A Classification of Factors Influencing Low Adoption of PETs Among SNS Users

Konstantina Vemou and Maria Karyda

Department of Information and Communication Systems Engineering,
University of the Aegean, Samos, GR-83200, Greece
{kvemou,mka}@aegean.gr

Abstract. Privacy concerns among Social Networking Services (SNS) users are increasing. However, Privacy-Enhancing Technologies (PETs) are not, yet, widely deployed and their deployment rate is marginally growing. This is surprising given the fact that PETs are widely recognized as effective at reducing privacy risks. This paper explores this paradox, by presenting a classification of the key factors influencing the adoption of PETs. The conclusions of our analysis suggest that, certain factors are overemphasized, while the importance of others has been overlooked. Our classification is based on relevant literature and experimental analysis of PETs, and can inform both practitioners for designing and enhancing PETs, as well as researchers, as we identify several open issues.

Keywords: Social Network Services, Privacy-Enhancing Technologies, adoption.

1 Introduction

Privacy concerns among Social Networking Services (SNS) users are increasing [1], [2], and there is even a small proportion of users who are willing to pay for privacy-friendly services [3]. Privacy research in SNS focuses on developing and applying Privacy-Enhancing technologies (PETs) to support users participating in social networks, while maintaining their privacy. PETs used in the context of SNS include, mainly, attribute-based controls, such as Facecloak, decentralized SNS, such as Diaspora and privacy management applications, such as MyPermissions Cleaner.

However, privacy enhancing technologies are not, yet, widely deployed [3], [4]; moreover the rate at which their deployment has grown over the last few years has not been substantial. This is surprising given the fact that PETs are widely recognized as effective at reducing privacy risks [4], [5]. This paper discusses this paradox and addresses the question why PETs adoption by social network users is so far limited. Understanding this issue and analyzing the underlying causes can serve as a guide for future research and practice, to provide users with more effective and attractive PETs.

To analyze the problem of low adoption of PETs, we have followed a multifaceted approach: First we identified all relevant factors associated with the low adoption of PETs from the extant literature. Then we conducted experiments with several PETs,

S. Furnell, C. Lambrinoudakis, and J. Lopez (Eds.): TrustBus 2013, LNCS 8058, pp. 74–84, 2013.

and evaluated them against these factors in order to derive more insights with regard to their use. This exploration resulted to a classification of key factors influencing low adoption of PETs in SNS, based on literature research and experimental use of PETs by the authors.

The literature analysis allowed us derive important conclusions and identify contradicting findings. For instance, while several papers argue on the importance of users being aware of PETs [6], [7], others suggest that awareness is not associated with their increased deployment. This paper provides a deeper understanding of the issues pertaining to the use of privacy enhancing technologies, whereas current approaches tend to shed light to specific aspects of the issue, while neglecting others.

The contribution of this paper is both theoretic and practical: On a theoretical level, we identify and provide a classification of the key factors influencing the limited use of PETs in the context of SNS. We discuss these factors and show that some may have been overestimated while the importance of others seems to evade researchers' attention. From a practitioner's viewpoint, we illustrate aspects of privacy protection that commonly used PETs fail to meet, thus contributing to users' abstention from the use of privacy preserving technologies.

The paper is structured as follows: in the following chapter, we describe PETs used in SNS. In chapter 3 the classification of key factors affecting PETs adoption by SNS users is presented. The last chapter contains conclusions deriving from our work, as well as highlights of areas for further research.

2 Background: Privacy Enhancing Technologies and Social Networks

Privacy concerns related to the use of Social Network Services are increasing [2]. To address these concerns several technological measures have been developed, aiming to protect published information from unauthorized audiences and raise the users' awareness when it comes to sharing personally identifiable information (PII). Such technologies, commonly known as Privacy Enhancing Technologies, or PETs, include a wide range of applications including access control, privacy signaling tools, third party tracking tools, social identity management systems and decentralization of Social Network Services.

PETs used in SNS include attribute-based controls which are based on encryption (e.g. Lockr [8], Persona [9] and EASiER [10]), role-based access controls, based on encryption and/or obfuscation or perturbation (e.g. BlogCrypt [11], FlyByNight [12], Facecloak [13], FaceVPSN [14] and NOYB [15]), and audience segregation (e.g. the Clique Prototype [7]). Another approach aiming at protecting PII via avoiding central repositories has been implemented either as web-based decentralized SNS (Diaspora [16], Vis-à-vis [17], Frenzy [18]) or as Peer-To-Peer SNS (Safebook [19], PeerSoN [20], Life Social [17], Likir [17]).

