid.
64 Ibid 364.
65 Ibid 365.
66 Ibid 365.
profit and the advertisement is directed to the exact type of the customer because the advertisement is displayed according to the user’s personal data, which often reflects one’s interest. Finally, the cloud service provider can ensure that the end users are using the latest up to date version and the service providers have the ability to roll out instant updates by themselves. The ability to do the above-mentioned helps to reduce tech support costs, and assist in protecting the company’s reputation from being damaged by claims of careless workmanship or poor security practices.

Hence, it can be seen that Cloud Computing not only benefits the end user, but also the service providers. Despite the obvious benefits, there are discrepancies involving the role played by the service provider and the responsibility held by this entity. In the following sections, this article will look at the position of cloud service providers in the older EU directive as well and the new EU new regulation to form a conclusion on the role played by cloud service providers.

2.4. Is a cloud service provider a controller or processor based on Directive 95/46/EC?

This section will deal with the complexity that surrounds the issue determining the role of CSP based on the directive. The role of CSPs is unclear because they are involved in both the role of processor and controller. Before embarking on the discussion of the role of the cloud service provider, it is important to know what a cloud service provider is. Cloud service providers, as mentioned above, are companies that offer network service, infrastructure, or business applications. The cloud service is hosted in data centers that can be accessed by companies or individuals using network connectivity.

The cloud service provider in simpler terms is generally an infrastructure that assists an individual company to store and manage data. Based on the cloud-computing model, cloud service providers fall under the role of processor and data users will be regarded as controllers. This is because of the availability of access by the end user and the right to do anything with the personal data. The cloud service provider is only in charged in regards to the role of processing and managing the data and does not have outright privilege to meddle with the personal data.

Nevertheless, despite the benefit that the cloud computing entails, there is a privacy and security issue in regards to personal data. This is often because when you contract to store the data in a cloud, you are putting your sensitive and personal data in another’s hand. There are a number of ways that data privacy and security can be compromised. First, the data stored can be shared with an unauthorized third party. There could also be a corruption of the data stored when the cloud provider tampers with the data, making it not usable and undetectable. There is also a trend of malicious internal users, who can access the data and use it for their own advantage. Furthermore, data can be lost or leaked. Finally, accounts or services can be hijacked due to the fact that the data is not under the client’s control.

However, despite the risks when one contracts with the cloud service provider, this service provider is often immune from legal liability. An example can be seen in the case of America Online, which paid Matt Drudges $3000 a month to write an online gossip column, but when Drudge used the column to accuse Clinton, a federal judge ruled that America Online bore no responsibility for his misconduct. This is a situation of an Internet service provider who shares the similar immunity as the cloud service provider.

There have been a lot of discrepancies surrounding the distinguishing of the controller from the processor. This can be seen in the case of GOOGLE SPAIN SL V. AEPD (THE DPA) & MARIO COSTEJA GONZALEZ, 13.5.2014 (“GOOGLE”), where in this case Google stored some data, which the data user requested to erase. This data was stored temporarily on a server at an unknown location. The question that was referred in this case is whether the activity of Google Search falls within the concept of processing in Article 2(b) of Directive 95/46 and whether the undertaking of managing Google Search is a controller of the personal data contained in the web pages that it indexes? The operation of loading personal data on an Internet page must be considered processing (as the court held in Lindquist). In exploring the Internet automatically, constantly and systematically in search of the information which is published there, the operator of a search engine “collects” such data which it subsequently “retrieves”, “records” and “organizes” within the framework of its indexing programs, “stores” on its servers and, as the case may be, “discloses” and “makes available” to its users in the form of lists of search results, which constitute processing, regardless of the fact that the operator of the search engine also carries out the same operations in respect of other types of information and does not distinguish between the latter and the personal data. Moreover, the search engine operator determines the purposes and means of that activity and thus of the processing of personal data that it carries out within the framework of the activity and is thus a controller. It is said that it will defeat the purpose and objective of Article 2(d) if the web provider is not held liable as a controller.

