JIT Mahasarakham University, Thailand
http://jit.it.msu.ac.th

Journal of Applied Informatics and Technology, 3(1), 1-13

Research Article

Privacy Compliance System by Design Platforms: A Case of Privacy Concerns for Thai Teenagers

Saranya Saetang*

Kasetsart University, Thailand

* Corresponding author. saranya.sa@ku.ac.th

Received:
15 November 2020
Revised:
10 January 2021
Accepted:
4 March 2021

Keywords:

Privacy, Privacy Invasion, Design, Privacy Compliance System, Thai Teenagers

Abstract: The concern over privacy is growing, and several attempts have been made to address privacy invasion and suggest privacy ethics in technology design. However, users' privacy is still customized by the technology around them. Teenagers who are technology savvy are often not aware of online privacy as much as adults. Therefore, their privacy was customized by the Internet or technology devices around them especially via their mobile phone. This study aims to present a design guideline for privacy compliance system by reviewing previous design platforms, and identifying the most concerns of privacy invasions for users and how they react to those invasions. From the legal and designer perspectives, the developer should consider privacy principles of system design, namely, notice/awareness, choice/consent, access/participation, security, enforcement/redress and anonymity/pseudonymity. By using open-ended questionnaires which were sent to 42 Thai teenagers, the results show that the most privacy invasion that students concerned is advertising via mobile phone messages. This invasion could cause annoyance and a waste of time and money. The teenagers react to the invasion varied from calling to the wireless service provider to help stopping those advertisements, blocking the intruders and finally, stopping the use of those services or applications. It was also found that teenagers are concerned only for the privacy invasions that interrupt while they were using the Internet applications, but they

have less concern over the collection of their personal information. At the end of this study, some practical implications are suggested as guidelines for a privacy compliance system.

1. Introduction

Nowadays, consumers have more concerns about their privacy rights. These concerns led to many attempts to evaluate and analyze marketing policy relating to consumers' privacy by both legislators and computer professionals (Foxman & Kilcoyne, 1993). However, there are still a lot of cases of privacy invasions, especially for students or teenagers who have less awareness of privacy invasion than adults when they are surfing the Internet via their mobile devices. By this reason, the developer could help users, especially for those teenagers by making a privacy compliance system which is a system that concerns about privacy by design. A software designer and engineer have to keep users 'privacy in mind from the beginning of the design processes.

This study aims to analyze from previous work on privacy design platforms and investigate some privacy invasions by technology that teenagers who are technologically savvy faced off, their privacy concerns and the ways they react to those invasions. As a result, some privacy design guidelines were suggested and privacy dimensions that teenagers had less aware of were investigated.

The paper begins with the literature review on the definitions of privacy which will help identifying the privacy dimensions, privacy invasion, its impact, and some privacy design platforms. Furthermore, by reviewing previous privacy work and conducting an open-ended questionnaire, this study hopes to provide some privacy principle for designing a privacy compliance system and more preliminary report on privacy invasion incidents and the reaction to those incidents. These incidents or concerns could be compared to the privacy design principles. Thus, the dimension that teenagers have or have less concern could be analyzed. Next section, the definitions of privacy, its dimensions and privacy invasion will be described. Then, the method used in this study and results will be explained. Finally, some implications for a guideline of privacy policy and privacy by design will be discussed.

1.1 Privacy

Definition: 'Privacy' stated by Boyle and Greenberg (2005) refers to an Irwin Altman privacy theory which is separated into three genres of 'Control'. These three genres describe 'Privacy' in more cover detail:

- Solitude is controlling over attention and interaction between the self and environment and self and other people. It can be controlled to be apart with someone, and it does not have to be alone.

- Confidentiality is controlling information access and fidelity (accuracy).
- Autonomy is controlling over identity and its expressions such as name, identity, physical appearance and action.

From the definition, control plays a primary role in privacy. If people can control their solitude, confidentiality and autonomy, they will feel that their privacy is not customized. On the other hand, if they cannot control their solitude, confidentiality and autonomy, they will feel that their privacy is invaded. The other definition of privacy is "freedom from unwanted intrusions by others, or the right to be l*et al*one (Foxman & Kilcoyne, 1993)". The latter definition is about rights. Thus, privacy, especially in the Internet world relates to rights over the information and control over the rights.