Privacy signaling technologies such as RMP-Respect My privacy [21] and P3P [22] can also be applied in SNS, while other tools include privacy wizards that help users set their privacy settings (e.g. Collaborative policy analysis [23], PriMa [24],

MyPermissions Cleaner [25], privacyfix [26], Priveazy LOCKDOWN [27]). Privacy Mirrors help users understand which of their personal information is visible to other users (such as Facebook's ViewAs and Search engine profile preview [28], Privacy Mirror [29], Privacy Check [30], PrivAware [31], make myself clear [32]).

There are also Social Network Visualization Tools (such as Vizster [33], Friendwheel [34]) and Personal Containers, which register which information about the user has been published and where they were published (Privacy Delegate [35], Privacy Butler [36]). Last but not least, there are tools that reveal which social networking services track users while surfing the internet (Disconnect [37]).

Despite this plethora of privacy tools, some of which are independent applications while others are embedded into SNS platforms, users still don't seem to be taking advantage of them, despite rising privacy concerns and thriving use of SNS. For instance, relevant literature reports on the limited use of access controls and privacy settings that are provided within the SNS platforms [38], [1], [39], [40]. It should be noted though that perception of low adoption of PETs is based mainly on literature and there is lack of published research and statistics about the use of specific standalone PETs in practice.

But why does this phenomenon happen? Why do so few users employ privacy enhancing technologies? Several reasons have been proposed, including lack of knowledge, lack of skills [5], the time needed to learn a new technology, the complexity of existing technologies [52] the multiplicity of approaches to privacy protection [41], cost [42], usability issues [41], lack of support by the platform [43], users cognitive and behavioral biases [42]. Another aspect of users' paradoxical behavior has been traced in their unawareness of some of privacy threatening e-service aspects [44]. Most relative studies try to answer this question by focusing on a specific aspect of the problem, especially to why some users change their privacy settings within SNS, when this is provided as an option, to limit the audience of what they share, while others don't [45], [5].

Up to now, however, no relevant study has attempted a thorough discussion of all factors contributing to the low adoption of PETs by SNS users. In the following we provide an in-depth discussion of the key factors we have identified through literature review and deployment of a large set of available PETs that are applied by SNS users.

3 Key Factors Affecting PETs Adoption by SNS Users

3.1 Awareness of Privacy Risks and PETs

It has been suggested that many SNS users are unaware of the existence of some PETs [46]. Moreover, it is often the case that users are not aware of certain privacy-threatening aspects of the services they are using, such as, for instance, privacy dangers deriving from third-party applications [44]. Therefore, they cannot benefit from special purpose PETs, such as those aiming at limiting the access of third party applications to personal information (e.g. MyPermissions Cleaner [25]). Relevant literature, however, also reports findings where individuals despite being aware of PETs, did not use them [4], [47].

Generally, privacy concerns and awareness of privacy risks are considered to contribute to a user's informed decision to reveal PII [6], as well as to take measures against its misuse. This is also true the other way around, as Xu and al. (2009) found the level of privacy concern to be inversely linked to perceptions of control on the flow of information disclosure, including PETs use [48]. The level of privacy concern acts as a motive for PETs use, however it is a weak predictor to the users' decision, as the user faces cognitive and behavioral biases [41].

Conclusively, being aware of privacy tools is an essential prerequisite for their use, awareness is only weakly linked to their deployment. It this thus important, to include other individual as well as technical related factors in order to gain a deeper understanding of the problem.

3.2 Requirements for Special IT Skills

Lack of technical skills and the time needed to learn a technology have also been identified as possible inhibitors for the use of PETs [5], [4]. As Yao [49] states, many online privacy protection strategies require technical skills beyond that of an average user, and this is true even for young adolescents [50].

Our experience from testing relevant tools, indicates that SNS users need to be familiar with the not so trivial use of browser extensions in order to use applications such as Priveasy Lockdown [27] and FaceVPSN [14]. Moreover, users need at least basic knowledge of concepts as encryption is applied in most access control solutions. For example, to use Blogcrypt [11] the user has to manually import and export encryption keys. Even worse, to use PETs deployed in distributed social networks, as in the case of Vis-à-Vis [17], users must be able to create and publish their own profile, and maintain them in their personal computer resources.