As can be seen above, this case has considered the objective and purpose of the directive in deciding the role the web provider plays. A controller is the entity or the individual that bears the burden of responsibility in regards to personal data. Thus, the manner in which a cloud service provider negates their obligations is through cloaking themselves as a processor based on the directive, and thus the processor will not be liable for any breach of data protection. Such an approach allows providers to avoid taking responsibility and lawsuits. In terms of service, most providers are silent on the issues of whether

---

67 Ibid 365.
68 Ibid 365.
70 Ibid.
71 Ibid.
72 The case involving Google Spain.
74 Ibid.
they are the controller of the personal data and several companies such as electric hosts, Window Azure, and many more have shifted their responsibility to the user by directly or indirectly stating in the contract that the data uses are the controllers. This is where the problem arises because although it appears that data users have outright privilege in regards to personal data, a cloud service provider themselves may breach data protection and cause a legal suit. Hence, is such an approach just? Can cloud service providers escape liability for failing to fall under either of the roles? A different approach was taken by Queen Mary research paper, which regarded the cloud service provider neither as a processor nor as a controller and rather urged consideration of the factual circumstances of a particular situation. This is consistent with the opinion stated in WP169 although in the opinion paper they have favored the binary distinction concept.

This Queen Mary paper makes one consider whether there is still a need to distinguish between roles in a cloud-computing infrastructure. Would a pragmatic approach assist in curbing the problem due to the rigid rule? It is important to note that the complexity surrounding cloud computing may not be suitable for such a rigid rule. The next sections will discuss how the EU General Data Protection has changed this position and the different approach taken by Canada where they have foregone the binary distinction and have adopted a more practical and factual based allocation of responsibility.

2.5. Position of the cloud service provider in the European Union’s general data protection regulation

General Data Protection Regulation (GDPR) is the outcome of over a four-year discussion, which finally led to the new regulation in the EU’s data protection framework. The GDPR will replace the current Directive and will be directly applicable to all member states without the need for implementation by national legislation. The Regulation will not take effect until 25 May 2018. It is said to contain some onerous obligations, many of which will take time to prepare. The Regulation is hoping to fit the current Cloud Computing Infrastructure and facilitate the growing of this particular area.

GDPR has made numerous changes following the Directive. One of the changes that has been made pertaining to the controller and processor’s position is that, GDPR has introduced some pliability for companies in situations where the purposes for which they process personal data do not or no longer require the identification of individuals. Based on Article 10, the controller will not be obliged to maintain, acquire or process additional information in order to identify the individual.73 Identifying the individual includes obligations concerning access, rectification, erasure, right to be forgotten and many more. The controller is not in a position to identify the individuals, unless the individuals provide information to exercise the rights stated above. However, if an issue arises, the controller bears the burden of proof for demonstrating that it is not in a position to identify the individual concerned.76

Besides that, one of the most crucial and most relevant amendments, in relation to this article is the fact that the processor can no longer hide from liability. In the directive, as mentioned earlier, the controller bears the legal burden of compliance. The GDPR, on the other hand, changes that by expanding the scope of application of EU data protection law requirements, recognizing the role that the processor also plays in protecting personal data.77 Based on the new regulation, the processor must process the personal data in accordance with the principle of data protection by design and data protection by default, inform the controller of a data breach. The processor must also demonstrate compliance with the GDPR by keeping up to date documentation about the processing, and prevent the personal data from being transferred to recipients in countries that do not provide an adequate level of protection.78

The new regulation provides that the processor is liable for any damages that arise from not complying with the responsibilities under the regulation or acting contrary to what the controller has set. The Directive does not specifically address the question of what happens when a processor departs from the controller’s instructions. However, the new regulation specifies that ‘where a processor, in breach of the GDPR, determines the purposes and means of any processing activity (i.e., if the processor makes its own decisions, rather than following the controller’s instructions), that processor is treated as a controller in respect of that processing activity’.79 Hence, an organization acting as a processor should be extremely cautious of this provision. In essence, any time that such an organization processes personal data for its own purposes, rather than the purposes of the controller, that organization becomes a controller, and is subject to the full compliance obligations of a controller in relation to that processing.80 Thus, liability will include the data breach that the processor has committed. This is a fairer approach than placing all the burden on the controller by merely stating that they fail to adequately exert controls over the processor. This setting, although a trouble under EU data protection law, was often successful, as the burden of noncompliance falls solely to the customer as the controller. However, upon the enactment of GDPR, the processors will be directly accountable to those whose data they process. Thus, clearly under the GDPR it will no longer be possible for CSP processors to position themselves as mere processors and evade the reach of the data protection rule.81

