2020

The Effect of Privacy Policies on Information Sharing Behavior on Social Networks: A Systematic Literature Review

Damion Mitchell
Dakota State University

Omar F. El-Gayar
Dakota State University

Recommended Citation

Mitchell, D., & El-Gayar, O. (2020, January). The effect of privacy policies on information sharing behavior on social networks: A Systematic Literature Review. In Proceedings of the 53rd Hawaii International Conference on System Sciences.

The effect of privacy policies on information sharing behavior on social networks: A Systematic Literature Review

Damion Mitchell
Dakota State University
damion.mitchell@trojans.dsu.edu

Omar El-Gayar
Dakota State University
omar.el-gayar@dsu.edu

Abstract

Online social networks (OSN) such as Facebook and Instagram have dramatically changed the way people operate. It however raises specific privacy concerns due to their inherent handling of personal data. The paper highlights the privacy concerns associated with OSN, strategies to protect the users' privacy, and finally the overall effect of privacy policies on information sharing behavior on OSN. In a systematic review, we examined 51 full papers that explore privacy concerns in OSN, strategies to protect users' privacy, and the effects of privacy policies on the users' information sharing behavior. The overall findings disclosed that users are concerned about their identity being stolen, and how third-party applications use their information. However, privacy policies do not have a direct impact on the information sharing behavior of OSN users. The findings help researchers and practitioners better understand the impact of privacy concerns on users' information sharing behavior on OSN.

Keywords – Privacy Concerns; Privacy Policies; Online Social Networks; Information Sharing; User Behavior.

1. Introduction

Online Social Networks (OSN) such as Facebook, Instagram, Twitter, and LinkedIn all play an important role in the lives of many daily. Boyd & Ellison [17] defined an OSN as a web-based service that allows individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system.

Beyond the usual vulnerabilities that threaten any distributed application over the Internet, online social networks raise specific privacy concerns due to their inherent handling of personal data [1]. Social network penetration worldwide is ever-increasing. In 2021, it is projected that there will be about 3.02 billion social media users[1]. This expansion will have a direct impact on the privacy and trust exhibited by users of these systems.

According to [2] the importance of social media not only lies in its role as a new kind of entertainment, but also in its role as a new information sharing and dissemination platform. It was further postulated that there is a plethora of challenges associated with the information sharing process, as on one hand, when people freely share personal information on for example Facebook, information privacy and data security emerge as a major concern for individual users. Therefore, more innovative and effective privacy policies and data protection mechanisms are needed to protect individuals' personal or public information shared in OSN platforms. Despite significant privacy concerns, OSN users continue to disclose private information online. This behavior is described by [3] and [4] as the privacy paradox, in which despite expressing concerns about online privacy, people do very little to protect themselves.

This privacy-compromising approach eventually results in a dichotomy between privacy attitude and actual behavior [5]. Other researchers have discovered a contradiction between privacy concerns users express and their disclosure of personal information on OSNs [6, 7, 8]. Furthermore, while an intention to limit data disclosure exists, actual disclosure often significantly exceeds intention [9]. Varian intimated that the notion of privacy calculus considers the value placed on certain pieces of personal information which are relinquished in exchange for promotional items, while other information which are considered more valuable are retained and protected [10].

In this research paper, we perform a systematic literature review to investigate the effect of privacy policies on information sharing behavior of OSN users. This systematic literature review seeks to explore, and present varying privacy concerns associated with OSN to identify areas of focus and highlight areas deserving of additional attention. In addition, the review seeks to explore the effects of these policies on the information

[1] *https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users*

URI: https://hdl.handle.net/10125/64259
978-0-9981331-3-3

sharing behavior of these users. Table 1 lists the research questions.

The succeeding section provides a background while section 3 describes the research methodology. Section 4 presents the results. Section 5 provides a discussion of findings and implications for future research, while Section 6 concludes this research.

Table 1. Research Questions and Explanation.

#	Research Questions	Explanation
RQ1	What are the privacy concerns associated with OSN users?	The intent of this question is to uncover the varying privacy concerns as expressed by users of OSN through a comprehensive literature review.
RQ2	What are some strategies based on the literature to protect users' privacy?	This question aims to determine different strategies which are either used or recommended to address the concerns from R1.
RQ3	What are the effects of privacy policies on users' behavior to information sharing?	This question seeks to understand how OSN users' information sharing behavior are affected by different privacy policies.

