International Journal of Soft Computing 8 (5): 371-376, 2013
ISSN: 1816-9503

Legal Issues of Data Protection in Cloud Computing

[1]Nazura Abdul Manap, [1]Salawati Mat Basir, [1]Safinaz Mohd Hussein,
[2]Pardis Moslemzadeh Tehrani and [2]Abdolhamid Rouhani
[1]Faculty of Law, The National University of Malaysia, 43600 Bangi, Selangor, Malaysia
[2]Faculty of Law, Universiti Kebangsaan Malaysia, 43650 Bangi, Selangor, Malaysia

Abstract: Cloud computing is a major internet-based technology that has transformed the way in which data is stored. Due to its ubiquitous use, countries have enacted various legislations to prevent the abuse of personal data by unauthorized parties. Cloud computing activities involving personal data must be subject to such restrictions and comply with measures imposed by the authorities. This research evaluates the Malaysian Personal Data Protection Act 2010 and the EU Data Protection Directive 1995 in order to establish whether these regulations adequately address issues related to cloud computing. It also explores whether legal issues of cloud computing affect the way personal data is handled and managed. The findings show that while the PDPA 2010 satisfies basic data protection issues in Malaysia, a review of the act is necessary to meet the latest security and privacy protection demands arising from the use of cloud computing technology.

Key words: Cloud computing, data privacy, legal issues, PDPA, EU

INTRODUCTION

Like other technologies, cloud computing has the demand and supply side. Through broadband internet connections, users are able to access cloud services separate from the particular computer possessing the program or the data they want to use. Such data and programs are managed by independent providers. Global access to such technology is through web-mail programs (e.g., Hotmail, Gmail or Yahoo! Mail) that are backed on online computer files, stored on personal videos (e.g., YouTube), provide online applications (e.g., Google Documents and Adobe Photoshop Express) and by those visiting social networking sites (e.g., Facebook and Twitter) (Khan, 2010). This digital-age development has transformed personal data into a commodity that can be traded (Border, 2012). Technological advances enable companies to collect greater quantities of information faster and to use it in a myriad of ways that were unknown before. Google for instance, scans user e-mails to determine which advertisements should be displayed on which sites while amazon retains information on purchases to make future recommendations to users and clients. Although, extremely beneficial to business generation, the free flow of sensitive personal information has its risks in regard to personal privacy and interests. International data privacy laws protect individual privacy interests by controlling how and in what form personal information is employed.

As the use of cloud computing becomes more widespread the demand for greater oversight on privacy matters increases correspondingly. The large amounts of information available on consumer habits and purchases make its extremely attractive for companies seeking to increase their presence or market share to tap into the source via advertisements. In drafting contractual privacy terms, companies have to maintain a judicious balance between protecting the privacy of their customers and succumbing to the temptation to profit from the data available to them (Stylianou, 2010). This makes it incumbent on cloud service providers to subject their privacy terms and conditions to proper evaluation and scrutiny. This study highlights aspects of the cloud environment that are vulnerable to abuse and examines the adequacy of the Malaysian Personal Data Protection Act 2010 (PDPA) and European Data Protection Directive 1995 in regulating and overcoming these issues. The Malaysian legislation could benefit from improved comprehensiveness and include stricter provisions that are provided for in its European counterpart.

THE EUROPEAN UNION APPROACH IN DATA PRIVACY LAW

Whilst sharing common goals and origins, the European Union and US data privacy laws differ in terms of their approach in protecting individual privacy. The EU

Corresponding Author: Nazura Abdul Manap, Faculty of Law, The National University of Malaysia, 43600 Bangi, Selangor, Malaysia

introduced the EU Data Protection Directive (Data Directive) in 1995 which has far-reaching and strict requirements for data collection and transfers. Although, the data directive allows for the unrestricted flow of data among EU countries and removes obstacles created by inconsistent regulatory standards, it also established complete recognition and protection of individual privacy rights through monitoring compliance by an independent body. Such compliance is secured by the imposition of sanctions and penalties for any violation by the European Council.

The data directive has its basis in the Organization for Economic Cooperation and Development (OECD) Privacy Guidelines developed in 1980 which was the first effort by an international body to deal with crossborder flows of personal data. Among other requirements the OECD recommended that data not be transmitted to countries that are not subject to the guidelines (Farina *et al*., 2008) and continues to revise and update them to keep them current.

