Turkish Online Journal of Qualitative Inquiry (TOJQI)

Volume 11, Issue 4, October 2020: 741- 745

Research Article

Protecting The Privacy of Customer's Personal In the Era of Cloud Computing

Abram Yuda Sibuea[1], Lidia Febrika Panjaitan[2], and Iskandar Muda[3]

Abstract

As a result of a shift in the world of technology, cloud computing users has growth from year to year. As a consequence of a major concern of cloud users, privacy and data protection are getting substantial attention in the field. There are still many issues regarding consumer protection in the aspect of personal data protection and standard clauses in privacy policy. Currently, a considerable number of papers have been published with a growing interest in privacy and data protection The aim of this paper is to highlight the results of existing primary studies published in privacy and data protection to identify current trends and open issues. A descriptive approach was adopted in this paper through a collection of previous literature on the privacy and data protection in maintaining the confidentiality of customer personal data.

***Keyword**: privacy, protecting privacy, privacy and data protection*

[1,2,3]Universitas Sumatera Utara

Introduction

In today's digital era, we use numerous platforms for social, marketing and learning purposes. We give permissions to these online platforms to access our personal data. This data may be sensitive or insensitive depending on a particular user. In most cases, users become careless and do not read the terms and conditions of diverse products/goods or advertising mechanisms. One of the biggest issues experienced by cluoud users are personal data protection and standard clauses in contracts that must be agreed by users before using the e-commerce platform. Most consumers did not read the term & condition and privacy policy on the e-commerce platform before accepting the contract

(Bakos et. al, 2013). Nowadays, there are many "free" online platforms which obligate consumers to be willing if their personal data is used by the platform provider for targeted marketing purposes (Yip, 2018).

Indonesia does not have regulation which is addressed specifically for personal data protection only, but Indonesia has laws pertaining to personal data protection (Ang, 2020). Indonesia's law on personal data protection is currently in the drafting phase. However there are some regulations governing personal data in Indonesia. Cloud storage has created new legal problems, namely how personal data from cloud storage users are protected from various kinds of disclosure and distribution by cloud storage service providers to third parties, while in Indonesia itself the ITE (Information and Electronic Transactions) Law has not clearly regulated security protection from private files stored in the cloud storage (Kusumawardhani and Masyithah, 2018).

1. Literature Review

In an analog world, where everybody holds information about others (Petronio 2000), peer-privacy protection appears to work according to "implicit norms about what, why, and to whom information is shared within specific relationships" (Martin, 2016). People implicitly negotiate what information they divulge (Petronio, 2015) and are mostly willing to respect others' privacy. However, with new information and communication technologies, these negotiations are largely absent.

Several researchers have reported that privacy in the definition adopted by the organization for Economic Cooperation and Development (OECD, 2002) is "any information relating to a recognized or identifiable individual (data subject)." In fact, the concept of privacy is vast and has a different perspective depending on countries, cultures, or jurisdictions. To be more precise, privacy is not just about hiding information, but it is a legitimate control over personal data since no one may get personal information without the consent of the owner unless there are laws that allow access to such information (Angin et al, 2010), for example, income information that the tax authorities can get from employers.

2. Research Methodology

A descriptive approach was adopted in this study through a collection of previous literature on the privacy and data protection in maintaining the confidentiality of customer personal data. Based on the literature review described, this study tries to explain how privacy and data protection with the principle of integrity and while maintaining the confidentiality of the personal data of service recipients. The previous literature that was researched to complete this paper was a journal published from 2010 to 2020.