The Internet User' Information Privacy Concerns (IUIPC): is a theoretical framework on the dimensionality of Internet users' information privacy concerns (Malhotra *et al*., 2004). Apart from the rights and control over the rights to information, this theory introduces three dimensions in order to measure the privacy concerns over information, namely, collection, control, and awareness of privacy practices. It was suggested that a companies' collection of customers 'personal data is perceived to be fair only when the consumer is granted control over their information and they are informed about the use of their information. Thus, the IUIPC is described as the degree to which the Internet users are concerned about the collection of their personal information, their control over those collected information, and their awareness of how the collected information is used (Malhotra *et al*., 2004).

1.2 Privacy Invasion and its Impact

From the definition of privacy mentioned above, privacy invasion can be described as a state when a person lost her/his control over solitude, confidentiality and autonomy or when her/his privacy rights are customized for example, when someone gained access to our personal information (i.e. reading our mail or keep our personal information) without our consent.

Technology somehow provides a new way to invade privacy, for instance, the Closed Circuit Television (CCTV) that records people in everyday life which people may think that it is an intrusion to his/her private affairs. In the age of the computer, where data can be rapidly transferred to anywhere, private information can be compromised in a variety of ways. One example is some personal data was kept when surfing the Internet using cookies. These cookies could be used to keep customers' information and track their behaviors on the Internet normally without customers' awareness (Jegatheesan, 2013). Actually, the cookies could be useful in terms of personalized using the Internet. However, some customers do not want their behaviors to be tracked. Thus, it could be seen that their privacy was customized.

One more example that privacy could be seen as privacy risk is the use of Facebook, the most popular social network site nowadays. The previous work shows that users aware of the privacy options on Facebook, but only 62 percent actually used them. Moreover, 70 percent of users posted their private information, for example, demographic data, such as age, gender, location, and their interests (Jones & Soltren, 2005). These behaviors cause risks of privacy invasion. The examples of privacy threats are an aggregation of personal data, commercial exploitation by third parties, harassment, profile hacking, and identity theft (Debatin *et al*., 2009). Even though Facebook causes risks to individual privacy, it is still popular and is used in everyday life since it is a tool that can create and maintain an interpersonal relationship. Therefore, it can be seen that people could trade-off their acceptable information risk for something that perceived usefulness.

When people who have concerns about privacy perceive that their privacy was invaded, they will do anything to stop the invasion. Some privacy invasion reactions from the previous literature review are:

- People will conceal or deceive their information (Hawk *et al*., 2008).
- People will not share their information online (Tchao *et al*., 2017).
- People will not use the Internet or not be online (opt-out from the Internet) (Gunnarsson & Ekberg, 2003).

These reactions could impede the growth of e-commerce and the technology acceptance from consumers. Therefore, privacy issues should be considered at the outset when designing a system to retain its customers.

1.3 Some Privacy Design Platforms

There is no universal rule to design a system that protects users' privacy. However, some guidelines could help to shape design for privacy compliance applications.

The fair information practice principles of the Federal Trade Commission (FTC) (1998) have been used as a reference by many previous works on privacy design strategies. The FTC is an organization that protects America's consumers from unfair and deception practices in the marketplace through law enforcement. There are five core fair information practice principles which are explained as follows:

- Notice/ Awareness: Customers/ Users should be given notice about their information when it was collected.

In this, the system should educate users to easier understand the privacy policy or how their information will be used for as the fact that most Internet users spread their own personal information and giving their consent via privacy policy without even reading it (Gunnarsson & Ekberg, 2003).

The good communication of privacy policy increases individuals' privacy control perception and decrease privacy risk perception with will cause the opting out from a system or an application (Xu *et al*., 2008).

Text-based privacy policy mostly goes unread by users who may have privacy concerns (Awad, & Krishnan, 2006). Thus, if they find out later that their information was used without their actually aware of, they will opt-out from the system. Therefore, making the privacy policy easily readable or understand is an important point when designing and developing a system.

- Choice/ Consent: Customers/ Users should be given choices to choose how their information will be used, for example, providing opt-in/opt-out options for customers. Moreover, the opt-in option should have some steps for customers to allow to use their information.

Providing clear opt-outs means to allow users to control and refuse for their information being used, stored and transmitted (Jegatheesan, 2013). In case that customers do not want to continue sharing their information with the company. They should find a way to do so. Otherwise, they will feel that their privacy was invaded.

- Access/Participation: Customers/ users should be able to access their information.
- Integrity/ Security: Customers/ users should have appropriate security procedure and access limitation to their information.
- Enforcement/ Redress: Customers/ users should have a mechanism to enforce the privacy policies and a remedy for the violation such as correction of misinformation or compensation for the unfair practices.