The data directive is expansive and applies to the processing of personal data by controllers (Dowling, 2008). Personal data is broadly defined to include any information relating to an identified or identifiable natural person (Lanois, 2010). Equally broad is the term processing which includes any operation or set of operations which is performed upon personal data ...", and uploading data into the cloud falls under this term under the data directive. In addition, the data directive applies to both public and private organizations and those that, although not established in the EU, use equipment located there to process personal data (CE, 1995). Finally, the definition of controller includes both private and governmental entities.

The data directive sets forth a number of obligations applicable to data controllers and processors. Whether an entity is considered a controller or a processor depends on the type of cloud computing system used although there are some obligations common to both. Thus, cloud providers have security requirements and must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access (CE, 1995).

For instance, data may only be collected for specified, explicit and legitimate purposes and must be adequate, relevant and not excessive and the controller must inform the data subject of both the controller's identity and why the personal information is being processed which must not deviate from the purpose for which it was sought (Schuffelen, 2010). The data directive also explicitly requires controllers to obtain the data subject's consent unless the information is a listed exception. Exceptions include processing that is necessary to perform a contract involving the data subject or required by a legal obligation or where there is a legitimate interest for doing so. Beyond general personal information, data subjects must be given a specific opportunity demur where sensitive information is at stake (Kuan Hon and Millard, 2012).

Finally, taking into account global implications, one of the most important aspects of the data directive is the requirement that a third party country must have adequate laws to protect personal data information that is transferred. Such protection would include having legislation similar to that in the data directive, providing broad, uniform coverage, a centralized enforcement agency to ensure compliance and allow for judicial remedy (Yen, 2010). The main concern of the European Union is whether the storage of customer data outside its territory would breach the provisions of the data directive and therefore, of the EU member state's national law related to the directive.

However, for cloud providers that house servers outside the European Union there are two practical possibilities provided by the EU directive itself such as Article 26 which allows for the transfer of the subject data to a non-EU country under certain conditions. Such data can be transferred to cloud computing provider with servers outside the European Union if: it has the consent of the consumer (data subject); the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject or the transfer is necessary to protect the vital interests of the data subject.

The EU data protection directive attempts to enable the free movement of data while protecting the privacy of member states and applies to any company processing personal data relevant to the European Union from both the public and private sectors and foreign organisations. It should be noted that under Article 25 (1) of the data directive, any transfer of data to countries outside EU that does not provide an adequate level of protection is prohibited. Cloud computing could violate the EU rules unless particular actions are taken to comply with the data directive. A simple and obvious way to comply with the data directive is to ensure that personal information does not leave the European Union and remains under the cloud computing service established within the EU. There are exceptions toward adequate level of protection.

The first exception is unambiguously given consent. The second exception is the transfer due to contractual obligations. This may occur among the data subject and

the controller or among the controller and a third party in the interest of the data subject. The third exception relates to public interest or vital interest relevant to a data subject. For instance, it would be acceptable to transfer medical data overseas in case of emergencies. The fourth is the special authorization that can be offered by member states if they perceive the transfer comes with sufficient safeguards, even to a region that does not provide adequate levels of protection. When no exemptions apply, it may still be possible to transfer personal information from the European Economic Area (EEA) if the adequacy requirement can be fulfilled such as EU-US Safe Harbour Principles which permits companies in the US to transfer personal data from the EU. Furthermore, as discussed earlier Model Clauses approved by the European Commission, Binding Corporate Rules and authorisation of the member states to transfer the personal data may also fulfill the adequacy requirement and permit to data transfer overseas even to countries that do not have adequate levels of protection.

Of particular importance to multinational companies attempting to circumvent the data directive is how to transfer data between an office or a resident in the EU to a third country which has not been deemed adequate under the directive. Strict EU data privacy laws and the lack of countries on the adequate protection list pose additional obstacles for such companies. Companies and countries who do not meet the EU adequate safeguards standards can overcome this barrier by meeting one of the four options provided for by the EU: consent, standard contractual clause, compulsory corporate rule and safe harbor framework.