3.3 Complexity and Diversity

The need for privacy protection, including adoption of PETs, stems from a set of multiple and different risks, resulting of different aspects of SNS use, e.g. posting of photographs, chatting, sharing friends list. As a result, different practices are applied to protect a user's privacy, some aiming at awareness and some aiming at information concealment. Moreover, researchers provide different solutions to the same aspects of privacy risks. An example is the implementation of access controls by obfuscation, as in NOYB [15] or encryption, as in StegoWeb [51]. This leaves the user with multiple and diverse tools or technologies to evaluate, in order to choose which one to use, a process that requires a significant amount of time, effort and knowledge. In addition to the diversity of PETs, users encounter complex and unusable interfaces [38] that make the tools difficult to configure [52], thus adding to the difficulty of PETs adoption.

3.4 Direct and Indirect Cost

As with other software products, the use of PETs may entail direct cost for acquiring the tool, as well as intangible costs, related to time for learning [53], limited functionality

and usability issues, such as how seamless is the authentication to third-party websites [41] etc.

Most users report they are not always willing to pay for acquiring a privacy tool, despite having privacy concerns [41]. Rose (2005) found that, although most participants in a survey reported being very sensitive to privacy issues, less than half of them would be willing to pay roughly $29 to have their privacy protected by means of property rights on personal information [41]. However, many PETs can be acquired and used with no direct cost.

Moreover, SNS users are not keen of experiencing delays, changing their habits of interacting with an e-service or discounting usability, due to PETs use. For example, a typical Facebook user with an average number of 130 friends [54], who wants to encrypt her posted data using FlyByNight, needs to encrypt messages with each of her friends public keys, thus experiencing significant overhead and delay [12].

Switching costs, usually described as platform lock-in, can also affect the intention of SNS users to deploy PETs, if this requires switching to a new SNS platform [53]. For instance, to use Scrambls, all recipients need to use the required platform plugin [55] to decrypt a message. Ajami and Ramadan [43] argue that if an SNS provider identifies the use of Facecloak, a PET that replaces selected information with other meaningful values when these are posted to the SNS, then they may suspend the user account. This also adds to the switching costs for the use of PETs, since a privacy sensitive user needs to switch to another social network platform in order to apply privacy preserving tools.

Generally, PETs are technologies that make processing of personal data more costly or may prevent it altogether. Only a subset of PETs can claim to be 'positive-sum' in the sense that they allow the delivery of services as well as or better than would be the case without them. [4]

3.5 Low Visibility of Effectiveness and Inadequate Feedback

Users' awareness of the benefits derived from preserving their privacy is also a critical factor with regard to their decision to use privacy enhancing applications. There are users who report that they do not believe in the effectiveness of PETs [56]. This can be attributed to the way PETs communicate, or rather fail to do so, their results and to the way they give feedback for actions they have performed to protect the user [57] or to the way privacy related dangers are presented by the technology used [58].

For instance, Disconnect, a block-tracking tool that filters traffic to third-party sites to prevent tracking, does not provide any feedback on the privacy risks deriving from the third-party websites that are blocked [37]. The same problem exists with the use of encryption enabling PETs that do not inform users who or what were prevented from accessing their personal information.

3.6 Privacy Requirements are Partially Addressed

Most privacy enhancing technologies meet specific, only, privacy requirements. While privacy protection generally entails protecting PII from unauthorized information

collection, processing and dissemination, informing users and providing them with control over their personal data [59], [60], each privacy tool typically meets only a small fraction of these requirements.

For instance, both FlybyNight [12] and NOYB [15] use encryption and obfuscation in order to conceal user's information from the SNS platform and unauthorized users, but fail to protect the future inappropriate use of this information by users that may be authorized to access it [43]. At the same time, other types of PETs, such as privacyfix [26] and MyPermissions Cleaner [25], aim at raising user's privacy awareness, by visualizing the entities that may access their information or highlight issues deriving from the privacy policy, but offer no actual data shield, unless the user actively changes her privacy settings.

3.7 The Role of the SNS Platform

Some PETs, such as P3P [22], need to be supported by the SNS provider in order for users to employ them. However, providers are not always happy to support PETs if they are not obliged to, as there is no evidence that they will gain competitive advantage by establishing the use PETs [61] and at the same time they need to abandon personal information collection and pay the cost of acquiring a technology, as well as changing their technical infrastructure [62].

