Proceedings of the Eleventh International Symposium on
Human Aspects of Information Security & Assurance (HAISA 2017)

Privacy Enhancing Tools: A Literature Review on End-User Role and Evaluation

A. Padyab and A. Ståhlbröst

Information Systems, Luleå University of Technology, Sweden
e-mail: {ali.padyab;anna.stahlbrost}@ltu.se

Abstract

Trends show that privacy concerns are rising, but end users are not armed with enough mechanisms to protect themselves. Privacy enhancing technologies (PETs) or more specifically, tools (PET-tools) are one of the mechanisms that could help users in this sense. These tools, however, reportedly have low adoption rates, and users tend to be reluctant to integrate them into their daily use of the Internet. Detailed scrutiny of current research on PET-tools, however, can guide future research to help overcome low adoption of these tools. We conducted a literature review on PET-tools to enumerate the types of tools available and how they are being evaluated, in order to shed more light on the missing elements in their evaluations. We reviewed and coded 72 articles in the PET-tool literature. Our results highlight two important issues: 1. Evaluation of most tools is performed using only artificial, summative and ex-post strategies; 2. While usability evaluation is quite common, evaluation of enhanced privacy is lacking. This research hopes to contribute to better PET-tool development, and encourage the inclusion of users in the evaluation and design process.

Keywords

Privacy Enhancing Technology, Tool, Privacy, Evaluation, End User

1. Introduction

Personal information is an integral part of technologies such as mobile devices and online social networks, which are especially susceptible to disclosing personal information (Padyab et al., 2016). A literature review on information privacy by Bélanger & Crossler (2011) revealed several relevant topics related to the field. One of these was *information privacy tools and technologies*, dealing with tools or technological solutions designed for protecting information privacy. These technologies facilitate the digital management and communication of personal information by different means, such as identity masking, traffic encryption, and web-based advertisement management (Goldberg, 2003).

Due to the lack of a generally agreed-upon definition for Privacy Enhancing Technology tools (PET-tools), we have defined them in the way that best captures our focus in this study: PET-tools are tools that form a subset of privacy enhancing technologies, and can be freely chosen by users to protect their privacy on their own private devices. Such tools have distinct user interfaces that require end-user interaction, and therefore could be regarded as standalone applications. The sole

promise of these tools is to enhance end-user privacy, however they can also take the form of add-ons (or plugins) to another system, for example the apps for enhancing Facebook privacy settings.

As individuals' privacy concerns increase, online privacy tools have attracted more attention. Only a minority of Internet users employ PET-tools, however, and most users disclose their personal information without any technological assistance to help them raise their awareness or make informed decisions (Kolter, 2010). Privacy-related technologies face several challenges that cannot be viewed purely through a software design lens, such as social awareness. Usability issues are another hindrance to the acceptance of such tools, since they may not be understandable to the general user (Habibipour et al., 2017). Since Cranor (1999) first called for the development of tools for successful online privacy initiatives, this call has largely been answered by computer scientists at the conceptual (proof of concept) level, as opposed to (Information Systems) IS researchers, who might enhance the understanding of factors influencing the use of technology by individuals, and formulate behavioral questions to be explored with respect to effectiveness and consequences of use (Bélanger and Crossler, 2011). Laudon (1996) argues that a large part of the crisis around privacy is due to the lack of tools on the market, while recent research shows that "Designers often forget to consider how they would measure the effectiveness of privacy protection tools, and that is something IS researchers should seek to answer" (Bélanger and Crossler, 2011, p. 1022).

The purpose of this paper is therefore to investigate user interaction with PET-tools, and suggest approaches and methods for their evaluation accordingly. To the best of our knowledge, no rigorous research has been carried out to spell out the nuances of user interaction with PET-tools. With this paper we seek to study privacy literature, asking first: *what types of user-interactive PET-tools are available, and how are they being evaluated?* By looking at the evaluation dimension, we hope to understand *how privacy is evaluated during the design process.* To explore our research questions and contribute new insights in this field to the privacy research community, we conducted a literature review. Our attempt will ultimately help make PET-tool designers aware of different evaluation metrics that could contribute to more helpful tool evaluations.

