VOL. 11, NO. 3, FEBRUARY 2016 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences
©2006-2016 Asian Research Publishing Network (ARPN). All rights reserved.
www.arpnjournals.com

A FRAMEWORK TO ASSESS PRIVACY IN CLOUD BASED SYSTEM

Maher Alghali, M. A. Najwa and I. Roesnita
Faculty of Science and Technology, Universiti Sains Islam Malaysia (USIM), Nilai, Malaysia
E-Mail: maher.alghali@yahoo.com

ABSTRACT

The development of technology and increasing use of the Internet have led organizations to change from the high cost of owning, maintaining and operating computer resources individually to a shared pool of configurable computing resources. These shared pools offer services such as computing and storage by using pay by use models. The services that are operated by service providers have been known as "cloud computing". Even though all the advantages of cloud computing, it is also facing many challenges. Privacy issues are the main challenges facing cloud computing and inhibit the cloud from a wide acceptance in practice. The privacy issues impose a strong obstacle to the adoption of cloud technologies. The literature shows that there is still a gap for efficient ways to increase the privacy of cloud computing. Thus, this paper intends to fill the gap by identifying all possible factors that may affect the privacy of cloud users and develop a conceptual framework explaining these effects.

Keywords: cloud computing, privacy concerns, personal information, cloud based system, conceptual framework.

INTRODUCTION

The modern improvement of cloud computing technology has exposed its ability to remodel the existing technique of information technology by providing new era of how computer resource is worked and purchased. With many benefits, cloud computing present an additional flexible way to use computation and storage resources to meet business needs on demand [1]. Duan, Yan, and Vasilakos (2012) expected the cloud computing will be the platform for the next generation internet. However, even though all the advantages of cloud computing, privacy issues are still main challenges facing cloud computing and inhibit the cloud computing wide acceptance in practice [2, 3]. Cloud computing is a new technology model that is different from other existing models which users have full control over data. Cloud computing uses the virtual computing technology to manage the physical data and machines, which the users only have a limit control over the resource. Thus, it is essential to understand privacy within the perspective of computing based cloud and determine the related privacy concerns in order to better analyze and design cloud-based systems. Most of the previous studies have focused on the cloud development and security rather than taking the cloud privacy into consideration. The literature fails to provide organizations and individuals an adequate approach to identify privacy requirements and select an appropriate CSP based on such requirements. As the model of cloud computing is quite new, many organizations are still keeping away from cloud services since they are not confidence if the CSPs are fit their privacy requirements. In this study, a privacy framework is proposed to fill this gap. This framework will be one step forward to encourage the organizations to take the advantages of cloud computing and give them a deep understanding of all privacy issues in the cloud computing.

Cloud computing

Cloud computing is a phenomenon of last few years on technology field. No other field of IT has generated as much publicity as Cloud computing [4]. Cloud computing attracts significant coverage from the leader of technology companies that offer clouds such as Amazon, Microsoft, and Google. Cloud computing providers (CSPs) generally offer a wide range of computing, storage and software as a service. The ultimate capability is allowing clients to run IT infrastructure in cloud daily. The main scheme of cloud computing is based on an essential principle of "reusability of IT capabilities. Although there has been significant effort to define cloud computing, up till now, there is yet no single, commonly agreed definition of different researchers defined cloud computing in different ways, because, their definition depends generally on fact how the researcher related to concept of clouds. The National Institute of Standards and Technology (NIST) which makes an effort to standardize the definition of cloud computing. NIST definition is accurate in regard of present solutions that leading IT vendors provide [5] "Cloud computing as -a pay-per-use model for enabling available, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, services) that can be rapidly provisioned and released with minimal management effort or service provider interaction".

The difference between cloud computing and other computing models is to expand the horizons across organizational boundaries. However, cloud computing is the combination of already known computing services such as high-performance computing, autonomic computing, distributed computing, and grid computing [6].