2. Background and Motivation

It was posited by [11] that a systematic literature review may be done for a variety of reasons, such as providing a theoretical background for subsequent research or answering practical questions by perusing existing research to gain insight on the matter under investigation. The advantage of this review is that, areas which have been covered along with proposed tools are discovered and can be used to shape future research. Additionally, this systematic literature review study provides an overall review for users in regard to privacy concerns in OSN, associated tools and strategies to minimize these concerns, in addition to the effects of privacy policies on information sharing behavior of OSN users. These users must understand the associated risks and solutions, while researchers need to know what further issues need to be investigated.

2.1 Privacy Definition

Bünnig and Cap [12] describe privacy as protecting personal information from being misused by malicious entities and allowing certain authorised entities to access that personal information by making it visible to them. While, Ni et al. [13] define privacy as a set of policies that force the system to protect private information.

2.1 Privacy Classifications

A distinction is made between two types of privacy by [14] which includes protecting users from exceedingly powerful Social Network Sites (SNS), and from other SNS users. Figure 2 summarizes the symbiotic relationships that exist between the users and service providers, and their implications on privacy. The authors posit that the service providers' goal is to sell services based on the personal data of their users, while users are concerned about the disclosure of personal data to these service providers. However, the users rely on the functionality of the service provider to manage their social identities. In other words, they are dependent on the functions available to control the visibility of shared items to protect their privacy from other users.

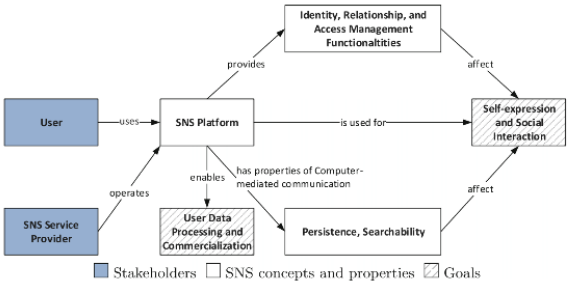

Figure 2. Relation between SNS stakeholders, their goals, and core concepts [14]

3. Research Methodology

A systematic literature review methodology [15] was incorporated to ascertain peer reviewed articles from electronic databases which presented artifacts that examined the privacy concerns associated with OSN users, and the effects of privacy policies on the users' information sharing behavior. A systematic review attempts to collate all empirical evidence that fits pre-specified eligibility criteria to answer a specific research question. It uses explicit, systematic methods that are selected with a view to minimizing bias, thus providing reliable findings from which conclusions can be drawn and decisions made [16]. Figure 3 provides details on the research process adopted in this study. The primary studies were examined from the designated databases, which are presented in the next section. The studies were recognized by applying inclusion and exclusion criteria. The data extraction was accomplished, and synthesis done. Finally, findings are provided to address research questions.

3.1. Search Strategy

Search query. We used different combinations of search strings *["privacy concerns" AND "privacy policies" AND "information sharing" AND ("online social networks" OR OSN OR social media OR social networking sites OR SNS)]* to find the primary studies. The search was performed using these queries, after which, a comparison was made on the initial results. The string combination that brought relevant and maximum results was utilized. Search strings that included behavioral pattern did not result in ample results as many of the papers did not mention the word behavior.

Time Period. The time period selected for this research was from 2006 to 2018. This period was selected as most of the work that deals with OSN occurred after 2005, as verified from the databases searched.

Selection of the Electronic Databases. To find primary studies, five databases were selected that include: ACM Digital Library, IEEExplore, AIS, Web of Science and ABI/Inform. These databases were selected because they are reliable and the studies published are peer reviewed, which provides a quality check of primary studies. In addition, they represent some of the leading search platforms used by Information Systems researchers, as such all results that appeared in these databases were considered.

Selection of Primary Studies. The studies were selected according to the inclusion and exclusion criteria outlined in **Table 2.**

Table 2. Inclusion and Exclusion Conditions Used**.**

Criteria	Conditions
Inclusion	Search strings should appear in title or abstract of the paper The language of the paper must be English The paper should discuss the behavior of OSN users towards their privacy Full-Text Papers
Exclusion	Poster presentations, books, conference panels and summaries, and research in progress papers. Papers published on unrelated topics such as crime, politics etc.