Besides that, the processing that is done on behalf of the controller has to provide ‘sufficient guarantees to implement

76 General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679), Article 12(1a).
78 Ibid 12.
79 ARTICLE 28(10).
81 Ibid.
appropriate technical and organizational measure in such a way that meet the expectation set in GDPR. The measure requires Cloud service providers to carry out personalized risk assessment for customers. This will entail a customized protection for different processing scenarios. Thus, upon implementation of GDPR, the processor may have a greater interest in the details of processing and how the platform is deployed and used by the customers.

Moreover, the General Data Protection Regulation has also introduced a record keeping obligation on data processors. This will consist of the details of the various processing activities and the types of data processing. This is to ensure compliance, where the EU data protection law requires processors to ensure that they keep records of their data processing activities. This is required in all those entities, which carry more than 150 employees. This burden is placed on Cloud Service Providers and their liability for the data they insert in the cloud. Such regulation does not exist in the current directives as the cloud service providers were not required to be monitoring the data they process.

The new regulation has also highlighted the principle of accountability by requiring a certain organization to appoint a Data Protection Officer. If required, the processor must allow the DPO to act relatively independently and, amongst other things, provide oversight concerning the risk associated with the processing operation. Some organizations that act as processors are likely to consider this to be a burdensome requirement and an expense. However, one of the biggest advantages of the GDPR source for CSP is that there is an open consent to subcontract and to make addition and replacement which gives room to change. This flexibility is vital for cloud service providers who serve thousands of customers.

In a subcontracting transaction, if the subcontractor has failed to maintain the requirement set in GDPR, the CSP is liable for the breach that occurred. This requirement has absorbed the contractual risk that is present in subcontracting by placing the burden on the original processor who delegates the job. Furthermore, over the long-term, the appointment of a DPO may help to reduce the risk of non-compliance with the GDPR.

Hence, it can be seen that there is a need for extra effort for the Cloud Computing entities. It is expected that the Cloud Service Provider that responds to the needs and wants of their customers will be more likely to amend the contract earlier, which reflects the new law. However, despite the challenges, the new regulation retains the binary distinction. This is not surprising that the Regulation did not do away with the distinction because Opinion 1/2010 has opined that the distinction is still needed and still serves a purpose.

Based on the above discussion of the regulation and the directive, it can be seen that distinguishing between the controller and the processor is fraught with difficulties and often causes a lot of misconstruction. Binary distinction by itself is a system that is flawed, although it carries the benefit of easier detection of the role-played. This is because such dissimilarity will not work in an environment that is complex dealing with millions of customers and tons of subcontracting. This can be distinguished from a normal buyer and seller relationship, which is simple and straightforward. Hence is it necessary to still hold to the concept, which is merely academic and cannot be applied in reality. This article will look at the Canadian Data Protection Act as in Canada they have departed from the binary distinction and have taken a diverse approach in allocating responsibility. This approach will be deliberated in the following section of this article.

3. A brief outlook on the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA)

Upon analyzing the discussion above, it can be construed that the system is fraught with errors and flaws thus allowing room for improvement. The reason for such blunders is that a lot has changed after the enactment of the directive and the directive, does not facilitate and assist the current cloud-computing environment. It is important to acknowledge that there is a need for a reform that matches the development which took place in cloud computing. In order to note the flaws in the system, it is important to study and contrast the position of other countries as analyzing the directive alone will not enable us to comprehend and produce a reasonable solution for the above said discrepancies. In this section, an analysis will be done on the Canadian data protection law and compare the Act with the system that was adopted by the EU. The reason for choosing Canada is their different approach taken in allocating responsibilities.