The obvious way to comply with the data directive to ensure that personal data does not leave the EU is to have the cloud computing service provided within the union and certain cloud vendors do offer segregated EU clouds to prevent personal data from being transferred outside the European Union. However, such a segregation is not always possible due to the inherent nature of cloud computing. One could envision cloud services obtaining the consent of each individual to permit the transfer of personal data outside of the EU in order to comply with the data directive, although on a large scale such a solution is not practicable.

To enable EU and non-EU personal data transfers while assuring privacy protection and compliance with the data directive, contractual clauses can be invoked. To this end, the European Commission has devised a set of EU-approved standard contract clauses or model contracts which were recently updated to better address the trend toward outsourcing and sub-processing (including cloud computing). A multinational group of corporations may transfer personal data outside of the European Union but within the group, if it can guarantee an adequate level of protection by adopting rules of corporate conduct known as the binding corporate rules. Nevertheless, it should be noted that these alone may not necessarily be sufficient because under the data directive, all parties handling the data need to be subject to the same obligations of confidentiality and security. These issues are not insurmountable but require caution on the part of multinational corporations before they access the facilities afforded by the cloud (Jansen, 2011).

Finally, most types of data processing and transfers between the EU and non-EU countries or companies which do not meet the adequacy requirement can still take place with the valid consent of the subject person.

MALAYSIAN APPROACH IN DATA PRIVACY LAW

Data user's liability: Under the PDPA 2010, there are certain responsibilities incumbent upon the data user in order to protect the data subject's personal data. The duties of the data user are stated in the principles of data protection which are provided in section 6-12 of the PDPA 2010.

According to the General Principle (section 6) of the PDPA 2010, a data user cannot process any personal data unless the data subject has given his consent to the processing of personal data. Also, personal data must be processed fairly and lawfully. Obtaining the consent from the data subject is mentioned in Article 7 of the data directive as one of the data controller's responsibilities. However, such a withdrawal is not unrestricted; withdrawal of consent is predetermined by the law and the data subject has the right to withdraw his consent at any time (Poullet, 2010).

Duty of notification: According to the PDPA 2010, a data user is required to inform data subjects by written notice on the processing of personal data by or on behalf of the data user. It must include the purpose of collecting personal data and whether it is mandatory or voluntary to provide personal data for the data subject.

Duty of notification by the data controller is also prescribed in Article 18 of the data directive. Article 29 of the Data Protection Working Party adopted on July 1, 2012 states that the data subject must be informed as to who processes their data for what purposes and to be able to exercise the rights afforded to them in this respect. Duty to notify a data subject falls under the concept of

transparency and as stated in the Working Party's Opinion on Cloud Computing is of key importance for a fair and legitimate processing of personal data.

Under the Working Party Opinion on Cloud Computing, transparency in the cloud means it is necessary for the cloud client to be made aware of all subcontractors contributing to the provision of the respective cloud service as well as of the locations of all data centres personal data may be processed by Khaw (2002).

Duty of securing personal data: The law requires the requires the data user to secure personal data and take practical steps to safeguard personal data of the data subject from any loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction. Article 17 of data directive, compels the controller to implement appropriate technical and organizational measures in order to protect personal data against accidental or unlawful destruction.

Duty of preservation of data retention: According to section 10 of the PDPA 2010, the processed personal data cannot be kept longer than is necessary. It does not set the time frame permitted to maintain personal data while leaves it to the opinion of the data user. Once there is no longer the requirement of data for the purpose which it was processed, the same should be destroyed or permanently deleted. In addition, according to Article 6 of the data directive, member states shall not keep the personal data longer than is necessary for the purposes for which the data were collected or for which they are further processed (Buttarelli, 2011).

Finally, it is the data controller's duty to ensure that the cloud provider implements secure erasure and that a basic contract exists between the controller and the cloud provider that includes clear terms for the erasure of personal data.

The duty to ensure integrity and reliability: Section 11 of the PDPA 2010 provides that a data user shall take reasonable steps to ensure that the personal data is accurate, complete, not misleading and kept up to date by having regard to the purpose including any directly related purpose for which the personal data was collected and further processed. This principle attempts to prevent undesirable outcomes for data subjects that might arise from incomplete, inaccurate or out of date collecting and processing of personal data by data users. Under the Working Party's Opinion on the Cloud Computing, integrity means the property that data is authentic and has not been maliciously or accidentally altered during processing, storage or transmission.