4. Results

The search was conducted on the selected databases by using the final search string on titles and abstracts of primary studies. The results obtained from each database are shown in **Table 3.**

Table 3. Numbers of papers found from primary sources

Database	# of Papers Found	Studies Selected	Studies Included
ACM Digital Library	152	37	14
IEEExplore	81	21	2
AIS	114	28	12
Web of Science	228	52	11
ABI/Inform	221	41	12
Total	**796**	**179**	**51**

The selection of primary studies was carried out by the following four distinct steps presented in Figure 3.

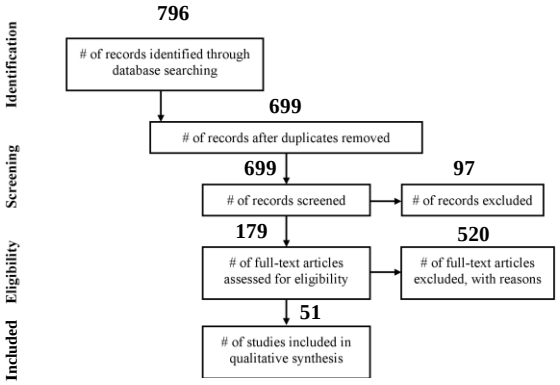

Figure 3. Flow of information through the different phases of a systematic review.

Step 1: Identification: We identified 796 studies that contained search string in their titles or abstracts. The criteria that the search string must appear in the title or abstract was followed strictly.

Step 2: Screening: The papers identified in the first phase were screened to remove duplications that excluded 97 studies. The exclusion criterion was applied on 796 papers that reduced the total count to 699 papers. At this point, we excluded papers that came under the category of extended abstracts, keynotes, and papers in other languages, such as Spanish and French.

Step 3: Eligibility: In this phase, the titles and abstracts of 699 papers were analysed to determine their relevance that made us exclude 520 papers. A total count of 179 studies comprises the final phase.

Step 4: Inclusion: We examine the full text of 179 studies to identify papers related to user behavior and privacy concerns in OSN. By applying the inclusion criteria, 51 papers were selected for full-text scanning.

Overall an analysis was done to unearth patterns to identify gaps and make recommendations for future research.

The results of the systematic literature review are presented below for each research question.

4.1. RQ1: What are the privacy concerns associated with OSN users?

Social networks can be described as web applications that allow users to create their semi-public profile [17], i.e., a profile that some information is public, and some is private, interact with friends, and build an online community. The increased popularity and use of OSNs have changed many individuals' lives in terms of how they work, form, and build social relations. This increase use has presented several concerns, paramount of which is that of privacy.

The concept of privacy is not new, but with the pervasiveness of OSN, the main privacy concerns revealed in the literature are shown in Figure 4**.** Privacy is of vital significance in OSNs, since the illegal revelation and improper use of users' private information can cause undesirable effects in people's lives. OSNs can capture, store, aggregate, redistribute, and use the personal data of individuals. According to [18] the problem is that the owner of this information is often unaware of, or at least unconnected to, its storage and utilization, and that such ubiquitous data collection is harmful to personal privacy.

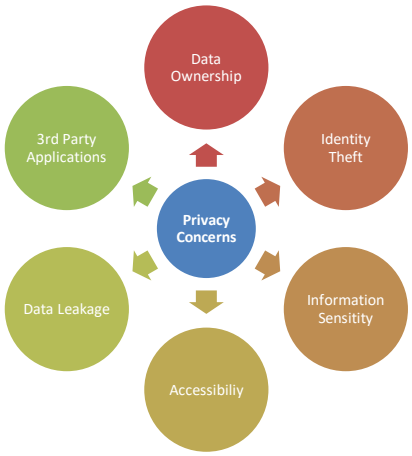

Figure 4. Main privacy concerns associated with OSN users

Privacy can be viewed from the standpoint of control. Whether it is control over personal data, the choice to disclose data, the physical presence of others, the number of others present in disclosure, or choosing which person to discuss and share issues with. Therefore, control is central to maintaining privacy. One of the privacy issues in social networks is the abuse and the leakage of profile and personal information of the users [19]. For example, [20] examined thirteen (13) online Social Network Sites, and it was discovered that each site leaked private information to tracking sites and to some third-party applications. Several studies [6, 21, 22] argue that users place themselves at greater risk for cyber stalking, identity theft, and surveillance when they disclose personal information on OSN. It was further opined by Zhang and his colleagues [23], that of import, is the need to have unauthorized entities detached from multiple private data files, as this may cause leak of useful information.