In section 2, we discuss user evaluation methods and privacy, while section 3 covers our approach to finding relevant literature, and our analysis process. Our findings as well as discussions are presented in section 4, followed by conclusion in section 5.

2. Background

There are various definitions of privacy, but referring to a classic one could help illustrate our intentions in this paper. Westin defines privacy as "people's ability to control the terms under which their personal information is acquired and used" (Westin, 1967, p. 13). Because of this, it is imperative that PET-tools comply with individual privacy preferences, and our assertion is that any PET-tool should feature

user-centered design. In this section, we want to give an overview of current practices in user technology evaluation.

Evaluation is a process intended to investigate the significance, value, or quality of something, based on a careful study of both its positive and negative features. In planning the evaluation process, it is important to determine when the evaluation will be carried out, and for what purpose. Formative evaluations are performed with the intention of changing or improving something, such as the design of a system (Pries-Heje et al., 2008). A summative evaluation, on the other hand, is carried out in order to determine the impact of the program or application being evaluated (ibid). Another option is to carry out the evaluation ex-ante (meaning before the technology is chosen and acquired or implemented), or ex-post (meaning after it is acquired or implemented) (ibid). The potential user can be involved in these approaches to evaluation, but the approaches as such are rather general in character, and as a result do not provide further guidance as to designing and carrying out user evaluations, or as to what their focus should be.

The aim of this paper is to shed light on how PET-tools should be evaluated, so we have broadened our scope to include the areas of interaction design and user evaluations. Here, evaluations of new technologies often focus on assessing usability qualities, such as learnability, satisfaction, memorability, errors, and efficiency (Preece et al., 2015).

Looking more specifically at PET-tools, most of these tools are complex to configure and operate for end-users, and as a result do not meet users' needs adequately. Currently, there is no strong consensus on how these kinds of user interfaces for awareness should be built (Iachello and Hong, 2007). This results in an absence of guidelines for testing and evaluating these types of tools. Because of this, it is important to establish appropriate metrics for user understanding and ability to express consent, and to try to consistently improve them over time.

3. Methodology

A comprehensive literature search followed the literature review methodology proposed by Okoli & Schabram (2010) was conducted, spanning using information systems, privacy, security, and human-computer interaction journals, as well as conference proceedings that available in IEEE and ACM databases. The following search terms were used: privacy; privacy enhancing tool + evaluation/assessment; privacy + evaluation; and privacy + tool + evaluation/assessment. If the advanced search engine permitted, we included a requirement for the term "evaluation" to appear in either the article title or abstract. The maximum amount of returned hits for each outlet was considered for inclusion. We also restricted results to articles written in English that were published from 2004 to 2016.

We carefully reviewed the abstract and conclusion sections of 2,087 articles (i.e. articles that deal with privacy enhancing (or related) tools designed for users and have performed evaluation). Our main criterion for inclusion was articles that deal

with privacy enhancing (or related) tools designed for users and have performed evaluation. After practical screening, 72 articles were selected for final review.

We used an evaluation framework (Venable et al., 2012, 2014) to examine the designed artifacts. Their framework guides researchers to find a suitable strategy to evaluate outcome. As suggested by Venable et al. (2012, 2014), we can gain a significant insight on type of methodology employed based on time (ex ante versus ex post), the setting of evaluation (naturalistic versus artificial) and functional purposes of the evaluation (formative versus summative) being considered. NVivo 10 was used as an assistance tool to analyze the literature. NVivo makes this process more automated to give text meanings in the form of nodes or concepts and classify the papers based on different classifiers.

4. Result and Discussion

The review led to several important findings about these tools and their user adoption. We will explore these findings in more detail in subsequent sections of this paper. The related literature associated with each finding is available in more detail in the supplementary document provided in the methodology section.

4.1. Types of tools

We observed that the types of tools in the papers we reviewed could be categorized based on three constructs: platform, type of private information addressed, and privacy enhancing approach.