©2006-2016 Asian Research Publishing Network (ARPN). All rights reserved.

Privacy in the cloud

There is a significant gap between CSPs and cloud users regarding privacy and transparency in the cloud. CSPs response to the privacy suspicions: "Clouds are more secure than whatever you're using now " [7]. On the other hand many studies and surveys show the privacy is the main reason for slowing to adopt the cloud computing. People often worry and uncertainty about hidden costs related to privacy breaches or lawsuits related to the violation of data of using a cloud computing [8] . Even though the most of the leading companies in the computer world provide cloud computing such as IBM, Google, Amazon, Microsoft, People are still cautious in using cloud computing to upload their high-value or sensitive data [8] . In the past few years, there are many privacy breaches happen, In order to give some real invasions of privacy and keep the size of this paper manageable, in the following some examples of privacy issues in Google.

Privacy policy Google Docs provides users with very limited knowledge of how Google can use user's data and where their data is stored. However, Google uses a vague language which undermines the privacy rights of legitimate users [9]. Moreover, according to Google policy, they may combine the users accounts information with information from other Google services or third parties [10] . However, in 2009 Security vulnerability has been discovered in Google Docs, which revealed documents for users belonging to other users. The vulnerability was fixed during hours, but it showed that users' information could be declared to others [9]. Furthermore, Google declared that 'information that is already available elsewhere on the Internet or in public records' is not to be regarded as private or confidential. Google also has the right to direct advertising to their users based on "information stored on the Services, queries made through the Services or other information' with respect to "other information" indeed contrary to the laws of privacy of various jurisdictions.

On other hand, Google's Privacy Policy changes continuously without notifying their users[9]. Based on Google Transparency Report, in the first half of 2014 and the second half of 2014, Google received 31698 and 30140 requests for disclosure user data, 9,981 requests were from United States. Google provided user data to the US government in 78% of the requests [11] Figure-1 shows the user data requests by reporting period. However, when the City of Los Angeles start to use Google Apps, the city officials requires that the data must be stored in the U.S because the City avoids taking the risk of other countries outside the legal jurisdiction of U.S control its data.

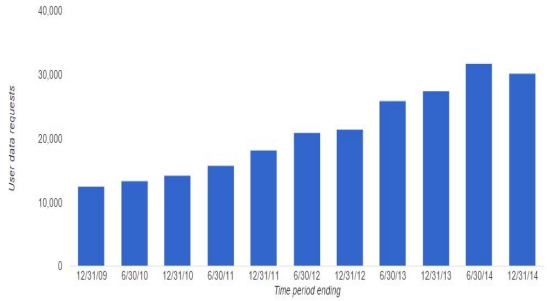

Figure-1. User data requests by reporting period [11].

METHODOLOGY

In order to obtain a convenient base which includes all possible factors that influence to the user privacy, a systematic search was performed to the literature that considers privacy concerns. This research was used privacy issues, privacy concern, privacy challenges of cloud computing as the major keywords for search. The main academic databases were used to extract relevant literature such as IEEE, Science Direct, ACM, Springer, Scopus, and the search engine Google Scholar.

LITERATURE REVIEW

Cloud computing privacy concerns

Pearson (2009) stated that one of the most important feature of the cloud computing is an infrastructure shared between organizations [12]. Therefore, there are issues related to stored and processed data somewhere remotely. Since there is grown in use of virtualization and sharing of resources among organizations, protection users data in the cloud is very essential to guarantee privacy of one user's data from another [13]. Another feature of cloud computing is a dynamic environment, which that allows services to be assembled and dynamically changed by users, and CSP can modify the provisioning of services [14]. Thus, personal and sensitive data could be moved in an organization and/or across organizational boundaries without having the appropriate controls over the data to ensure compliance and protection. Whereby, this privacy risk cloud results in loss of reputation and credibility with CSPs and their user. Mowbray, M. and S. Pearson also highlighted that, several countries rules may limit processing and store of personal or sensitive information on cloud computing that do not adhere to the regulatory requirements[15]. In addition, conflicting issues may also arise because the distributed data in cloud may have different legal location laws that apply at the same time [16]. Another feature of cloud computing is recovery via replication or backup. However, the copies of user data pose privacy risks inherent in storing copies; providing access to the copies, erasure techniques[17] . Furthermore, Data ownership is also one of cloud computing privacy