Before explaining the method in allocating responsibilities, it is important to understand what the Canadian Act does and what it says in relation to personal information. The Canadian Act, which is known as the Personal Information Protection and Electronic Documents Act (PIPEDA), came into full effect on January 1 2004. In 2011, it took effect for federally regulated departments and agencies and all commercial

---

82 Ibid.
86 Ibid.
activity in Canada. The federal Privacy Commissioner, who has the authority to make public statements about violations of the Act and/or refer serious cases to the federal court, administers this Act. Literally, all of the provinces of Canada have their own privacy protection and right to inform legislation. The PIPEDA would not apply if the federal Privacy Commissioner feels that the privacy laws are substantially similar to PIPEDA.

The PIPEDA applies to personal information collected, used or disclosed by organizations engaged in commercial activities, from banks and retail outlets to airlines, communication companies and law firms. In exercising rights under PIPEDA, one can always request the organization to send you your personal information, which they have in their system. The organization must give you the information within a reasonable time and at minimal or no cost. Furthermore, one can always correct one’s record if they found an error or omission of the data of the organization. If the organization refuses to correct its records, you may be required to attach a statement of your disagreement to the file. Moreover, one can file a complaint, if they believe that any business is acting contrary to PIPEDA. One might be able to make a complaint if a particular organization refuses to allow the exercise of the rights mentioned above.

One can also bring the complaint to the Office of the Privacy Commissioner of Canada. Furthermore, if the Privacy Commissioner still has not addressed your concerns, you may under certain circumstances, take your complaint to the Federal Court of Canada. In cases where the Privacy Commissioner supports your position but has not been able to resolve the dispute, the Commissioner may also choose to take your complaint on your behalf. The above-mentioned are some of the ways that enable the exercise of rights under PIPEDA. The Canadian Commission has provided a number of solutions if any problem arises because of personal information. The number of solutions seems to suggest that the Canadian Commission takes the privacy of the personal information very seriously. Hence, it is important to look at how the PIPEDA has been influenced by the Fair Information Practice.

Schedule 1 of PIPEDA sets out 10 principles of Fair Information Practice, which forms the ground rules for the collection, use and disclosure of personal information, as well as providing access to personal information.

These principles give one the control that they have over the personal information that is handled by the private sector. The organization is responsible for the protection and the fair handling of personal information, throughout the organization and in dealings with third parties. Nevertheless, it is important to know the definition of Personal Information. Personal information is defined under Part 1 of the Act as any information about an ‘identifiable individual’, except employee information such as the name, title, business address, or telephone number of an employee of an organization. Similarly, personal information also includes ‘personal health information’, which encompasses any information concerning an individual’s physical and mental health, treatment or care records, tissue or organ donation and incidental information collected in the course of providing health care services.

One of the unique characteristics of PIPEDA is its flexibility. Flexibility can be seen in the form of consent sought by an organization and in the variation of consent required based on the type of personal information. For example, an organization requires express consent when the information is considered sensitive, and an implied consent with information that is less sensitive. This Act allows the case of discretion in requiring consent. This can be seen under principle 3 of Schedule 1 of PIPEDA, which deals with consent, the knowledge and consent of the individual are required for the collection, use of disclosure of personal information ‘except where it is inappropriate.’ It also includes a note, which points out the situation where it will be impractical to seek consent such as in cases that involve legal, medical and security reasons when obtaining consent can defeat the purpose of collecting the information in the first place.

Although, flexibility is ideal in a Cloud Computing environment, which is always evolving, it is important to know that there can be room for abuse in the system. Flexibility, more often than not, opens the gate for abuse. An example of such situation can be seen in a school, which places much, emphasis on strict and regimented rules produces disciplined students, whereas schools which are relaxed and consist of flexible rules produce more notorious students. This is because flexibility has always opened the gateway for abuse of the privilege given. Only a society with a strong and principled mentality will be able to not misuse the flexibility given.