4.1.1. PET-tools for different platforms

PET-tool scholars have shown an interest in protecting user privacy within a variety of technologies and platforms, with a particular focus on those systems with a high potential for private information leaks. One rich source of personal information that may be prone to leaks are online social networks (OSNs), and Facebook in particular. For example, Egelman et al., (2011) found that current control mechanisms for limiting access to personal information across different groups are insufficient in Facebook, and that the network's privacy modification settings are unsatisfactory. The researchers offered a solution giving users the ability to see a Venn diagram illustrating overlapping networks of user groups in order to make decisions about granting access to information.

4.1.2. Privacy enhancing approach

Each tool attempts to enhance user privacy using different means, whether it be a single approach, or a combination of different approaches. The approaches are deepened within user privacy concerns. Our analysis shows that the approaches can be divided into 3 different categories.

Information about risks: The tools in this category make users aware of potential privacy breaches. In that sense, the tools give users a deeper understanding with respect to one or more dimensions of privacy and their implications, thus raising awareness. These might also indicate that how, what, when, from, who, where, why, and which information could infringe on user privacy. For example, Andersen et al., (2006) designed a prototype mobile application that gave users information on their contacts, such as activity, status, relation, and vicinity. As a result, they discovered that in order to preserve privacy, users needed to be given a set of mechanisms to limit their exposure to their contacts based on individual privacy preferences. ProtectMyPrivacy (Agarwal and Hall, 2013) uses a crowdsourcing approach to build a recommendation engine for iOS apps that allows apps to be rated based on different privacy breaches. New users of iOS apps get information on recommended protection settings for each particular app. A similar approach has been used by J. Lin et al., (2012) for Android apps.

Offering to hide detail: In this approach, users are offered the option to hide their personal data based on their preferences on a dimension of privacy. Some Internet services require access to personal user data, and some PET-tools are designed to limit this access by either denying or using dummy data. Here, in contrast to the previous approach, the assumption is that users are already aware of the breach, and they are not given more information about it. LP-Guardian (Fawaz and Shin, 2014) is a PET-tool designed for smart phone users in situations where they don't feel comfortable revealing their location.

Controlling user's data access: This approach gives users control over who can access their information. It is popular for social media sites, since users have a larger audience that includes the public. Due to the complicated nature of social media and who can see what, these PET-tools facilitate adjustments to complex and sometimes unsound user settings through different control mechanisms defined by access control policies. The work of Wishart et al., (2010) introduced a collaborative approach to authoring privacy policies that considers the needs of all parties affected by the disclosure of information on social media. Similarly, Shehab et al., (2012) presented an access control framework for managing the sharing of data belonging to social media users with third party apps. Also in the same vein is Lockr, an application that gives users the ability to define their own access control policies for sharing their online social media content to other systems (Tootoonchian et al., 2008).

4.1.3. Type of personal information

Personal information is a widely used term in the PET-tool literature to denote data that, if they were to become public, could lead to an impact on a user's privacy. The way personal information is sometimes defined in the PET-tool literature is vague, however, in terms of how granular it is, and is often limited to broad terms such as personal content, personal data, information, and data. In general, the reviewed papers fail to give a clear picture of what constitutes personal information, and what aspect of user privacy the PET-tool is trying to protect/enhance. Researchers largely

explored location threats on mobile devices, since they are equipped with various location tracking technologies. Apps offering services based on location have various implications for privacy, which PET-tool designers contributed to by providing finer grained controls as well as enhancing usability and functionality (e.g. Fawaz and Shin, 2014). Among the mentioned types of personal information on social media, photo privacy has been the main focus of PET research within OSNs.

To summarize, we observed that the types of tools in the papers we reviewed could be categorized based on three constructs: platform, type of private information addressed, and privacy enhancing approach. The starting point for tool development is the platform, each of which presents different challenges in respect to revealing private information. The privacy enhancing approach is linked to the other two constructs based on what the platform is capable of protecting, along with the type of private information that needs to be protected from exposure.

4.2. Evaluation of tools

4.2.1. Timing, setting and functional purposes of the evaluation

One of our findings was that summative evaluation was used for most of the PET-tools. One explanation for the use of summative evaluations might be that researchers are not trying to develop a specific PET-tool, but rather are studying the general concepts, testing hypotheses, and exploring the theories behind PET-tools and their effects on enhancing the technology. The tools that these academics build are prototypes that are more focused on technical aspects of the solution, whereas formative studies put more focus on the privacy aspect of PET-tools, and on the effects of the tools on users' privacy-related behavior. We found that only seven studies used formative evaluation to improve the artifact, along with summative evaluation to show the validity of their solution. Two used just a formative approach, since their design was in the mock-up phase.