©2006-2016 Asian Research Publishing Network (ARPN). All rights reserved.

issue. These legal suspicions could make it difficult to verify how and who responsible of ensuring the privacy and confidentiality of users' information in the cloud.

Pearson and Charlesworth [18] (2009) raise the concern "that the speed and flexibility of adjustment to vendor offerings that benefits business and provides a strong motivation for the use of cloud computing might come at the cost of compromise to the safety of data"[18]. However, this compromise gives the impression to affect users' privacy. Another privacy issues for clients of cloud computing exist such as disclosure of personal information. These privacy issues are grown when clients are obliged to give personal information involuntarily, or uncomfortably. Usually in these cases the organizations that are collecting the information will not give a valid reason to the clients for collecting their information [19]. Katzan Jrand Harry 2012 recommend that the integrity and accountability of the organization regard to their information practices is essential to allay concerns of privacy and user confidence building to reduce the risk of privacy cloud [20]. In addition, Chow, R., *et al* (2009) stated that due to the lack of control in the cloud, organizations are only save a lesser amount of sensitive information in the cloud [21]. They have concern related to the abundance of data and cheap data mining tools, indirect data mining performed by the CSP by analyzing transactional and relationship information. The Table-1 shows the finding of the key privacy concerns in cloud computing.

Table-1. Cloud computing privacy concerns.

	Access	Compliance	Storage	Retention	Destruction	Audit and monitoring	Privacy breaches
[9]	√	√	√	√	√		
[15]		√	√	√	√	√	√
[22]	√	√	√	√	√	√	√
[23]	√	√	√	√	√	√	√
[24]	√	√	√	√	√	√	√
[25]	√	√	√			√	
[26]		√	√			√	
[27]	√		√		√		√

Access

The main concern is whether the organization is able to provide their users to access to their personal information and modified if inaccurate. The cloud users have a right to be known with what personal information is being held, and they have a right to make a request to stop processing in certain cases [3].

Compliance

Legal compliance is an important concern for cloud computing. While data security laws and regulations is not similar in various countries around the world, There is no existing privacy standard or comprehensive legal framework organize and manage the rights and boundary of CSPs and cloud service customers [25]. Both CSPs and cloud service customers have to deal with existing regulatory requirements and service level agreements. The cloud users store their personal and sensitive data in the cloud which out of their control. However, CSPs may be compelled to disclose user's data to the government request regarding to national security or to local regulatory. The law is obligatory where the data are retained or where data are transferred. However, there is the possibility user data transferred across international boundaries without having the adequate controls to guarantee compliance and protection of the information. Compliance issues are split among the CLSPs, Internet provider and users. Moreover, the cloud users need to ensure that their private data is protected and stored separately from others and not combined with another user data [26] .

Storage

The physical location of the cloud server brings up additional questions. First the disclosure and out control storage may has negative consequences due the legal and regulation of protection personal information. The privacy risk can be increased because of foreign country surveillance as the data may be transferred to another data centre in another without the knowledge of the organization, which led to possible violation of domestic law of the country where the data is stored. However, Privacy laws in different countries restrict the ability of organizations to transfer some types of data to other countries. Conflicting issues may also arise because; the many locations of stored data have different regulation that is valid at the same time. Second the use of shared infrastructure to commingle the data with other organizations that use the same CSP can lead to many commingling and segregation issues. The stored data are at more risk from malicious behavior than processing in

©2006-2016 Asian Research Publishing Network (ARPN). All rights reserved.

the cloud, because the stored data may retention in the cloud for long period of time and the exposure time for attack is much longer.