A typical example is Facebook's complex access control mechanisms, offered in Privacy Settings. While privacy breaches due to this type of access control have reached spotlight and Google+, a competing SNS provider is built on the idea of personal circles [63], Facebook has not redesigned social networks organization on the principles of audience segregation to support PETs such as Clique Prototype [7]. Finally, the application of basic access controls in some SNS was a late response to privacy advocate requests and not an initiative of SNS providers to protect personal information [64].

3.8 Responsibility Misconceptions

When it comes to privacy protection, many users have the belief that providers and government are applying necessary measures to ensure it, and are not aware that privacy protection is partly their responsibility as well. In fact, a Location Based Services Privacy survey, conducted in 2009, showed that PETs were perceived to be a relatively weaker mechanism for enhancing control and reducing privacy risk because they shift the responsibility of privacy protection on the individual users [48]. What is more, most existing PETs for SNS are based on the user's choice to use, such as browser add-ons that encrypt posted messages or highlight potential privacy issues, deriving from default privacy settings. Studies have shown that belief of low effectiveness of privacy regulation or company privacy policies is an incentive for protection technology adoption by the user [65], so low adoption of PETs appears as a result of this belief.

Complex privacy policies published in most SNS contribute to this finding because many users misinterpret their presence as enabled privacy protection, while if the

presentation was simple and direct, they could understand the privacy issues and would be willing to pay for PETs [41][66]. On the other hand, SNS compliance to privacy regulations is difficult to audit, due to lack to accountability mechanisms. For example, there is the discussion of whether self-regulation, co-regulation or direct regulation should be used to enforce respect to users' stating their preference by employing the Do Not Track (DNT) mechanism [3].

3.9 Culture

Privacy concerns and privacy behavior are culture dependent. It has been found, for instance, that in Eastern culture, excessive self-disclosure is considered inappropriate, so privacy concerns are increased [67]. In 2009, a study by Hichang Cho et al. found that internet users' privacy concerns and behavioral responses such as opt-out and avoidance, varied significantly across nationalities, and they can be partially explained by national culture values [68]. However, multinational studies do not focus on how effectiveness of individual privacy protection mechanisms and strategies, including PETs, is perceived by individuals of different cultural background [48][68].

4 Conclusions and Further Research

The protection of PII in SNS is a complex issue involving several stakeholders, such as the users, PETs industry and developers, SNS providers, governments and regulatory bodies and third parties (e.g. advertisers). It thus calls for combined solutions, in which economic forces, cryptographic technologies, and targeted regulatory guidelines conspire to create a system with adequate enforcement and control powers (see also OECD (1997)) [41].

This paper presents an in-depth analysis of the key factors contributing to the limited adoption of privacy supporting technologies among SNS users. To the best of our knowledge, this is the first attempt to provide a unified view of the problem. Extant literature provides partial explanations derived from specific viewpoints: e.g. some researchers draw on social theory and employ diffusion of innovation models, others employ behavioral theories and technology acceptance models [41] or even economic theories [41]. This paper presents a critical discussion of all factors that have been identified and provides an integrated approach to the problem.

Our analysis has showed that the importance of awareness is rather overestimated, since many users are aware of different PETs but still refrain from their use. Cost, both direct and indirect, also contributes to low PETs adoption, but it is also the issues of the diversity and multiplicity of tools and applications that needs to be considered. Moreover, complexity and usability issues are also important determinants of PETs deployment, while the fact that users tend to underestimate their effectiveness due to low visibility of their results, seems to be ignored by vendors and developers.

It is also important to note that PETs currently offer very specific and limited functions with regard to privacy requirements in the context of SNS and that researchers and providers need to provide more integrated privacy solutions. Finally, the role of

culture seems to play an important role with regard to users' inclination against the use of PETs, and should be further explored.

Our effort to identify and evaluate the adoption of specific PETs by SNS users, was limited by the complete lack of relevant statistics and studies on the actual use of privacy tools by SNS users. Future research includes measuring the importance of each of the factors we have identified through a qualitative analysis, using actual user data.