Another interesting finding was that most of the evaluations happened after implementation (i.e., ex-post). The timing of the evaluation dictates to what extent the results can affect the design; ex-post evaluation makes it more difficult to implement improvements if anomalies are detected. Seven articles used both ex-ante and ex-post evaluations, while three used only ex-ante. The remaining papers used only ex-post evaluation.

We further observed that most evaluations took place in the artificial setting of a closed lab environment. Only 10 studies focused on the use of tools in a natural setting with their intended users, employing event logs, questionnaires, and qualitative methods.

4.2.2. Evaluation methods

While PET-tools make use of different technological solutions on the back end, performance evaluation was the most-used strategy in articles we reviewed. Different lab-based evaluation methods that measured the validity of the solution were used as a proof of concept. There was less research on usage of publicly available PET-tools. We found one study evaluating PET-tools by Geiger & Cranor (2006), in which they looked at six different disk-scrubbing tools used to wipe out hard disk data.

In the artificial types of evaluations, different methods of usability testing, after-test questionnaires/interviews, scenarios, accuracy, feature comparison, statistical analysis, threat analysis, microbenchmarking, flexibility, efficiency, energy consumption and compatibility testing were all popular metrics. The naturalistic evaluations used questionnaires, interviews, observation, and comparative approaches. Our study showed that most of the articles focused on the usability of the tools from the point of view of the functionality of the software itself, without accounting for behavioral changes. Qualitative evaluations form only a small part of PET-tool research. Semi-structured interviews after tool usage was more common, while early evaluation of the design by involving users in the design process, and to identify user problems that needed to be addressed, was minimal (e.g. Caine et al., 2010; Sadeh et al., 2009).

4.2.3. Evaluation measures

Our findings show that there are a range of factors influencing PET-tool usage. Privacy itself is not bound to only one single concept, but rather to a collection of different social and technical aspects, varying from individual end user concerns, to the time it takes to complete the privacy settings process. Measures used to evaluate end user privacy have been used in direct connection to the PET-tool as a dependent factor. The majority of the papers evaluated privacy in terms of the tool's specific purpose, and evaluations varied from a simplistic question to an extensive questionnaire, or an in-depth interview. Tools were tested based on what aspect of privacy they were designed to protect (i.e., what type of private information). It is evident, therefore, that researchers touched only upon privacy in terms of the measures related to their tools**.** Total 53 tool-related evaluation constructs were emerged as the result of peer group discussions and cooperative content coding (Figure 1).

No evaluation of the privacy-enhancing qualities was made in 19 papers; these studies were confined to evaluations using the tool-related measures. In terms of privacy-related constructs used for evaluation, 30 of these were found in the reviewed articles. The various privacy-related measures we found are illustrated in Figure 2. The five most common measures among the reviewed papers were privacy preferences and privacy concern which are related to privacy-related constructs. Usability, accuracy, and time were most common tool-related measures.

"Privacy preferences" was the construct that was used most often. It was employed to measure how end users adjust tool's privacy settings to the desired privacy level, and was predominantly used with PET-tools designed to enhance privacy settings for OSNs such as Facebook (e.g. Junior et al., 2014). In other cases, where OSNs were not the focus, the construct was used to evaluate end user privacy management practices via user adjustment of the range of privacy settings provided by the tool.