Even though the FTC fair information principles are less comprehensive than the European data protection legislation framework (Colesky *et al*., 2016), it should be considered as a basic procedure that developers should keep in mind when designing a system. Apart from legal platforms, next, there are three more interesting work on privacy by design for designers to consider when developing a system which are:

Privacy Compliance Design for Ubiquitous Computing (From the work of Langheinrich (2011))

Additionally, following the fair information practices and the European Directive (which now called General Data Protection Regulation (GDPR) (Skendžić *et al*. (2018))), Marc Langheinrich (2011) presents seven main areas of innovation and system design in ubiquitous computing where computer computing is everywhere as follows:

- Notice: it is related to the FTC mentioned above. Customers/ Users should be given notice about their collected information.
- Choice and Consent: This is also relevant to the FTC mentioned above. To collect users 'data, the process should be consented from the data subject with a choice that they can opt-in or opt-out the process all the time.
- Anonymity and Pseudonymity: Anonymity is a state of being not identifiable with other subjects. Pseudonymity is solving the problem of using the application that requires authentication by assigning a certain identity to a certain real-name individual.
- Proximity and Locality: This principle will use the state of being next in place or nearby distance to activate or sending some data without any complicated authentication protocols. These could be seen in using sensors for collecting and processing data.
- Adequate Security
- Access and Recourse: The data have a limit access requirement depending on a well-defined purpose and could keep data as long as it is necessary for the purpose.

Ten Mistakes about Privacy in System Design (From the work of Hansen (2011))

Furthermore, the interesting work in system design of Marit Hansen (2011) who has years of experience working for the Data protection Authority of Schleswig-Holstein, Germany, suggests ten mistakes about privacy in system design as follows:

- Mistake 1: Storage as Default. In this, some storing data such as temporary files and log files are always neglected when assessing privacy risks because storing data is a precondition of all kinds of system. In some cases, the data are stored without usage and never been removed which harm privacy.
- Mistake 2: Linkability as Default. Link people with their data is easy to be done by using data relationship in the database for users' profile. Therefore, pseudonym could be used to identify the real individual.
- Mistake 3: Real Name as Default. To collect data and create accounts for some application as Facebook, real names of users always collected which it could link to the real person. Therefore, a system designer has to think about pseudonym as a user account as well.

- Mistake 4: Function Creep as Feature. Function Creep is the data processing beyond the original defined purpose.
- Mistake 5: Fuzzy or Incomplete Information as Default. Normally, privacy policy always be a summarized version which not provide the details. In this case, misunderstanding about the privacy policy might happen. Therefore, the privacy policy should be clear, easy to understand and provides complete information for users.
- Mistake 6: "Location Does Not Matter" but it does matter in law. Location information on data processing took place should be recorded for legal reference.
- Mistake 7: No Life Cycle Assessment
- Mistake 8: Changing Assumptions or Surplus Functionality. When there is some add-on functions or requirements, privacy policy might be changed and should be communicated or re-considered. Otherwise, all privacy guarantees may be gone.
- Mistake 9: No Intervenability Foreseen. The system should provide users some opt-out methods or control the rights to access their personal data in case that they want to change those rights in the future.
- Mistake 10: Consent Not Providing a Valid Legal Ground. The consent considered valid if it is in the same format or meet various legal requirements for each country. Thus, developers should use the right consent form for their users.

The Seven Foundational Principles for Privacy by Design (From the work of Cavoukian (2009))

Finally, as mentioned in the introduction section, Ann Cavoukian (2009), who has had experience working as the Information and Privacy Commissioner of Ontario for many years, suggested that privacy compliance system could be based on 7 principles as follows:

- Proactive not reactive, Preventative, not Remedial
- Privacy as the default. It has to be thought of in every system process.
- Privacy Embedded into Design. It has to be set at the outset of the design processes.
- Full functionality - Positive Sum not Zero Sum. Everybody who works with the system has to have their privacy compliance, not only for the owner of the system. Moreover, the goal of protecting an individual's privacy and the goal of the system should be attained simultaneously.

- End-to-end security – The system has to have a life cycle protection.
- Visibility and Transparency. This principle encourages openness of the privacy policy. In turn, the data collection is visible and transparent to all stakeholders.
- Respect for User Privacy

These principles are to ensure that a system should proactively provide privacy as the default for users from the outset of designing a system.

In Materials and Methods part, these privacy platforms, both in legal and system design perspective, will be analyzed to come up with privacy guidelines for developers to design a system.