References

1. Acquisti, A., Gross, R.: Imagined communities: awareness, information sharing, and privacy on Facebook. In: Danezis, G., Golle, P. (eds.) PET 2006. LNCS, vol. 4258, pp. 36–58. Springer, Heidelberg (2006)
2. Boyd, D., Hargittai, E.: Facebook privacy settings: Who cares? First Monday 15(8) (2010)
3. ENISA: Privacy considerations of online behavioural tracking, report (2012)
4. London Economics: Study on the economic benefits of privacy-enhancing technologies (PETs). Final Report to The European Commission DG Justice, Freedom and Security (2010)
5. Compañó, R., Lusoli, W.: The Policy Maker's Anguish: Regulating Personal Data Behavior Between Paradoxes and Dilemmas. In: Moore, T., et al. (eds.) Economics of Information Security and Privacy, pp. 169–185. Springer Science+Business Media, LLC (2010)
6. Pötzsch, S.: Privacy Awareness: A Means to Solve the Privacy Paradox? In: Matyáš, V., Fischer-Hübner, S., Cvrček, D., Švenda, P. (eds.) The Future of Identity. IFIP AICT, vol. 298, pp. 226–236. Springer, Heidelberg (2009)
7. Van den Berg, B., Leenes, R.E.: Audience Segregation in Social Network Sites. In: Proceedings for SocialCom 2010/PASSAT 2010 (Second IEEE International Conference on Social Computing/Second IEEE International Conference on Privacy, Security, Risk and Trust), pp. 1111–1117. IEEE (2010)
8. Tootoonchian, Y.G.A., Saroiu, S., Wolman, A.: Lockr: Better privacy for social networks. In: Proceedings of the 5th ACM International Conference on emerging Networking EXperiments and Technologies (CoNEXT), pp. 169–180. ACM, New York (2009)
9. Baden, R., Bender, A., Spring, N., Bhattacharjee, B., Starin, D.: Persona: An online social network with user-defined privacy. In: Proceedings of the ACM SIGCOMM 2009 Conference on Data Communication, pp. 135–146. ACM, New York (2009)
10. Jahid, S., Mittal, P., Borisov, N.: EASiER: Encryption-based Access Control in Social Networks with Efficient Revocation. In: Proceedings of 6th ACM Symposium on Information, Computer and Communications Security, pp. 411–415. ACM, New York (2011)
11. Paulik, T., Földes, Á.M., Gulyás, G.: BlogCrypt: Private content publishing on the Web. In: Proceedings of the Fourth International Conference on Emerging Security Information, Systems and Technologies, SECURWARE 2010, pp. 123–128. IEEE (2010)
12. Lucas, M.M., Borisov, N.: Flybynight: mitigating the privacy risks of social networking. In: Proceedings of the 7th ACM Workshop on Privacy in the Electronic Society, pp. 1–8. ACM, New York (2008)
13. Luo, W., Xie, Q., Hengartner: Facecloak: An architecture for user privacy on social networking sites. In: 2009 International Conference on Computational Science and Engineering, pp. 26–33. IEEE (2009)