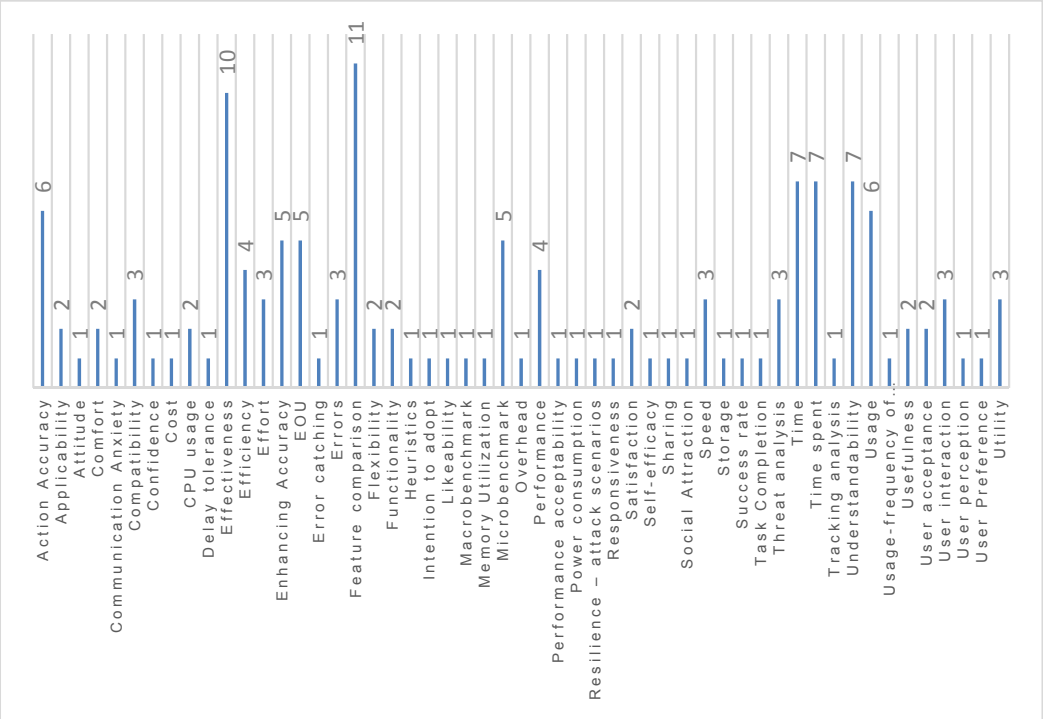

Figure 1. Tool-related measures for evaluating PET-tools and frequency of use

"Privacy concern" was used to measure the extent to which the end user was willing to disclose certain personal information through different channels. This was explored in terms of either the accessing of personal information by third parties, or the potential unintended disclosure of personal information through communication channels, such

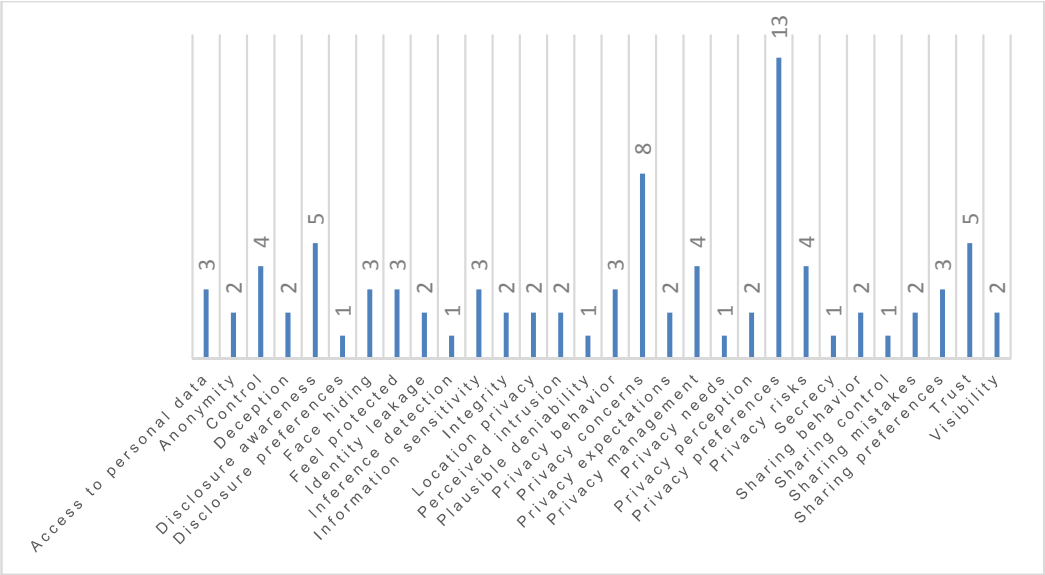

Figure 2. Privacy-related measures used to evaluate PET-tools along with the number of occurrence