Under PIPEDA, it is important to allocate the appropriate responsibilities to the organization, which has the discretion and freedom in regards to the personal information of the data user. Under article 5(3), the Act limits the PIPEDA applicability by stating that ‘an organization may collect, use or

---

84 Ibid.
86 Ibid.
87 Ibid.
88 Ibid.
89 Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5).
disclose Personal Information only for purposes that a reasonable person would consider appropriate in the circumstances. This provision applies even if the organization could have obtained the consent from the data user. This serves to provide additional security for the privacy rule that may emerge from the flexibility of the act. In allocating the responsibility to the actor, Canadian PIPEDA takes a different approach in comparison to the EU. This is because they do not use the binary distinction like how the EU chooses to approach. It, on the other hand, approaches it based on accountability, which is one of the principles of the 10 commandments on the Fair Information Practice. The Canadian privacy law does not employ the concept of data controller and data processor and simply refers to the collection, use or disclosure of personal information by organizations in the course of commercial activities.

This leads us to the question about what the obligations in PIPEDA are. PIPEDA obliges the companies who are subject to the PIPEDA to employ a privacy officer who is accountable in monitoring the organization’s compliance. The companies will have to determine whether the purpose of the collection of information requires express consent. The information that was obtained must be safeguarded appropriately according to the sensitivity of the information. If any organization is found to have fallen short of the requirement set, the user, how the privilege to exercise the right of the organization, regardless of what role it is playing in Cloud Computing Infrastructure. This appears to be an easier concept from the rigorous job of distinguishing the controller and processor based on the Directive.

In conclusion, the PIPEDA and the directive are very different. There are a number of drawbacks that exist in PIPEDA as a result of its provision of substantial similarity. However, there are no arguments found against the nonexistence of the separation of the roles. Hence, does the binary distinction lose the practicality in modern day Cloud Computing? It can be seen based on the above discussion that the Canadian approach is better.

4. Conclusion

A public consultation was initiated by the Commission following the publication of its 2010 Communication, “A Comprehensive Approach on Personal Data Protection in the European Union,” with a deadline of January 2011. The Commission received a total of 305 responses, which consist of 54 from citizens, 31 from public authorities and 220 from business associations, and non-governmental organizations. The respondents provided opinions on issues identified as critical by the Commission. On improving individuals’ rights, the majority of stakeholders felt that “the current lack of harmonization is detrimental to economic activity within the EU.” This is one of the major reasons for the new enactment of law governing data protection in the EU. However, it is too early to say where the reformation is sufficient and the problem may not arise in the regulation.

Based on the study done above, there seems to be certain flaws despite the fact there is new regulation enacted to solve the discrepancies. This paper makes the following recommendations:

1. Emphasis should be placed on accountability. This is a similar approach to that of the Canadian act, which emphasized the principle of accountability, which is one of the 10 principles of Fair Information Practice. Following the principle of accountability is a much more just solution than determining the responsibility based on the roles.
2. The EU should maintain flexibility in the system. As mentioned above, it is extremely vital that the regulation that governs cloud computing is flexible to accommodate the complexity of the cloud environment and the future growth.
3. The responsibility should be based on the factual circumstances rather than the roles they play. It appears that the EU has placed much emphasis on the role rather than action that is being carried out by the actor. To increase fairness, it is important that a pragmatic approach be taken rather than emphasizing solely on the distinction of the controller and processor.

As mentioned earlier, Cloud Computing is an ever-evolving infrastructure. It is sometimes hard to anticipate the growth that will come in the near future. There is also a large area, which is open for abuse if the responsibility and liability is not allocated accordingly. This is what we note as accountability and how it is important to hold the actor responsible for his own action. Based on the discussion above, one can see the discrepancies involved in the distinguishing and placing of responsibility in the controller and processor. Canada has indeed taken a more preferable method in comparison to the EU directive and it is rather disappointing that the EU has chosen to maintain such distinction in their new regulation.

101 Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5).
104 Ibid.
105 Ibid.
106 Ibid.
Based on the discussion of the article above, it can be seen that the Canadian approach is definitely a much more just and ideal approach compared to the adoption of the binary distinction in the allocation of responsibility. The new regulation, although it includes amendments to reduce the problem of distinguishing the roles, still maintains the binary distinction. It is likely that maintaining such a method will continue to cause problems in regards to distinguishing the roles.

Acknowledgment

The University of Malaya, Grant Number BK034-2016, has supported this work. The author expresses her sincere gratitude to Mr. Manely Stewart for his insightful comments. Without his precious support it would not be possible to conduct this research. The author would also like to especially thank Dr. Saeid Baradran for his support and assistance.