Retention

The retention and ownership of the data on the cloud also become more and more questionable. It is essential that organizations should be aware of how long the retention period of the data on the cloud; the retention policy that governs the data, the ownership of the data (organization or the CSP) and how to impose the retention policy. These issues may be rising in some cases, for instance, if CSP stops the services due to conflict of interests or the CSP may make a decision to mortgage the organization data due to overdue of payment or the service could be suspended for non-payment. However, it may be difficult to authoritatively represent or even understand the series of actions to solve these issues. Thus, it is important these concerns should be confirmed early in the contract.

Destruction

Concerns also exist with regard to destroying the data at the end of the service. It is so complicated to destroy all copies of because the difficulty to come across all copies. However, it is not possible to ensure that all copies of the data are completely deleted. The organization could only be unable to access the data, but the data actually are not deleted. The organization should take into account this issue in regulation and make CSPs responsible for any damage. The organization also should enforce the CSP to not keep their data longer than necessary to avoid any potential privacy breaches.

Audit and monitoring

There are several concerns around audit and monitoring in the cloud, these issues involving in how the organizations can monitor the cloud provider, and how to provide necessary controls and procedures to assurance the users their privacy requirements are met. However, audit and monitoring have great value as they enhance a sense of trust of organizations about the CSP effort in ensuring the privacy. The CSP must be transparent about the privacy breaches; governance policy and activity report therefore, organizations are in a better position to make a more suitable decision.

Privacy breaches

In case of any privacy breaches occur, CSP should be responsible of managing these breaches and should provide the organizations with direct notice of any privacy breaches, so that the organization can handle the situation effectively as possible. The organization and CSP should also make clear how the breach can be determined and the steps of notification process of breaches.

Information privacy concerns theoretical background

The researches of information privacy concern are becoming more and more importance of information system researchers. Various approaches to clarify the diversities of privacy concern levels or to explore the influence of privacy concerns on several factors have been discussed in the literature cross multiple disciplines as well as within the new interdisciplinary fields[28] [29].The concept of "information privacy concerns" has become the essential construct within information system researched and has carried out as an alternative to use the concept of information privacy [30]. The privacy concerns has been defined by as the "individual's subjective views of fairness within the context of information privacy" [31]. Milberg (2000) Indicate that information privacy concerns impact on individuals' attitudes, such as preferences and willingness to give the information[32] .However, according to Bélanger (2011) most researches apply one of two framework: Concern For Information Privacy (CFIP [33] or Internet User's Information Privacy Concerns (IUIPC))[29, 31]. Smith *et al*. (1996) conducted the first a serious of studies to measures individuals' concerns about organizational information privacy practices. Their efforts led to developing a new multidimensional scale, which called concern for information privacy (CFIP). CFIP has four dimensions, which are collection of personal information, unauthorized secondary use of personal information, errors in personal information, and improper access to personal information. (CFIP) was later revalidated by Stewart and Segars (2002) which has since accepted as the most generality scales for assess individuals' concerns [34, 35]. A few years later, Malhotra (2004) has expanded the CFIP from offline marketing to the Internet perspective. Malhotra (2004) has been focused on "the individual's' perceptions of fairness/justice the context of information privacy". The scale of Internet Users Information Privacy Concerns IUIPC of Malhotra included three second order factors which are control, awareness, and collection as presented in Figure-2. In addition Malhotra (2004) has declared that IUIPC is more general than CFIP due the additional factor with strong relation to Global Information Privacy Concern (GIPC). Besides that, the IUIPC is more flexible and could easily extend to new types of information privacy because it is based on social contract theory. However Buchanan and Paine (2007) have used IUIPC for specific modern privacy sensitive technologies (e.g., email, e-banking) [36], and Zhang and Wang (2011) used IUIPC to assess the privacy of online social networks (Facebook) privacy [37]. As a reliable instrument, the scale of (IUIPC) has been widely applied in different contexts, ranging from direct marketing to e-commerce and to healthcare. Thus, it is appropriate to identify information privacy concerns of cloud based system by adopt (IUIPC).