Similarly, under the PDPA 2010, a data subject is accorded certain rights. These are right of accession to the processing of his personal data; right to correct personal data which the data user's offering a copy of the personal data with respect to the data access request under section 30 and the requestor observes same inaccuracy of personal data; right to withdraw consent which a data subject may withdraw his consent to the processing of personal data by notice in writing and the data user should not continue the processing of personal data; right to prevent processing likely to cause damage or distress which a data subject is entitled by notice in writing to the data user to request at the end of such appropriate period in the situation to discontinue or not to begin the processing of or processing for a specified purpose which is possible to inflict substantial damage or substantial distress to him or another and right to prevent processing for direct marketing which a data subject is entitled by notice in writing to request the data user at the end of such appropriate period in the situations to discontinue or not to begin the processing of his personal data for direct marketing purpose.

Where the data subject is not satisfied with the ability of the data user to comply with the notice whether totally or partly, he may apply to the commissioner who may impose on data user measures to comply with the notice. This also protects the data subject's rights with regard to his personal data when processing personal data in cloud computing technology.

Although, a data subject's rights are protected under the Malaysian legal system the fact that data is not stored on a person's computer could still give rise to personal data protection risks in cloud computing systems. These risks include: unwanted or unauthorised access where the data subject has no control over the security of company data being stored in the cloud; disclosure of personal data; utilising personal data in direct marketing which may make a cloud computing provider breach the right of processing for the purpose of direct marketing due to its nature and personal data stored in cloud computing systems and might be offered to marketers and the problem of ownership which a data subject may faced problems in regaining their full control of the data being abandoned with the termination of their contractual relation with the cloud computing service provider, the cloud provider keeps the data as determined contractually even after expiry of the contract such as social networking sites.

Transborder data flows in cloud computing: Problems may also occur in the transborder flow of data in cloud computing services where cloud providers locate and

operate their services solely or partly using overseas servers. Therefore, different jurisdictions have imposed strict regulations on the transfer and storage of data. The problems that may occur in the transborder flow of data in cloud computing services are jurisdictional issues, data subject's right, storage of personal data, creation of a new data stream.

According to the PDPA 2010, transferring personal data to a place outside Malaysia is prohibited and amounts to an offence unless the country involved is specified by the Minister in the Gazette. In determining countries in the Gazette, the Minister must ensure that there is a similar law enforced in those particular countries or those countries warrant an adequate protection for the data subject's rights and freedoms with regard to the processing, collection, holding or use of personal data. However, in a situation where the data subject has assented to the transfer of the personal data or in case of necessity the above rule would not be applicable.

The factors which must be considered to implement decisions by the Minister are: there is in that place any law which is substantially similar to this act or that serves the same purposes as this Act or that place ensures an adequate level of protection in relation to the processing of personal data which is at least equivalent to the level of protection afforded by this Act. Therefore, the Minister must specify countries that have data protection laws. The list may include all countries in the European Economic Area (EEA), Japan, Hong Kong, Korea, Canada, Australia, Macao, New Zealand and Argentina. In addition, the Minister must investigate whether the laws in those countries are considerably similar to those in the PDPA 2010.

Taken together, under the PDPA 2010, industries, organisations or individuals who are identified as data users transmitting data overseas are obliged to comply with the requirements of the Act. They should also consider the risks inherent in the transborder flow of data in cloud computing. It is also the legal right of data subjects to be aware that their data might be at risk in transborder transactions under cloud computing and that they can as such have the option to terminate the data processing.

COMPARISON BETWEEN MALAYSIA AND EUROPE

The definition of a data controller in the data directive is almost similar to the definition of the data user in the PDPA 2010. Both prescribe obligations on the responsible party as data controllers or data users in processing personal data to comply with data protection legal obligations. Therefore, it is important to classify the parties involved in cloud computing as data user (data controller), data processor or perhaps neither.

Generally, cloud computing providers in Europe and Malaysia are considered as data users or data controllers. Although, there are various views in this respect in the ambit of the European Union, Giovanni Buttarelli, the European Data Protection supervisor, believes that a cloud service provider should be treated as a data user (data controller). Furthermore, under the current data directive a data processor is the person who stores personal data on behalf of the data controller. According to PDPA 2010, social network service providers are specified as a data user (processing, controlling, storing, etc.).