as sharing content. Concerns were studied in terms of positive/negative impact on the adoption of tools, using quantitative feedback (e.g. Herath et al., 2014). PET-tool "usability" was another factor that was often evaluated, as was user acceptance. Although they do not directly affect a person's privacy, an application's design and implementation flaws can lead to the leakage of information or a reluctance to use privacy-related features. Researchers evaluated an application's functionality in some cases by comparing pre-solution and post-solution settings, and in others by enumerating the strengths of the proposed tool as compared to competing tools. The relationship between user involvement and usability was considerable. Studies that involved users at different stages employed usability testing, giving participants tasks related to the usability aspects of the tool, such as ease of use, effort, usefulness, etc. Iachello, et al. (2005), for example, studied the usability of automatic features in location-based services, concluding that users are more likely to use manual features because this gives them more control.

The evaluation of accuracy was also used quite frequently in PET-tool evaluation, appearing in two different forms in the papers we reviewed: performance accuracy and usability accuracy. Since a user's true privacy preferences might be complicated to implement, some researchers tried to minimize this complexity by measuring the performance accuracy of the PET-tool being studied, assessing how close the tool was able to come to approximating the preferences in question. The accuracy of the privacy enhancing approach, and the accuracy of the user in performing assigned tasks during testing were used as measures to indicate improvement. Fang & LeFevre (2010), for example, used accuracy to measure the e□ectiveness of their Facebook privacy settings wizard in reducing the amount of user e□ort, while still producing highly accurate settings.

Time was used in two contexts in PET-tool evaluation: as a value to measure the speed of tool performance, and as a measure of the amount of time it took users to complete a given task during testing. As was the case with accuracy, mentioned above, time can be both dependent and independent of user input. When it comes to performance, time is a factor that can indicate the applicability of a solution (e.g., Carminati, Ferrari, & Perego, 2009), or that a tool is superior to other solutions based on processing speed (e.g., encryption time in Besmer & Richter Lipford, 2010). Some researchers also focused on the amount of time users spent completing assigned tasks using the PET-tool. In those studies, time spent was used as a metric to show improvements in the amount of time it took PET-tool users to complete a given process. Time spent was used in the reviewed papers in conjunction with tool understandability to indicate the effort required to carry out a task. Lin, et al. (2012) showed how their tool reduced the time it took for users to understand Android apps' privacy permissions.

5. Conclusion

This is the first literature review to investigate the types of privacy tools with end user interaction and their role in design and evaluation of the tools. The results highlighted that there are three main enhancing approaches such as informing about risks, offering to hide detail and controlling user's data access. Reviewed literature showed that it is still unclear what measures are suitable to evaluate a PET-tool. The results of our study may help the designers of future PET-tools be more aware of the types of measures that can be used to evaluate their tools, especially when studying previous efforts and outcomes. In our literature review on PET-tools there was no evaluation standard in the form of a model, method or framework being used as a basis for evaluating PET-tools. Further research to establish evaluation criteria for privacy affecting systems or PET-tools can give rise to a better understanding of users' socially constructed practices of privacy management, compared to the aftermath of PET-tool use (Padyab, 2014). Adopting and testing privacy-related theories within evaluation of PET-tools is also an avenue of research that is worth exploring. There are some scattered privacy-related evaluation guidelines available in the literature, but they are either very specific to a particular technology (e.g. Just, 2004), or there is a lack of information on their usage (Bellotti, 1997). We encourage researchers to design new evaluation frameworks for PET-tools, or to use currently available ones while reporting their strengths and weaknesses.

6. Acknowledgment

This work was funded by the European Commission in the context of the Horizon 2020 PrivacyFlag project (Grant Agreement No. 653426). The authors are very grateful to the two anonymous reviewers for their constructive comments.

7. References

Agarwal, Y. and Hall, M. (2013), "ProtectMyPrivacy: Detecting and Mitigating Privacy Leaks on iOS Devices Using Crowdsourcing", Proceeding of the 11th Annual International Conference on Mobile Systems, Applications, and Services, ACM, New York, NY, USA, pp. 97–110.