Another issue related to privacy is because many OSN provide an Application Programming Interface (API) for third-party developers to create applications that can be used on their platform. These third-party applications can track social network users' activities or allow advertisement partners to access and collect social network users' data for commercial and advertising purposes [24]. Prior work has reported that even though third-party applications are widely used for nonthreatening purposes, they are oftentimes exploited by attackers to compromise many accounts for despicable purposes such as propagating spam and malware on OSNs [25, 26, 27, 28].

Information sensitivity and their disclosure also represent a major concern for OSN users [29, 30, 31]. The level of privacy concern depends on the type of requested information [32]. Studies have shown that users show more concern regarding requests for information concerning medical records, social security numbers and questions about media habits compared with less sensitive information [33]. Yang and Wang postulated that when the sensitivity level of requested information is high, users' privacy concerns and behavioral intentions are impacted [32].

Furthermore, users are generally concerned about their privacy with the prevalence of identity theft [29, 34, 35], which is the most reported concern from OSN users. Identity theft is a type of attack on OSNs in which the adversary attempts to collect personal information of OSN users so that he can impersonate the victim of the attack [36]. It was further explained by [36] that this type of attack to OSNs may originate from both inside and outside the network.

4.2. RQ2: What are some strategies based on literature to protect users' privacy?

Privacy protection strategies (Figure 5) are the techniques with which individuals safeguard their information and mitigate potential privacy breaches.

There have been several studies done to better understand what strategies can be employed by OSN users to safeguard their information privacy. Some researchers have examined technologies such as anonymizers, URLs blocker, and web cookie managers [37] and their impact on protecting OSN users' privacy. Another strategy that has been used by OSNs providers is that of privacy setting function such as coarse-grained

access control [38]. In addition, mechanisms to facilitate robust authentication and encryption as also widely used [39]. It was presented by [40] that in some instance aspects of the users' profile can be encrypted using public key cryptography. Also, cryptography has been used to also protect users' information from the inquisitive eyes of the service providers [40, 41, 42, 43]. From the users' standpoint, [44] found that the most common strategy mentioned was that of firewalls and antivirus software.

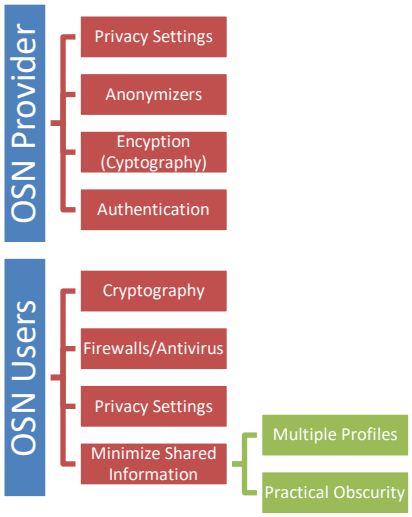

Figure 5. Strategies used to protect privacy of OSN users.

It was further shown that some users sought to limit the amount of information shared, and in other instances using the privacy settings provided by the OSN providers. Other users take more drastic measures such as frequent deactivation of accounts or constantly deleting comments which have already been read or use coded languages so that only a portion of one's network understands the messages [45, 46]. It was further opined by [47] that some users maintain more than one profiles on a single site to manage boundaries in their lives, while others create profiles that are not completely concealed, but difficult to locate. Overall, the strategies employed by OSN users may include filtering, ignoring, using pseudonym for blocking purposes, or withdrawal [48].

4.3. RQ3: What are the effects of privacy policies on user's behavior to information sharing?

As enunciated by [49] privacy policies which are stated by the service provider are intended to convey to the users, information on how their personal data will be protected. Information sharing is of paramount importance for many individuals who decide to join OSNs. It has been of great interest to researchers who have been studying the effects of privacy policies on user's behavior to information sharing. It was postulated by [50] that users will express very strong concerns about privacy of their personal information but be less than vigilant about safeguarding it. According to [51], OSN information sharing behavior has two dimensions: The first dimension is sharing regularity which is related to the frequency of the information sharing behavior. The second dimension is sharing density which is related to the level of online private information revelation. Four classifications of user behavior in ONS which are depicted in Figure 6 were presented by [52]. These include social investigation, social affiliation, and frequency of use, and information control which is provided through privacy interface features. In a longitudinal study by [53] it was revealed that higher OSN usage led to more self-disclosure.