2. Materials and Methods

This study reviewed literatures in legal platforms and system design perspectives and analyzed them for privacy compliance for system design and guidelines. Moreover, open-ended questions were sent to Thai teenagers in the higher education to collect their opinions on their most concern for privacy invasions and how they react to those invasions. The respondents were 42 students (age 18-20 years old) by convenience sampling from the computer science department of Kasetsart University, Thailand.

3. Results and Discussion

From literatures in legal platforms and system design perspectives, it can be summarized the relation of each privacy principles for privacy compliance system design as in Table 1.

From Table 1, the most privacy principles mentioned from the legal platforms and system design perspectives are relevant to the FTC platform and ‘Anonymity/ Pseudonymity’ qualification. Therefore, to design privacy compliance system should follow these principles, namely, notice/awareness, choice/consent, access/participation, security, and enforcement/redress. Moreover, in the ubiquitous computing world, ‘anonymity/ pseudonymity’ should be also considered as a privacy protection mean for users ; consequently, the link to the real person could not be done easily.

Additionally, the results from the questionnaires were analyzed using content analysis. The summarized results are presented as follows.

Table 1. Relation of the legal platforms and design principles for privacy compliance system

From the FTC	From the work of Langheinrich (2011)	The seven foundational principles Cavoukian (2009)	From the work of Hansen (2011)
- Notice/Awareness	- Notice	- Visibility and Transparency	- Privacy policy should be clear, easy to understand and provides complete information
- Choice/Consent	- Choices/Consent	-	- Provide the opt-out methods to control the access rights to users 'data
- Access/Participation	- Access and Recourse	-	- Stored data or data processing should be used as a well-defined purpose
- Integrity/Security	- Adequate security	- End-to-end security	-
- Enforcement/ Redress	-	-	- Provide the opt-out methods to control the access rights to users 'data
-	- Anonymity/ Pseudonymity	-	- Real name should not be set as a default for user 'account
		* respect to users 'privacy and proactively embedded privacy concerns to the design phrase	* pay attention to legal aspects such as the details of privacy policy, the location where the data processing took place and a valid form of users' consent.

* The highlight part contains the relevant content among platforms

It can be seen that students' privacy is customized through mobile and PC (personal computer) applications such as messaging, Internet and social media (i.e. Facebook). They can be seen in Table 2. With that, the most privacy invasion that students face is advertisements via mobile phone messages (represents 34.48% out of all answers), advertising in applications (represents 25.86% out of all answers), spam mail (represents 18.97% out of all answers), unwanted tagging via Facebook (represents 15.52% out of all answers) and advertisement via phone call (represents 5.17% out of all answers), respectively.

Moreover, it can be noticed that the most privacy invasion for teenagers is the advertising either from messaging, windows popping up or calling that interrupt their use

Table 2: Privacy invasion incidents

No.	Privacy invasion incident	Total (people)	Total in %
1	Advertising messages via mobile phone	20	34.48
Reaction	- Call to their mobile phones' network service provider to help stop those messages - Delete those messages		
2	Advertising in applications and pop-up windows	15	25.86
Reaction	- Use applications with advertisements free version - Do not use those applications with an advertisement - Block pop-up windows in the browser setting		
3	Spam mails	11	18.97
Reaction	- Delete unknown senders' mails - Block unknown senders or report those mails as spam mail		
4	Unwanted tagging via Facebook	9	15.52
Reaction	- Remove the tags - Block those people who tagged them from friends' list		
5	- Advertising via a phone call	3	5.17
Reaction	- Do not receive the unknown phone number		

of the Internet and mobile devices which are irrelevant to their interest and cause annoyance and waste of their time. The work of Zhu and Chang (2016) suggested that customers/users do not want to be targeted for advertising because they do not like having their online behavior tracked. However, if the advertisement is relevant to what they are interested or they perceive the benefits outweigh the risk of privacy invasion, they will still continue using the website or application and have the willingness to be profiled for online personalization (Awad, & Krishnan, 2006).

The students reacted to the privacy invasion varied from asking their mobile network service provider to stop advertisements, blocking the intruders and stopping using the services or applications that may customize their privacy. Thus, they try everything they can to avoid those invasions and annoyance. However, when students reach their limit to control their applications, they will stop using them.

It could also be noted that no one has mentioned about a case of their information was collected (such as in the form of cookies). This implies that they might not be aware of this case unless they find out later. Thus, giving users a notice when collecting their information and choices should be clearly stated.

4. Conclusions

The design of a system should comply with the fair information practice principles of the FTC and system designer's perspectives, namely, notice/awareness, choice/consent, access/participation, integrity/security, enforcement/redress and anonymity/ pseudonymity.