Andersen, B.L., Jørgensen, M.L., Kold, U. and Skov, M.B. (2006), "iSocialize: Investigating Awareness Cues for a Mobile Social Awareness Application", Proceedings of the 18th Australia Conference on Computer-Human Interaction: Design: Activities, Artefacts and Environments, ACM, New York, NY, USA, pp. 7–14.

Bélanger, F. and Crossler, R.E. (2011), "Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems", MIS Q., Vol. 35 No. 4, pp. 1017–1042.

Bellotti, V. (1997), "Technology and Privacy", in Agre, P.E. and Rotenberg, M. (Eds.), , MIT Press, Cambridge, MA, USA, pp. 63–98.

Besmer, A. and Richter Lipford, H. (2010), "Moving Beyond Untagging: Photo Privacy in a Tagged World", Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, ACM, New York, NY, USA, pp. 1563–1572.

Caine, K.E., Zimmerman, C.Y., Schall-Zimmerman, Z., Hazlewood, W.R., Sulgrove, A.C., Camp, L.J., Connelly, K.H., et al. (2010), "DigiSwitch: Design and Evaluation of a Device for Older Adults to Preserve Privacy While Monitoring Health at Home", Proceedings of the 1st ACM International Health Informatics Symposium, ACM, New York, NY, USA, pp. 153–162.

Carminati, B., Ferrari, E. and Perego, A. (2009), "Enforcing Access Control in Web-based Social Networks", ACM Trans. Inf. Syst. Secur., Vol. 13 No. 1, p. 6:1–6:38.

Cranor, L.F. (1999), "Internet Privacy", Communications of the ACM, Vol. 42 No. 2, pp. 28–38.

Egelman, S., Oates, A. and Krishnamurthi, S. (2011), "Oops, I Did It Again: Mitigating Repeated Access Control Errors on Facebook", Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, ACM, New York, NY, USA, pp. 2295–2304.

Fang, L. and LeFevre, K. (2010), "Privacy Wizards for Social Networking Sites", Proceedings of the 19th International Conference on World Wide Web, ACM, New York, NY, USA, pp. 351–360.

Fawaz, K. and Shin, K.G. (2014), "Location Privacy Protection for Smartphone Users", Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, ACM, New York, NY, USA, pp. 239–250.

Geiger, M. and Cranor, L.F. (2006), "Scrubbing Stubborn Data: An Evaluation of Counter-Forensic Privacy Tools", IEEE Security Privacy, Vol. 4 No. 5, pp. 16–25.

Goldberg, I. (2003), "Privacy-Enhancing Technologies for the Internet, II: Five Years Later", in Dingledine, R. and Syverson, P. (Eds.), Privacy Enhancing Technologies, Springer Berlin Heidelberg, pp. 1–12.

Habibipour, A., Padyab, A., Bergvall-Kåreborn, B. and Ståhlbröst, A. (2017), "Exploring Factors Influencing Participant Drop-Out Behavior in a Living Lab Environment", in Stigberg, S., Karlsen, J., Holone, H. and Linnes, C. (Eds.), Nordic Contributions in IS Research, Vol. 294, Springer International Publishing, Cham, pp. 28–40.

Herath, T., Chen, R., Wang, J., Banjara, K., Wilbur, J. and Rao, H.R. (2014), "Security services as coping mechanisms: an investigation into user intention to adopt an email authentication service", Information Systems Journal, Vol. 24 No. 1, pp. 61–84.

Iachello, G. and Hong, J. (2007), "End-user privacy in human-computer interaction", Foundations and Trends in Human-Computer Interaction, Vol. 1 No. 1, pp. 1–137.

Iachello, G., Smith, I., Consolvo, S., Abowd, G.D., Hughes, J., Howard, J., Potter, F., et al. (2005), "Control, Deception, and Communication: Evaluating the Deployment of a Location-Enhanced Messaging Service", in Beigl, M., Intille, S., Rekimoto, J. and Tokuda, H. (Eds.), UbiComp 2005: Ubiquitous Computing, Springer Berlin Heidelberg, pp. 213–231.