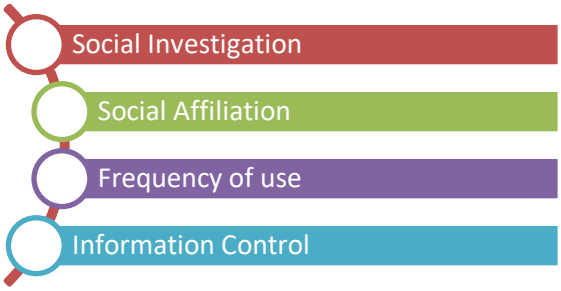

Figure 6. Classification of User Behavior in OSNs.

Moreover, several studies find support for a dichotomy between stated privacy concerns and the actual behavioral response [5, 6, 47]. It was [35] who showed that generally speaking, users will reduce the amount of information disclosed in response to their privacy concerns. According to an interesting finding by [54], when releasing personal information, the users tend to use an all-or-nothing approach, this means their personal information either is restricted to "only friend" or remains completely open to the public. Social influence and online trust increased online self-disclosure whilst privacy risk belief decreased self-disclosure [55]. Other research studies on OSN have identified that user perceptions of self-anonymity lower individuals' privacy concerns which, in turn, affects self-disclosure [56]. It is apparent that when OSN users are knowledgeable about the use of their personal information, they are more likely to disclose personal information.

5. Discussions

In this section we discuss the results of the three stated research questions.

5.1 Privacy Concerns

For RQ1, the review identified different privacy concerns associated with OSN users. The most popular

concerns were that of identity theft and the users not knowing what third-party applications are doing with their information. The major concerns outlined were found to be consistent across the different sources. It was apparent that OSN users are generally more perturbed about their identity being stolen compared to the fear of what third-party applications are doing with their data. There was no one study that examined whether these concerns exist across age groups. It was very interesting that users' privacy concerns and behavioral intentions are impacted greatly, especially when the sensitivity level of the information being requested in high.

5.2 Privacy Preserving Strategies

In terms of RQ2, several strategies have been employed both at the system providers' level and the user level to protect users' privacy. One of the main approaches used at the providers' level is that of robust encryption and authentication. This is normally supplemented by associated privacy settings. In the context of the users, outside of adjusting the provided privacy settings manager, many opt to minimize the information shared on these platforms to protect their privacy. Even though users are most times aware of the associated privacy settings on these OSNs, they do not review them or are reluctant to modify them to suit their needs.

5.3 Effects of Privacy Policies on Users' Behavior

RQ3 examined the effects of privacy policies on user's behavior to information sharing. It was obvious that when users are conversant with the privacy policies and especially how their information will be shared, the disclosure of personal information was more likely. However, while behavior cannot be measured directly, activities performed by OSN users can certainly determine users' behavior in terms of their information sharing habits. Therefore, based on our findings, privacy policies do not have a direct impact on the information sharing behavior of OSN users. In addition, users generally do not read these sometimes-laborious policies, and this ignorance impact their behavior on OSN. The findings show the major issue related to the privacy paradox, whereby users even though are concerned about their privacy do nothing to address those concerns. Several studies highlighted this paradoxical behavior amongst OSN users.

5.4 Internal/External Validity

Internal validity is generally considered a main threat in a systematic literature review, as it is a form of secondary study, which does not involve human participation. To militate against this internal validity, all studies that contained the search strings were considered; for optimum search coverage, five main databases were used, with cross referencing done on Google Scholar. Furthermore, Construct validity could also have been an issue, but by following the well-established guidelines provided by [5] this threat was mitigated.

6. Conclusion

The purpose of this study was to conduct a systematic literature review to explore the effects of privacy policies on the information sharing behavior of OSN users. OSNs play an important role in the lives of many daily; with it comes specific privacy concerns due primarily to the inherent way in which personal data are handled. Due to the plethora of privacy concerns, several strategies such as anonymizers, privacy setting managers, authentication, encryption and minimal information sharing have been implemented or employed to militate against these concerns. Privacy policies do not have a direct effect on the information sharing behavior of OSN users. The study contributes to extant knowledge by systematically analysing evidence from literature and providing a view on the privacy concerns, strategies, and effects of these policies on OSN users' information sharing behavior. The research community may build on the results of this study to investigate other factors relating to privacy concerns such as age, gender, and culture. The findings may offer OSN providers a fulsome understanding of how privacy concern among users can affect usage of these OSN. Also, the review may help practitioners in suggesting further privacy preserving improvements to OSN providers. In addition, this study can help academic institutions and other organizations to better understand and educate their stakeholders on how to minimize and alleviate varying privacy concerns within their context.