14. Conti, M., Hasani, A., Crispo, B.: Virtual private social networks. In: Proceedings of the First ACM Conference on Data and Application Security and Privacy, pp. 39–50. ACM, New York (2011)
15. Guha, S., Tang, K., Francis, P.: NOYB: privacy in online social networks. In: Proceedings of the First Workshop on Online Social Networks, pp. 49–54. ACM, New York (2011)
16. Diaspora*, https://joindiaspora.com/
17. Shakimov, A., Lim, H., Caceres, R., Cox, L.P., Li, K., Liu, D., Varshavsky A.: Vis-à-Vis: Privacy-preserving online social networking via Virtual Individual Servers. In: Third International Conference on Communication Systems and Networks, COMSNETS 2011, pp. 1–10. IEEE (2011)
18. Frenzy – The Dropbox powered social network, http://frenzyapp.com/
19. Cutillo, L.A., Molva, R., Strufe, T.: Safebook: a privacy preserving online social network leveraging on real-life trust. IEEE Communications Magazine 47(12), 94–101 (2009)
20. Buchegger, S., Schiöberg, D., Vu, L.H., Datta, A.: PeerSoN: P2P social networking: early experiences and insights. In: Proceedings of the Second ACM EuroSys Workshop on Social Network Systems, pp. 46–52. ACM, New York (2009)
21. Kang, T., Kagal, L.: Enabling Privacy-awareness in Social Networks. In: Intelligent Information Privacy Management Symposium at the AAAI Spring Symposium 2010 (2010)
22. Cranor, L.: P3P: Making privacy policies more useful. IEEE Security and Privacy 1(6), 50–55 (2003)
23. Toch, E., Sadeh, N.M., Hong, J.: Generating default privacy policies for online social networks. In: Proceedings of the 28th of the International Conference Extended Abstracts on Human Factors in Computing Systems, pp. 4243–4248. ACM, New York (2009)
24. Squicciarini, A., Paci, F., Sundareswaran, S.: PriMa: an effective privacy protection mechanism for social networks. In: Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security, pp. 320–323. ACM, New York (2010)
25. My permissions.org – Scan your permissions. Find out who gained access to your personal info, http://mypermissions.org/
26. Privacyfix – Lock down your privacy, https://privacyfix.com/start
27. Priveazy – The 'eazy' way to protect your privacy and stay safe online, https://www.priveazy.com/
28. Data use Policy | Facebook, Interactive Tools, https://www.facebook.com/about/privacy/tools
29. Privacy Mirror on Facebook, http://apps.facebook.com/privacy_mirror/
30. Privacy Check, http://www.rabidgremlin.com/fbprivacy/
31. Becker, J., Chen, H.: Measuring Privacy Risk in Online Social Networks (2009), https://www.cs.pitt.edu/~chang/265/proj10/zim/measureprivacyrisk.pdf
32. Make myself clear, protecting you from you since (2012), http://makemyselfclear.com/
33. Heer, J., Boyd, D.: Vizster: Visualizing Online Social Networks. In: Proc. IEEE Symp. Information Visualization, pp. 32–39 (2005)
34. Friend Wheel, https://friend-wheel.com/
35. Monjas, M.A., Del Alamo, J.M., Yelmo, J.C., Hogberg, J.: Privacy Delegate: a browser-based tool for privacy self-management in social networks, Ericsson Position paper: W3C Workshop on identity in the browser (2010)

36. Wishart, R., Corapi, D., Madhavapeddy, A., Sloman, M.: Privacy Butler: A Personal Privacy Rights Manager for Online Presence. In: Proceedings of the 8th IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops), pp. 672–677. IEEE (2010)
37. In private browsing & search | Stop online tracking & malware | Disconnect, https://disconnect.me
38. Strater, K., Lipford, H.: Strategies and struggles with privacy in an online social networking community. In: Proceedings of the 22nd British HCI Group Annual Conference on People and Computers: Culture, Creativity, Interaction, vol. 1, pp. 111–119. British Computer Society, Swinton (2008)
39. Madejskiy, M., Johnson, M., Bellovin, S.M.: The Failure of Online Social Network Privacy Settings. In: CUCS-010-11 (2011), http://academiccommons.columbia.edu/catalog/ac:135406
40. Hallinana, D., Friedewalda, M., McCarthyb, P.: Citizens' perceptions of data protection and privacy in Europe. Computer Law & Security Review 28, 263–272 (2012)
41. Acquisti, A.: The Economics of Personal Data and the Economics of Privacy, DRAFT (November 24, 2010), http://www.heinz.cmu.edu/~acquisti/papers/acquisti-privacy-oecd-22-11-10.pdf
42. Acquisti, A., Grossklags, J.: Privacy Attitudes and Privacy Behavior: Losses, Gains, and Hyperbolic Discounting (2004), Preliminary draft http://www.heinz.cmu.edu/~acquisti/papers/acquisti_grossklags_eis_refs.pdf; Final version in Camp, J., Lewis, R. (eds.): The Economics of Information Security. Kluwer (2004)
43. Ajami, R., Ramadan, N., Mohamed, N., Al-Jaroodi, J.: Security Challenges and Approaches in Online Social Networks: A Survey. IJCSNS International Journal of Computer Science and Network Security 11(8) (August 2011)
44. Wang, N., Grossklags, J., Xu, H.: An Online Experiment of Privacy Authorization Dialogues for Social Applications. In: Proceedings of the 2013 Conference on Computer Supported Cooperative Work, CSCW 2013, pp. 261–272. ACM, New York (2013)
45. Lewis, K., Kaufman, J., Christakis, N.: The Taste for Privacy: An Analysis of College Student Privacy Settings in an Online Social Network. Journal of Computer-Mediated Communication 14, 79–100 (2008)
46. Flash Eurobarometer 225: Data Protection in EU: Citizens' Perception. European Commission (2008)
47. Oomen, I., Leenes, R.: Privacy Risk Perceptions and Privacy Protection Strategies. In: de Leeuw, E., Fischer-Hübner, S., Tseng, J., Borking, J. (eds.) IFIP International Federation for Information Processing, Policies and Research in Identity Management, vol. 261, pp. 121–138. Springer, Boston (2008)
48. Xu, H., Gupta, S., Rosson, M.B., Carroll, J.M.: Effectiveness of Privacy Assurance Approaches in Location-Based Services: A Study of India and the United States. In: Proceedings of the Eighth International Conference on Mobile Business, pp. 278–283. IEEE (2009)
49. Yao, M.Z.: Self-Protection of Online Privacy: A Behavioral Approach. In: Trepte, S., Reinecke, L. (eds.) Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web. Springer, Heidelberg (2011)
50. Youn, S.: Determinants of Online Privacy Concern and Its Influence on Privacy Protection Behaviors Among Young Adolescents. Journal of Consumer Affairs 43, 389–418 (2009)