The European data directive's main concern is the protection of personal data and is based extensively on the OECD privacy guidelines. Since, the principle of data privacy has been established by the OECD, countries must comply with this guideline in order to harmonize with modern technological development. As such, all countries could benefit in economic cooperation and other areas by adhering or using these guideline. Countries such as Malaysia should seek to introduce the most rigorous privacy standards to enhance competitiveness and reduce costs of compliance. In this regard, Malaysia would benefit from distinguishing personal data and sensitive data and establish a data protection authority.

CONCLUSION

By the advance of technology, cloud computing the same as other technology brings its own advantages and simultaneously its shortfalls. The PDPA 2010 is the most relevant legislation pertaining to the processing of personal data in Malaysia which also covers the processing of personal data in cloud computing technology. There are some data protection responsibilities of the data user provided in the Act. These responsibilities are provided with respect to the Malaysian legislator's intention to protect the data subject's rights. In conclusion, although the PDPA 2010 generally clarifies the responsibilities of the data user, additional amendments should be introduced with respect to cloud computing in Malaysia. However, the data directive is the most comprehensive data privacy legislation. In order to strengthen the relevant legislation and promote data privacy protection, Malaysia should adopt legislation modeled after that directive. This would allow Malaysia to meet data directive adequacy requirements and data would flow freely between these two jurisdictions which have data-sharing technologies.

Furthermore, Malaysia's adoption of a comprehensive framework would result in a global harmonization of data privacy laws over time which is essential for achieving competing goals.

REFERENCES

Border, A.C., 2012. Untangling the web: An argument for comprehensive data privacy legislation in the United States. Suffolk Trans. Law Rev., 35: 363-631.

Buttarelli, G., 2011. Standards in the cloud. A Transatlantic Mindshare Sophia Antipolis, 28-29 September 2011. http://docbox.etsi.org/workshop/011/201109_CLOUD/01_ToolsAndLegalConcepts/EDPS_BUTTARELLI.pdf.

CE., 1995. Directive 95/46/EC of the European parliament and of the council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official J. Eur. Commun., L281: 31-39.

Dowling, D.C., 2008. Sarbanes-oxley whistleblower hotlines across Europe: Directions through the Maze. J. Int. Law., Vol. 42.

Farina, C.R., S.A. Shapiro and T.M. Susman, 2008. Administrative Law of the European Union: Transparency and Data Protection. ABA Section of Administrative Law and Regulatory Practice, Chicago, III, Pages: 139.

Jansen, W., 2011. Guidelines on security and privacy in public cloud computing. The National Institute of Standard and Technology, U.S Department of Commerce, 800-44 NIST Special Publication. http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf.

Khan, S., 2010. Apps. Gov: Assessing privacy in the cloud computing era. N. C. J. Law Technol., Vol. 11.

Khaw, L.T., 2002. Towards a personal data protection regime in Malaysia. J. Malaysia. Comp. Law, Vol. 29.

Kuan Hon, W. and C. Millard, 2012. Data export cloud computing-How can personal data be transferred outside the EEA? The Cloud of Unknown, Part 4. Queen Mary School of Law Legal Studies Research Paper No. 85.

Lanois, P., 2010. Caught in the clouds: The Web 2.0, cloud computing and privacy. New J. Technol. Intell. Prop., 9: 29-29.

Poullet, Y., 2010. Cloud computing and its implications on data protection. Research Centre on IT and Law (CRID), Namur, Belgium. http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079_reps_IF10_yvespoullet1b.pdf.

Schuffelen, M., 2010. Exploring privacy problems and possible solutions in cloud computing targeted at the consumer. Master's Thesis, University of Tilburg, Netherland.

Stylianou, K., 2010. An evolutionary study of cloud computing services privacy terms. John Marshall J. Comput. Inf. Law, 27: 593-593.

Yen, O.S., 2010. The Malaysia personal data protection act: A brief overview. KKDN: PQ/PP/1505(13829) 1 Legal Taps. http://www.3nityweb.com/aypartners5/download/LegalTAPS-Aug2010.pdf.