7. Future Works

There are several areas about privacy concern and the effects of privacy policies on users' behavior that warrant further investigation. First, studies can be advanced in seeking to answer the question of how privacy-preserving applications be used by OSN users. Second, an examination on how online purchase decision of users can be used as a measure of their privacy protection behavior. Third, understanding users' attitude toward privacy and the contributing factors that motivate them to share information on these OSN platforms must be further examined. Four, an exploration of the role of behavioral change and its potential to understand and devise mechanisms to address the privacy paradox might prove important. Five, this study presented several privacy preserving strategies. However, a good starting point for discussion and further research would be to examine the correlation between different strategies and

the general privacy concerns exhibited by users. Sixth, this study can be expanded to include a quantitative literature review on privacy concerns using meta-analysis. Finally, longitudinal studies can be done to examine the individual user's privacy concern over time. This may offer valuable understandings into the dynamic nature of privacy concern and the effects of privacy policies on the users' behavior.

8. References

[1] L. Cutillo, R. Molva and T. Strufe, "Privacy Preserving Social Networking through Decentralization," in Proc of 6th International Conference on Wireless On demand Network Systems and Services, Feb 2009, pp. 145-152.

[2] Jin, X. (n.d.). Information Sharing in the Era of Social Media. Retrieved from https://jyx.jyu.fi/bitstream/handle/123456789/50876/9789513967116.pdf?sequence=1

[3] Barnes, S.B., 2006. A privacy paradox: Social networking in the United States. First Monday, 11(9). Retrieved from http://firstmonday.org/article/view/1394/1312.

[4] P.A. Norberg, D.R. Horne, D.A. Horne The privacy paradox: personal information disclosure intentions versus behavior J. Consum. Affairs, 41 (1) (2007), pp. 100-126

[5] Acquisti, A., 2004. Privacy in electronic commerce and the economics of immediate gratification. In: EC '04 Proceedings of the 5th ACM Conference on Electronic Commerce, USA, 21-29.

[6] Tufekci, Z. 2008. Can you see me now? Audience and disclosure regulation in online social network sites. Bulletin of Science, Technology and Society. 28, 20 (2008), 20-36.

[7] Gross, R. and Acquiti, A. 2005. Information revelation and privacy in online social networks. In Proceedings of the 2005 ACM workshop on privacy in the electronic society

[8] Govani, T. and Pashley, H. 2005. Student awareness of the privacy implications when using Facebook. Paper presented at the Privacy Poster Fair at Carnegie Mellon University School of Library and Information Science (December 14, 2005). http://lorrie.cranor.org/courses/fa05/tubzhlp.pdf

[10] Varian, Hal R. Economic Aspects of Personal Privacy. Internet Policy and Economics: Challenges and Perspectives. 2009, pp. 101-09. 101-109. Dordrecht and New York: Springer, 0, 2009.

[11] Okoli, C. and Schabram, K. (2010), "A guide to conducting a systematic literature review of information systems research", Sprouts: Working Papers on Information Systems, Vol. 10 No. 26, pp. 1-49

[12] Bunnig, C.; Cap, C.H., "Ad Hoc Privacy Management in Ubiquitous Computing Environments," Advances in Human-oriented and Personalized Mechanisms, Technologies, and Services, 2009. CENTRIC '09. Second International Conference pp.85, 90, 20-25 Sept. 2009.

[13] Ni, Q., Bertino, E., Lobo, J., Brodie, C., Karat, C. M., Karat, J. & Trombeta, A. 2010. "Privacy-aware role-based access control," ACM Transactions on Information and System Security (TISSEC), 13, 24.

[14] Netter, M.: Privacy-preserving Infrastructure for Social Identity Management. Ph.D. thesis, University of Regensburg (2013)

[15] Liberati, A., Altman, D. G., Tetzlaff, J., Mulrow, C., Gøtzsche, P. C., Ioannidis, J. P., … Moher, D. (2009). The PRISMA Statement for Reporting Systematic Reviews and Meta-Analyses of Studies That Evaluate Health Care Interventions: Explanation and Elaboration.

[16] Oxman AD, Guyatt GH (1993). The science of reviewing research. Ann NY Acad Sci 703: 125–133. Discussion 133–124

[17] D. M. Boyd and N. B. Ellison, "Social Network Sites: Definition, History, and Scholarship," J. Computer-Mediated Communication, vol. 13, no. 1, pp. 210–30. http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html, Oct. 2007.