3. Discussion and Result

Current data privacy exercise in mobile cloud computing, the number of investigations is increasing regarding the setup, cryptography, authentication, and accounts creation of data privacy exercise (Alnajrani et al, 2020). Also, for data privacy threats and attacks in mobile cloud computing, the results of this study show the need for research in eavesdropping attacks, internal attacks, improper security policies and practices in some locations, internal multi-layer attacks, inference attacks on user privacy, and data breach threats (Tambunan et al., 2018). In addition, our

exploration shows that there are open research issues in encryption, authentication, security, trust, privacy, architectures, various attacks, energy consumption, and testing.
In the digital world, we use various online applications and services. We give some kind of permission to every web-site or application to get accessto our data. The digital user seems very casual about the security of his personal and sensitive data (Verma et al, 2020). The technology of AI and its subset, machine learning are evolving at a tremendous pace in the field of digital advertisement. The popularity of different social networks and user services is highlighted in this paper. Various protocols in digital advertising are also discussed with some of the existing primary algorithms in digital advertising. Although we believe that future scope is totally concerned about the sole discretion of the individual. But here, the responsibility belongs to each and every individual present in this universe.

Law to protect privacy, while legal protection is a need that can answer this need. The definition of the right to privacy and protection of personal data are two things that are related to each other, which is personal data, which is the property of each individual that needs to be protected and is one part of human rights that is universally recognized, both legal instruments (Haganta, 2020).
The use of location data to control the coronavirus pandemic can be fruitful and might improve the ability of governments and research institutions to combat the threat more quickly. However, the use of such large amounts of data comes at a price for individual freedom and collective autonomy. The risks of the use of such data should ideally be mitigated through dedicated legal frameworks which describe the purpose and objectives of data use, its collection, analysis, storage and sharing, as well as the erasure of 'raw' data once insights have been extracted (Zwitter, 2020). However as shown above, legal frameworks including human rights standards are currently not capable of effectively ensuring data protection, since they focus too much on the individual as the point of departure.

Over the last years much has been written about the balance between security and individual freedom, particularly on the false trade-off between privacy and security (Solove 2011). Furthermore, research over the past years has proven again and again that the combination of the production of unprecedented amounts of data and improving techniques to analyse large data sets are rendering most – if not all – state of the art practices to pseudonymize/anonymize datasets meaningless, at least as time moves on (Rocher et al. 2019). The United Nations Special Rapporteur on the right to privacy has rightfully highlighted the risks resulting from the combination of 'closed' datasets with 'open' ones (Cannataci 2017). In our work on Mobile devices as stigmatizing security sensors we have proposed the concept of 'technological gentrification' which describes our lives in environments that are permanently monitored and where those believing in the benefits of omnipresent data render the choices of others de-facto obsolete (Gstrein and van Eck 2018).

Privacy has always been interdependent. However, an increasing integration of technology in data transfers affects the ease and scale with which interdependent privacy breaches happen and the consequences that they entail (Kamleitner and Mitchell, 2019). Choice implies that customers have the options to decide whether to disclose their information and how their information will be used (Chang et al, 2018). In fact, customers could select the extent to which their information may be shared during the information disclosing process, and they can refuse to disclose the information if they do not want to. Thus, choice essentially positions the decision-making power into the hands of the customers. When customers can decide, thus having control, they are likely to unlink their own decision (i.e., choice) from an organization's information practices.

4. Conclusion

The challenge of personal data protection is growing and necessitates a better understanding of the dynamics that induce the sharing of others' information. The framework highlights the limitations of current regulation, which largely fails to reflect the interdependent and dynamic nature of privacy. Archive security is very important for users when storing and processing data in cloud storage. This is because there are personal files in the cloud storage that must be kept confidential. Cloud storage service providers as holders of important roles in protecting archives users have the obligation to maintain the security and confidentiality of archives in carrying out their services. Archival security refers to policy procedures, processes, and activities to protect information from various types of loss or stolen and leaked by irresponsible people.

Access and notice have rather similar significant effect on one's perceived effectiveness of privacy policy. This means customers value an organization's effort to inform them about its information practices and to allow them to make changes to personal data. When the customers perceive privacy policy as more effective, they will see themselves as having more control toward how their data will be used and thus able to avoid any potential risk associated with the sharing of the data.

Reference

Alnajrani, Hussain Mutlaq; Norman, Azah Anir; Ahmed, Babiker Hussien. (2020) Privacy and data protection in mobile cloud computing: A systematic mapping study. PLoS ONE 15(6).