©2006-2016 Asian Research Publishing Network (ARPN). All rights reserved.

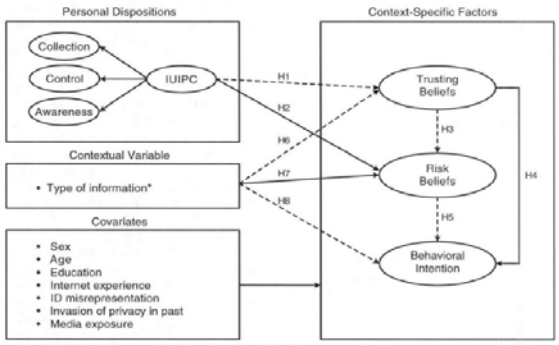

Figure-2. IUIPC, [31].

Data collection

The data collection refers to the concern about the amount of users' data that are being gathered by organizations. The collection of user data should be limited to the minimum amount of data needed for the purpose for which it is collected[23]. Smith et al. 1996 have defined the data collection factor as "the degree to which a person is concerned about the amount of individual-specific data possessed by others relative to the value of benefits received" [33] . The users usually release their data in order to benefits from specific services after evaluating the value and significance of these services. However, users will be unwilling to provide their personal information if they expected useless services. Recently, advertising networks, marketers, and other data profiteers companies depend on the collection of personal data from the online users to advertise their products and services. However, in the cloud computing environment, concerns arise about how to guarantee the collect the minimum amount of data and how to use the data only for an original purpose. It looks logical to expect that collection of personal information will be a significant factor of privacy concerns among cloud users Thus, data collection is assumed important factor of this research which is also a dimension of CFIP and IUIPC.

Control

Control over user data is exceptionally important in the information privacy context and it is often exercised through approval, modification, and opportunity to opt-in or opt-out [31]. Users usually take high risks to submission their data and processing by others. Cloud computing is often suggested as an effective and economical solution that will exchange the client server paradigm. The paradigm shift of cloud computing results in the loss of control over data as well as depends on the CSPs to process the data. Also, cloud user's data could be compromised by CSP with other competitive organizations data which use the same CSP. In cloud computing, users are worried about how, when, why and where their data is processed [38]. The issue of control becomes more apparent when there is a lake of transparency for users what happens with their data in cloud computing. Thus, the control factor is likely to be one of the most important components of privacy concern framework of cloud computing users.

Awareness

Awareness refers to the degree to which user is concerned about the awareness of organizational information privacy practices [31]. According to an online survey among cloud computing users, almost half of the end-users were unaware that they are in fact they are using one or more cloud services [39], while, the overwhelming majority of the participants (more than 90%) agreed that companies need to inform users if they store and process personal information in the cloud. Cloud computing is playing a significant part of IT future, but the privacy risks and the unawareness of users necessitates the push for improving the transparency of the technology. According to Malhotra (2004) awareness is a passive dimension of information privacy. Thus, we believe the awareness factor will be significant affect on user's privacy concerns about organizational practices.

PROPOSED CLOUD PRIVACY FRAMEWORK

The proposed framework is developed based on the research model of IUIPC and based on a broad literature review that has identified the significant effect factors in user privacy as shown in Figure-3. The literature review identifies seven key constructs which are Access compliance, storage, retention, destruction, audit and monitoring, and privacy breaches. This proposed conceptual framework is only one that conceded all those factors in a single framework.