[18] D. J. Houghtona and A. N. Joinsona, Privacy, Social Network Sites, and Social Relations, Journal of Technology in Human Services, Volume 28, pages 74-94, Issue 1-2, 2010. doi:10.1080/15228831003770775

[19] M. Ladan, Social Networks: Privacy Issues and Precautions, ICDS 2015: The Ninth International Conference on Digital Society, 2015.

[20] Krishnamurthy, B. and Wills, C. E. 2010. On the leakage of personally identifiable information via online social networks. ACM SIGCOMM Computer Communications Review, Jan. 2010.

[21] Acquisti, A. and Gross. R. 2006. Imagined Communities: Awareness, Information Sharing and Privacy on The Facebook. In Proceedings of the 6th Workshop on Privacy Enhancing Technologies, Cambridge, UK, 2006.

[22] Mohamed. A. 2010. Online Privacy Concerns Among Social Networks' Users. Cross-Cultural Communication., 6(4), 74-89.

[23] C. Zhang, J. Sun, X. Zhu, and Y. Fang, Privacy and Security for Online Social Networks: Challenges and Opportunities, IEEE Network, Vol.24, No.4, pp.13-18, July-August 2010.

[24] Christofides, E., Muise, A., and Desmarais, S. 2012. "Risky Disclosures on Facebook: The Effect of Having a Bad Experience on Online Behavior," Journal of Adolescent Research (27:6), pp. 714–731.

[25] M. Egele, G. Stringhini, C. Kruegel, and G. Vigna. COMPA: Detecting Compromised Accounts on Social Networks. In NDSS, 2013.

[26] J. Song, S. Lee, and J. Kim. CrowdTarget: Target-based Detection of Crowdturfing in Online Social Networks. In ACM CCS, 2015.

[27] G. Stringhini, G. Wang, M. Egele, C. Kruegel, G. Vigna, H. Zheng, and B. Y. Zhao. Follow the Green: Growth and Dynamics in Twitter Follower Markets. In ACM Internet Measurement Conference (IMC), 2013.

[28] K. Thomas, F. Li, C. Grier, and V. Paxson. Consequences of Connectivity: Characterizing Account Hijacking on Twitter. In ACM CCS, 2014.

[29] Nosko, A., Wood, E., and Molema, S. 2010. "All about me: Disclosure in online social networking profiles: The case of FACEBOOK," Computers in Human Behavior (26:3), pp. 406–418.

[30] Wang, Y., Leon, P. G., Norcie, G., Acquisti, A., and Cranor, L. F. 2011a. "' I regretted the minute I pressed share': A Qualitative Study of Regrets on Facebook," Symposium on Usable Privacy and Security 2011, Pittsburgh (USA) (August 2015), pp. 1–16.

[31] Wang, Y., N., Cranor, G., and Faith, L. 2011b. "Who Is Concerned about What? A Study of American, Chinese