51. Besenyei, T., Földes, A.M., Gulyás, G.G., Imre, S.: StegoWeb: Towards the Ideal Private Web Content Publishing Tool. In: Proceedings of SECURWARE 2011, The Fifth International Conference on Emerging Security Information, Systems and Technologies, pp. 109–114. IARIA (2011)
52. Leon, P.G., Ur, B., Balebako, R., Cranor, L.F., Shay, R., Wang, Y.: Why Johnny Can't Opt Out: A Usability Evaluation of Tools to Limit Online Behavioral Advertising. In: Proceedings of SIGCHI Conference on Human Factors in Computing Systems, pp. 589–598. ACM, New York (2012)
53. Edlin, S.A., Harris, R.G.: The Role of Switching Costs in Antitrust Analysis: A Comparison of Microsoft and Google. Forthcoming in Yale Journal of Law and Technology 15 (February 7, 2013)
54. Facebook Statistics | Statistic Brain, http://www.statisticbrain.com/facebook-statistics/
55. Scrambls, https://scrambls.com
56. Hallinana, D., Friedewalda, M., McCarthyb, P.: Citizens' perceptions of data protection and privacy in Europe. Computer Law & Security Review 28, 263–272 (2012)
57. Shin, D.H.: The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption. Interacting with Computers 22, 428–438 (2010)
58. Kobsa, A., Teltzrow, M.: Contextualized Communication of Privacy Practices and Personalization Benefits: Impacts on Users' Data Sharing and Purchase Behavior. In: Martin, D., Serjantov, A. (eds.) PET 2004. LNCS, vol. 3424, pp. 329–343. Springer, Heidelberg (2005)
59. Solove, D.J.: A taxonomy of privacy. University of Pennsylvania Law Review 154(3) (January 2006)
60. Schwaig, K.S., Kane, G.C., Storey, V.C.: Compliance to the fair information practices: How are the Fortune 500 handling online privacy disclosures? Information and Management 43(7), 805–820 (2006)
61. Fairchild, A., Ribbers, P.: Privacy-Enhancing Identity Management in Business. In: Camenisch, J., Leenes, R., Sommer, D. (eds.) Digital Privacy. LNCS, vol. 6545, pp. 107–129. Springer, Heidelberg (2011)
62. Feigenbaum, J., Freedman, M.J., Sander, T., Shostack, A.: Economic barriers to the deployment of existing privacy technologies (position paper). In: Proceedings of the Workshop on Economics of Information Security (2002)
63. McNulty, S.: The Google+ Guide: Circles, Photos, and Hangouts. Peachpit Press (2012)
64. Beato, F., Kohlweiss, M., Wouters, K.: Enforcing Access Control in Social Network Sites. In: Procedings of Hot Topics in Privacy Enhancing Technologies, HotPETS (2009)
65. Lwin, M., Wirtz, J., Williams, J.D.: Consumer online privacy concerns and responses: a power–responsibility equilibrium perspective. Journal of the Academy of Marketing Science 35, 572–585 (2007)
66. Bonneau, J., Preibusch, S.: The Privacy Jungle: On the Market for Data Protection in Social Networks. In: Economics of Information Security and Privacy, pp. 121–167. Springer, US (2010)
67. Zhao, H., He, M.: Study on Social Culturology of the 'Internet Sharer'. In: Proceedings of the 1st IEEE Symposium on Web Society, pp. 219–224. IEEE (2009)
68. Cho, H., Rivera-Sánchez, M., Lim, S.S.: A multinational study on online privacy: global concerns and local responses. New Media & Society 11(3), 395–416 (2009)