Privacy is about the rights and control over the rights to personal information. According to Internet users' information privacy concerns (IUIPC), there are three dimensions of privacy that people have concerns on, namely, collection, control, and awareness of privacy practices. However, it was found that teenagers' main concern on privacy invasion caused by interrupting incidents such as the advertising either from messaging, windows popping up or calling, but have less concern over their information collection and the usage for marketing purposes of the firms. Therefore, advertisement using interrupt incidents should be used as much as necessary to reduce the annoyance and the firms should consider more on the return benefits of customers/users.

This study has some limitations that the case study is specifically for Thai students in higher education because this work want to survey and gain the preliminary results for further research. This study could be expanded to have more case studies to gain more insight. However, some implications could be useful when design a privacy compliance system.

5. Acknowledgements

This research was supported by Kasetsart University, Thailand.

6. References

Awad, N.F. and Krishnan, M.S. (2006). The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS Quarterly, 30*(1), 13-28.

Boyle, M., and Greenberg, S. (2005). The language of privacy: Learning from video media space analysis and design. *Journal ACM Transactions on Computer-Human Interaction, 12*(2), DOI= http://doi.acm.org/10.1145/1067860.1067868, pp.328-370.

Cavoukian, A. (2009). *Privacy by design: The 7 foundational principles*. Information and Privacy Commissioner of Ontario, Canada.

Colesky, M., Hoepman, J.H. and Hillen, C. (2016). A critical analysis of privacy design strategies. *IEEE Security and Privacy Workshops (SPW)*.

Debatin, B., Lovejoy, J.P., Horn, A. and Hughes, B.N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication, 15*: 83–108.

Foxman, E.R. and Kilcoyne, P. (1993). Information technology, marketing practice, and consumer privacy: ethical issues. *Journal of public policy and Marketing, 12*(1): 106-119.

Gunnarsson, A. and Ekberg, S. (2003). *Invasion of privacy, spam one result of bad privacy protection*. Master thesis, Blekinge Institute of Technology, Sweden.

Hansen, M. (2011). Top 10 Mistakes in System Design from a Privacy Perspective and Privacy Protection Goals. *7th PrimeLife International Summer School (PRIMELIFE)*. Sep 2011, Trento, Italy: 14-31.

Hawk, S.T., Hale, W.W., Raaijmakers, Q.A.W. and Meeus, W. (2008). Adolescents' perceptions of privacy invasion in reaction to parental solicitation and control. *The Journal of Early Adolescence, 28*: 583– 608.

Jegatheesan, S. (2013). Cookies – Invading our privacy for marketing, advertising and security issues. *International Journal of Scientific and Engineering Research, 4*(5): 3.

Jones, H. and Soltren, J.H. (2005). *Facebook: Threats to privacy*. Available from: http://www-swiss.ai.mit.edu/6805/student-papers/fall05-papers/facebook.pdf. [May 30, 2020].

Langheinrich, M. (2011). Privacy by design – principles of privacy-aware ubiquitous systems. In G.D. Abowd, B. Brumitt, and S. Shafer, editors. *Ubicomp 2001 Proceedings, volume 2201 of Lecture Notes in Computer Science*, 273–291.

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

Skendžić, A., Kovaèić, B. and Tijan, E. (2018). General data protection regulation—Protection of personal data in an organization. *Proc. 41st Int. Convent. Inf. Commun. Technol. Electron. Microelectron*. (MIPRO): 1370-1375.

Tchao, E.T., Diawuo, K., Aggor, C.S. and Kotey, S.D. (2017). Ghanaian Consumers Online Privacy Concerns: Causes and its Effects on E-Commerce Adoption. *International Journal of Advanced Computer Science and Applications, 8*(11): 157-163.

The Federal Trade Commission. (1998). *Privacy online: a report to congress*. Retrieved May 30, 2020, from https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf.

Xu, X., Dinev, T., Smith, H.J. and Hart, P. (2008). Examining the Formation of Individual's Privacy Concerns: Toward an integrative view. *in International Conference on Information Systems, Paris, France*. Available from: https://faculty.ist.psu.edu/xu/papers/conference/icis08a.pdf. [April 1, 2020].

Zhu, Y.Q., and Chang, J.H. (2016). The key role of relevance in personalized advertisement: Examining its impact on perceptions of privacy invasion, self-awareness, and continuous use intentions. *Computers in Human Behavior,* 65: 442–447.