and Indian Users' Privacy Concerns on Social Network Sites," Trust and trustworthy computing (10), pp. 146–153.
[32] Yang, S. & Wang, K. (2009). The influence of information sensitivity compensation on privacy concern and behavioral intention. The Database for Advances in Information Systems, 40, 1.
[33] Ward, S., Bridges, K., and Chitty, B. (2005). "Do Incentives Matter? An Examination of On-line Privacy Concerns and Willingness to Provide Personal and Financial Information." Journal of Marketing Communications, Vo. 11, No. 1: pp. 21- 40.
[34] Johnson, M., Egelman, S., and Bellovin, S. M. 2012. "Facebook and privacy: it's complicated," Proceedings of the eighth symposium on usable privacy and security. ACM (Section 2), pp. 1–15.
[35] Krasnova, H., Spiekermann, S., Koroleva, K., and Hildebrand, T. 2010. "Online social networks: why we disclose," Journal of Information Technology (25:2), Palgrave Macmillan, pp. 109– 125
[36] Deliri, S., and Albanese, M. (2015). Security and privacy issues in social networks. DOI: 10.1007/978-3-319-20062-0_10
[37] Turner, E., & Dasgupta, S. (2003). Privacy on the Web: An examination of user concerns, technology, and implications for business organizations and individuals. Information Systems Management, 8–19. Retrieved from http://www.tandfonline.com/doi/abs/10.1201/1078/43203.20.1.20031201/40079.2
[38] Fire, M., Goldschmidt, R. & Elovici, Y. (2014). Online Social Networks: Threats and Solutions. Communications Surveys & Tutorials, IEEE. Volume: PP, Issue: 99. DOI: 10.1109/COMST.2014.2321628
[39] Beye, M., Jeckmans, A.J.P., Erkin, Z., Hartel, P.H., Lagendijk, R.L. & Tang, Q. (2010). Literature overview-privacy in online social networks (2010). Technical Report TR-CTIT-10-36, Centre for Telematics and Information Technology. Retrieved http://eprints.eemcs.utwente.nl/18648/
[40] Lucas, M.M. & Borisov, N. (2008). Flybynight: Mitigating the Privacy Risks of Social Networking. Proceedings of the 7th ACM workshop on Privacy in the electronic society (WPES '08), pp 1–8. ISBN: 978-1-60558-289-4
[41] Anderson, J., Diaz, C., Stajano, F., Leuven, K. U., and Bonneau, J. 2009. "Privacy-Enabling Social Networking over untrusted networks," in WONS: Barcelons, Spain, pp. 2-7.
[42] Guha, S., Tang, K., and Francis, P. 2008. "NOYB: Privacy in Online Social Networks," in Proceedings of the first workshop on online social networks, pp. 49-54.
[43] Starin, D., Baden, R., Bender, A., Spring, N., and Bhattacharjee, B. 2009. "Persona: An Online Social Network with User-Defined Privacy Categories and Subject Descriptors," in SIGCOMM'09: Barcelona, Spain, pp. 135-146.
[44] Paine, C., Reips, U.D., Stieger, S., Joinson, A., & Buchanan, T. (2007). Internet users' perceptions of "privacy concerns" and "privacy actions." International Journal of Human-Computer Studies, 65(6), 526–536. doi:10.1016/j.ijhcs.2006.12.001
[45] Vitak, J., & Kim, J. (2014). "You can't block people offline": examining how facebook's affordances shape the disclosure process. Proceedings of the 17th ACM Conference on Computer
[46] Madden, M. 2012. "Privacy management on social media sites," Pew Research Centre.
[47] Stutzman, F., & Hartzog, W. (2012). Boundary regulation in social media. In Proceedings of the ACM 2012 conference on Computer Supported Cooperative Work (pp. 769–778). Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1566904
[48] Wisniewski, P., Lipford, H., & Wilson, D. (2012). Fighting for My Space: Coping Mechanisms for SNS Boundary Regulation. Proceedings of the 2012 ACM Annual Conference on Human Factors in Computing Systems - CHI '12, 609. doi:10.1145/2207676.2207761
[49] Jianning Geng, Lin Liu, and Barrett R. Bryant. 2010. Towards a personalized privacy management framework. In Proceedings of the 2010 ICSE Workshop on Software Engineering for Secure Systems (SESS '10). ACM, New York, NY, USA, 58-64. doi:http://www.ezproxy.dsu.edu:2107/10.1145/1809100.1809109
[50] Awad, Neveen Farag 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).
[51] Salehan, M., and Kim, D. J. 2012. "The Effect of Attitude, Social Trust and Trust in Social Networking Sites on Two Dimensions of Sharing Behavior," 18th Americas Conference on Information Systems, Seattle, WA, 2012.
[52] Waheed, H., Anjum, M., Rehman, M., & Khawaja, A. (2017). Investigation of user behavior on social networking sites. PLOS ONE, 12(2), e0169693. https://doi.org/10.1371/journal.pone.0169693
[53] Trepte, S. and Reinecke, L. (2013), "The reciprocal effects of social network site use and the disposition for self-disclosure: a longitudinal study", Computers in Human Behavior, Vol. 29 No. 3, pp. 1102-1112.
[54] Strater, K. & Lipford, H.R. (2008). 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, British Computer Society, Interaction-Volume 1 pp. 111-119.
[55] Posey, C., Lowry, P.B., Roberts, T.L. and Ellis, T.S. (2010), "Proposing the online community self-disclosure model: the case of working professionals in France and the UK who use online communities", European Journal of Information Systems, Vol. 19 No. 2, pp. 181-195.
[56] Jiang, Z.J., Heng, C.S. and Choi B.C. (2013), "Research note-privacy concerns and privacy-protective behavior in synchronous online social interactions", Information Systems Research, 24, 3, 579-595.