Ang, Millencia, (2020), Consumer's Data Protection And Standard Clause In Privacy Policy In E-Commerce: A Comparative Analysis On Indonesian And Singaporean Law. The Lawpreneurship Journal, 1,1.

Angin P., Bhargava B., Ranchal R., Singh N., Linderman M., Othmane L. B., & Lilien L et al. (2010). An entity-centric approach for privacy and identity management in cloud computing. In 2010 29th IEEE symposium on reliable distributed systems (pp. 177–183). IEEE.

Bakos, Yannis et. al. (2013). Does Anyone Read the Fine Print? Consumer Attention to Standard-Form Contracts. *Journal of Legal Studies*, 5.

Cannataci J (2017) Report of the special rapporteur on the right to privacy. Office of the High Commissioner for Human Rights, Geneva.

Chang, Y. et al. (2018). The role of privacy policy on consumers' perceived privacy. Government Information Quarterly. https://doi.org/10.1016/j.giq.2018.04.002

Gstrein OJ, van Eck GJR (2018) Mobile devices as stigmatizing security sensors: the GDPR and a future of crowdsourced 'broken windows'. SSRN Scholarly Paper. Social Science Research Network, Rochester.

Haganta, R. (2020). Legal Protection of Personal Data as E-Commerce Consumer Privacy Rights Amid the Covid-19 Pandemic. Lex Scientia Law Review 4(2), 77-90.

Kamleitner, Bernadette; and Mitchell, Vince. (2019). Your Data Is My Data: A Framework for Addressing Interdependent Privacy Infringements. *Journal of Public Policy & Marketing*, 38(4), 433-450.

Kusumawardhani, Dwininda; and Masyithah, Deby Claudia. (2018). Security and Privacy of Cloud Storage as Personal Digital Archive Storage Media. *Record and Library Journal*, 4(2), 167-173.

Martin, Kirsten (2016). Understanding Privacy Online: Development of a Social Contract Approach to Privacy. *Journal of Business Ethics*, 137(3), 551–69.

Organisation for Economic Co-operation and Development. (2002). OECD guidelines on the protection of privacy and transborder flows of personal data. OECD Publishing.

Petronio, Sandra (2000), "The Boundaries of Privacy: Praxis of Everyday Life," in LEA's Communication Series. Balancing the Secrets of Private Disclosures, Sandra Petronio, ed. Mahwah, NJ: Lawrence Erlbaum Associates, 37–49.

Petronio, Sandra (2015), Communication Privacy Management Theory, in The International Encyclopedia of Interpersonal Communication, Bruhn Jensen, ed. New York: John Wiley & Sons, 335–47.

Rocher L, Hendrickx JM, de Montjoye Y-A (2019) Estimating the success of reidentifications in incomplete datasets using generative models. *Nat Commun* 10(1):1–9.

Solove DJ (2011) Nothing to hide: the false tradeoff between privacy and security. SSRN Scholarly Paper. Social Science Research Network, Rochester.

Tambunan, B., Sihombing, H., & Doloksaribu, A., (2018). The effect of security transactions, easy of use, and the risk perception of interest online buying on the e-commerce tokopedia site (Study on Tokopedia. id site users in Medan city). In *IOP Conference Series: Materials Science and Engineering*. Vol. 420, No.1, 012118. IOP Publishing. http://iopscience.iop.org/article/10.1088/1757-899X/420/1/012118/meta

Verma, Rajat; Awasthi, Charu; Mishra, Prashant Kumar. (2020). Privacy & Security Concerns in Digital advertising: A Critique. *International Journal of Advance Science and Technology* 29(10S). 2993-3001.

Yip, Man. (2018). Protecting Consumers' Personal Data in the Digital World: Challenges and Changes. *Research Collection School of Law*, 106&108.

Zwitter, Andrej; and Gstrein, Oskar J. (2020). Big data, privacy and COVID-19 – learning from humanitarian expertise in data protection. *Journal of International Humanitarian Action* 5(4). 45-61.