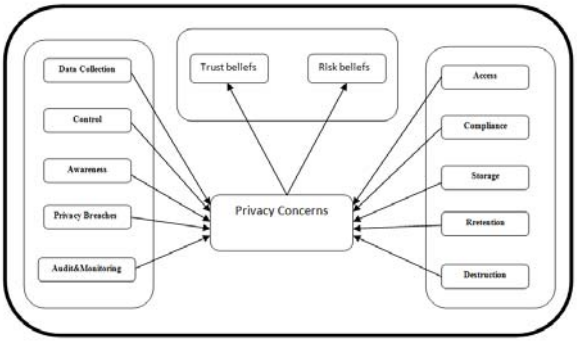

Figure-3. The proposed framework to assess privacy in cloud based system.

CONCLUSIONS

The main objective of this paper is to identify the factors that may influence individual users' privacy. We expect our study to identify potential privacy issues which become more important to cloud users. Furthermore, this study presented a basic conceptual framework that could be beneficial in enhancing the privacy in cloud computing by contributing Influencing factors on privacy. Most of the

©2006-2016 Asian Research Publishing Network (ARPN). All rights reserved.

existing works of literature on this topic considered a limited number of factors. The contribution of this framework is in extracting all potential issues and concerns of privacy related to cloud computing and give more opportunities to improve the privacy for any organization that want to adopt cloud computing. The further study plan is to develop universal cloud based system privacy framework. The first step will be to develop cloud based system privacy concerns instrument based in this framework. The second step will be to determine the influence of the factors on user privacy in cloud-based system. The third step is to test the significant of the various factors and to test the relationships between these factors.

REFERENCES

[1] Mahmoud Al-Shawabkeh, Madihah Mohd Saudi, Najwa Hayaati Mohd Alwi. 2015. Computer Security Factors Effects towards Online Usage of Internet Banking System. ARPN Journal of Engineering and Applied Sciences. 10(2): 532-539.

[2] Chuang I., *et al*. 2011. An effective privacy protection scheme for cloud computing. In: Advanced Communication Technology (ICACT), 13th International Conference on. IEEE.

[3] Maher A., H. Najwa and I. Roesnita. 2014. Towards an Efficient Privacy in Cloud Based E-Learning. International conference on Intelligent Systems, Data Mining and Information Technology (ICIDIT'2014) Bangkok (Thailand).

[4] Ammurathavalli V. and V. Ramesh. 2013. Factors influencing the adoption of cloud computing by small and medium-sized enterprises (SMES).

[5] Mell P. and T. Grance. 2011. The NIST definition of cloud computing.

[6] Gong C., *et al*. 2010. The characteristics of cloud computing. In: Parallel Processing Workshops (ICPPW), 39th International Conference on. IEEE.

[7] Kshetri N. 2013. Privacy and security issues in cloud computing: The role of institutions and institutional evolution. Telecommunications Policy. 37(4): 372-386.

[8] Goodburn M.A. and S. Hill. 2010. The Cloud Transforms Business. Financial Executive. Financial Executive. 26(10): 34.

[9] Svantesson D. and R. Clarke. 2010. Privacy and consumer risks in cloud computing. Computer Law and Security Review. 26(4): 391-397.

[10] Policy G.P. 2015. Google Privacy Policy, Google, Editor.

[11] Google, Transparency Report - Google. 2015.

[12] Pearson S. 2009. Taking account of privacy when designing cloud computing services. In: Proceedings of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing. IEEE Computer Society.

[13] Foster, I., *et al*. Cloud computing and grid computing 360-degree compared. in Grid Computing Environments Workshop, 2008. GCE'08. IEEE.

[14] Alghali M., N.H.M. Alwi and R. Ismail. 2013. Privacy in Cloud Based E-Learning. In: The Second International Conference on Informatics Engineering and Information Science (ICIEIS2013). The Society of Digital Information and Wireless Communication.

[15] Chen D. and H. Zhao. 2012. Data security and privacy protection issues in cloud computing. in Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on. IEEE.

[16] Gellman R. 2012. Privacy in the clouds: risks to privacy and confidentiality from cloud computing. in Proceedings of the World privacy forum.