Junior, M.P., Xavier, S.I. de R. and Prates, R.O. (2014), "Investigating the Use of a Simulator to Support Users in Anticipating Impact of Privacy Settings in Facebook", Proceedings of the 18th International Conference on Supporting Group Work, ACM, New York, NY, USA, pp. 63–72.

Just, M. (2004), "Designing and evaluating challenge-question systems", IEEE Security Privacy, Vol. 2 No. 5, pp. 32–39.

Kolter, J.P. (2010), User-Centric Privacy: A Usable and Provider-Independent Privacy Infrastructure, EUL Verlag, Lohmar, available at: https://www.ics.uci.edu/~kobsa/phds/kolter.pdf.

Laudon, K.C. (1996), "Markets and Privacy", Communications of the ACM, Vol. 39 No. 9, pp. 92–104.

Lin, J., Amini, S., Hong, J.I., Sadeh, N., Lindqvist, J. and Zhang, J. (2012), "Expectation and Purpose: Understanding Users' Mental Models of Mobile App Privacy Through Crowdsourcing", Proceedings of the 2012 ACM Conference on Ubiquitous Computing, ACM, New York, NY, USA, pp. 501–510.

Okoli, C. and Schabram, K. (2010), "A Guide to Conducting a Systematic Literature Review of Information Systems Research", SSRN Electronic Journal, available at:https://doi.org/10.2139/ssrn.1954824.

Padyab, A., Päivärinta, T., Ståhlbröst, A. and Bergvall-Kåreborn, B. (2016), "Facebook Users Attitudes towards Secondary Use of Personal Information", Proceedings of the 37th International Conference on Information Systems (ICIS 2016), Dublin, Ireland, p. 20.

Padyab, A.M. (2014), "Getting More Explicit on Genres of Disclosure: Towards Better Understanding of Privacy in Digital Age (Research in Progress)", Norsk Konferanse for Organisasjoners Bruk Av IT, Vol. 22 No. 1, available at: (accessed 17 September 2015).

Preece, J., Sharp, H. and Rogers, Y. (2015), Interaction Design: Beyond Human-Computer Interaction, John Wiley & Sons.

Pries-Heje, J., Baskerville, R. and Venable, J. (2008), "Strategies for Design Science Research Evaluation", Conference Proceedings, 16th European Conference on Information Systems, National University of Ireland.

Sadeh, N., Hong, J., Cranor, L., Fette, I., Kelley, P., Prabaker, M. and Rao, J. (2009), "Understanding and Capturing People's Privacy Policies in a Mobile Social Networking Application", Personal Ubiquitous Comput., Vol. 13 No. 6, pp. 401–412.

Shehab, M., Squicciarini, A., Ahn, G.-J. and Kokkinou, I. (2012), "Access control for online social networks third party applications", Computers & Security, Vol. 31 No. 8, pp. 897–911.

Tootoonchian, A., Gollu, K.K., Saroiu, S., Ganjali, Y. and Wolman, A. (2008), "Lockr: Social Access Control for Web 2.0", Proceedings of the First Workshop on Online Social Networks, ACM, New York, NY, USA, pp. 43–48.

Venable, J., Pries-Heje, J. and Baskerville, R. (2012), "A Comprehensive Framework for Evaluation in Design Science Research", in Peffers, K., Rothenberger, M. and Kuechler, B. (Eds.), Design Science Research in Information Systems. Advances in Theory and Practice, Springer Berlin Heidelberg, pp. 423–438.

Venable, J., Pries-Heje, J. and Baskerville, R. (2014), "FEDS: a Framework for Evaluation in Design Science Research", European Journal of Information Systems, Vol. 25 No. 1, pp. 1–13.

Westin, A.F. (1967), Privacy and Freedom, Antheneum, New York, NY, USA.

Wishart, R., Corapi, D., Marinovic, S. and Sloman, M. (2010), "Collaborative Privacy Policy Authoring in a Social Networking Context", 2010 IEEE International Symposium on Policies for Distributed Systems and Networks (POLICY), presented at the 2010 IEEE International Symposium on Policies for Distributed Systems and Networks (POLICY), pp. 1–8.