[17] Nahra K.J. 2008. HIPAA security enforcement is here. IEEE Security and Privacy. 6(6): 70-72.

[18] Pearson S. and A. Charlesworth. 2009. Accountability as a way forward for privacy protection in the cloud, in Cloud computing. Springer. pp. 131-144.

[19] Tweney A. and S. Crane. 2007. Trustguide2: An exploration of privacy preferences in an online world. IOS Press.

[20] Katzan Jr, H. 2011. On the privacy of cloud computing. International Journal of Management and Information Systems (IJMIS). 14(2).

[21] Chow R., *et al*. 2009. Controlling data in the cloud: outsourcing computation without outsourcing control. In: Proceedings of the 2009 ACM workshop on Cloud computing security. ACM.

©2006-2016 Asian Research Publishing Network (ARPN). All rights reserved.

[22] Pearson S. and A. Benameur. 2010. Privacy, security and trust issues arising from cloud computing. in Cloud Computing Technology and Science (CloudCom), 2010 IEEE Second International Conference on. IEEE.

[23] Mather T., S. Kumaraswamy and S. Latif. 2009. Cloud security and privacy: an enterprise perspective on risks and compliance. "O'Reilly Media, Inc.".

[24] Popović K. 2010. Cloud computing security issues and challenges. In: MIPRO, Proceedings of the 33rd international convention. IEEE.

[25] Mouratidis H., *et al*. 2013. A framework to support selection of cloud providers based on security and privacy requirements. Journal of Systems and Software. 86(9): 2276-2293.

[26] Zhou M., *et al*. 2010. Security and privacy in cloud computing: A survey. In: Semantics Knowledge and Grid (SKG), Sixth International Conference on. IEEE.

[27] Senthilkumar S. and M. Viswanatham. 2014. ACAFD: Secure and Scalable Access Control with Assured File Deletion for Outsourced Data in Cloud. Journal of ICT Research and Applications. 8(1): 18-30.

[28] Dinev T. and P. Hart. 2006. An extended privacy calculus model for e-commerce transactions. Information Systems Research. 17(1): 61-80.

[29] Bélanger F. and R.E. Crossler. 2011. Privacy in the digital age: a review of information privacy research in information systems. MIS quarterly. 35(4): 1017-1042.

[30] Xu H., *et al*. 2011. Information privacy concerns: linking individual perceptions with institutional privacy assurances. in Journal of the Association for Information Systems. Citeseer.

[31] Malhotra N.K., S.S. Kim and J. Agarwal. 2004. Internet users' information privacy concerns (IUIPC): the construct, the scale, and a causal model. Information Systems Research. 15(4): 336-355.

[32] Milberg S.J., H.J. Smith and S.J. Burke. 2000. Information privacy: Corporate management and national regulation. Organization science. 11(1): 35-57.

[33] Smith H.J., S.J. Milberg and S.J. Burke. 1996. Information privacy: measuring individuals' concerns about organizational practices. MIS quarterly. pp. 167-196.

[34] Stewart K.A. and A.H. Segars. 2002. An empirical examination of the concern for information privacy instrument. Information Systems Research. 13(1): 36-49.

[35] Smith H.J., T. Dinev and H. Xu. 2011. Information privacy research: an interdisciplinary review. MIS quarterly. 35(4): 989-1016.

[36] Buchanan T., *et al*. 2007. Development of measures of online privacy concern and protection for use on the Internet. Journal of the American Society for Information Science and Technology. 58(2): 157-165.

[37] Zhang N., C. Wang and Y. Xu. 2011. Privacy in online social networks.

[38] Hölbl M. 2011. Cloud Computing Security and Privacy Issues. The Council of European Professional Information Societies (CEPIS).

[39] Quah A.M.Y. and U. Röhm. 2013. User awareness and policy compliance of data privacy in cloud computing. In: Proceedings of the First Australasian Web Conference - Vol. 144. Australian Computer Society, Inc.