Denial of Choice: Group Level Disclosure of Private Information

Tharntip Tawnie Chutikulrungsee, Oliver K. Burmeister, Yeslam Al-Saggaf, Maumita Bhattacharya

Denial of Choice: Group Level Disclosure of Private Information

Tharntip Tawnie Chutikulrungsee , Oliver Kisalay Burmeister, Yeslam Al-Saggaf, and Maumita Bhattacharya

School of Computing and Mathematics, Charles Sturt University
{tchutikulrungsee, oburmeister, yalsaggaf, mbhattacharya}@csu.edu.au

Abstract. While online social networks (OSNs) allow users to selectively share content as well as limit access to information within users' own virtual spaces, unfortunately there is little or no control on other-generated content. The full study explores an interdependent privacy regarding other-generated disclosures on OSNs from insiders' perspectives (the 'discloser' and the 'disclosed'), based upon their lived experiences. An online survey was used to recruit suitable participants who meet the purposive sampling criteria. This paper presents some preliminary findings from a current study, based on an online survey. The online survey result reveals a likelihood of activities associated with other-generated disclosure. This study makes a contribution to the scant literature on OSN interdependent privacy as well as draws attention to tackle these privacy issues in order to discover effective detection mechanisms towards practical solutions in the future.

Keywords: Online social networks information privacy • users' privacy • disclosure

1 Introduction

Online privacy is not only a global problem becoming difficult to ignore but also one of the most significant debates in law and moral philosophy, particularly in an era of ubiquitous computing and online social networks (OSNs). One of major privacy issues on OSNs is information disclosures by either users themselves or others during interaction or activities, especially tagging and re-sharing. While managing information we share ourselves is difficult, how to manage information that others share about us is more complicated and challenging. Of particular concern is that there is little or no control on other-generated disclosures, particularly outside users' profiles. For instance, if a user posts a comment in a friend's space, the friend cannot specify which users can view the comment. In another case, when a user uploads a photo and tags friends who appear in the photo, the tagged friends cannot restrict who can see this photo.

Other-generated disclosures lead to privacy issues such as privacy breaches, privacy invasions, privacy violation, privacy infringement, privacy threats, or privacy risks despite existing lengthy privacy policies as well as fine-grained privacy settings. In advanced societies, media have repetitively reported other-generated disclosures on news stories, court cases, and allegations. Some cases of other-generated disclosures can be claimed for legal protection whereas other cases are still under a shadow of the law, which varies differently among countries. A lack of sufficient privacy control and absolute legal protection highlight a need to better understand a privacy interdependence in OSNs and to effectively manage this privacy at a group level.

Although there is considerable research on OSN privacy [1,2,3,4,5,6], the majority tend to view privacy as independent, mostly focus on self-disclosures [3,4], [7,8,9]. So far only a few studies has highlighted a concept of privacy interdependence on OSNs [10,11,12]. Nonetheless, the interdependent privacy regarding other-generated disclosures has yet been unexplored, particularly within the scope of this present study that is based on both insiders' viewpoints and lived experiences. In addition to an attempt to fill the gap in existing literature, this study aims to provide an in-depth understanding of these phenomena in multi-dimensional aspects together with interdependent privacy. This present study is valuable and makes contribution to OSN communities, service providers, organisations, and users. The OSN service providers can gain benefits from this study in terms of technical or operational designs, collaborative privacy management and control among users, as well as privacy policies. In addition, business, organisations, and communities would gain insights into users' privacy concern, influences of other-generated disclosures, and awareness of interdependent privacy to apply those insights in terms of marketing campaign as well as preserving customers' privacy. This study also increases users' awareness and suggests strategies to mitigate risks of these phenomena.

This article presents preliminary findings from a current study on other-generated disclosures and interdependent privacy on Facebook. The next phase in the work, not described in this article, is to gain deeper understanding of these phenomena through a qualitative study, based upon users' lived experiences, from both engaging parties – the 'discloser' and the 'disclosed'. To the best of our knowledge, this is the first study of its kind that explores an interdependent privacy on OSNs in multi-dimensional aspects ranging from motivations, perceptions, types of disclosed contents, actions as well as effects on both online and offline relationships.

The remainder of the paper is organised as follows: Section 2 presents an overview of some of the key concepts associated with privacy and disclosures on OSNs, along with related literature. Section 3 presents the methodology and Section 4 describes the findings, limitations and future directions of the study. Finally, conclusions are drawn in Section 5.

2 Background and Literature

Boyd and Ellison [13] initially defined the term “social network sites” as web-based services that allow users to 1) create a public or semi-public profile, 2) articu-late the list of connected users, 3) view and traverse lists of connection within the system. Nonetheless, a variety of terms are used interchangeably in public such as social networking sites, online social networks (OSNs), social media, and social webs. However, Boyd and Ellison [13] argued that the term “social networking sites” is improper for OSNs’ emphasis and scope.

OSNs like Facebook, Google+, Twitter, and Instagram have attracted billions of users worldwide and become increasingly embedded in daily life activities, especially in the evolution of smartphones. So far, Facebook is the largest and the most popular SNSs of 1.04 billion daily active users worldwide whereas 934 million mobile daily active users on average for December 2015, where a majority of our daily active users (83.6%) are outside the US and Canada [39].

An upsurge in OSN users and its popularity is owing to OSN distinction in multi-functional all-in-one platforms offering users with abilities to generate, publish, comment, share, or distribute rich content as well as interact to a large audiences worldwide with free-of-charge. Accordingly, OSNs have become a large resource of free information that can be easily accessed, leaped, crawled, inferred, or misused at any time. This results in crafting a big hole in privacy and security.

Online privacy is a challenging issue of great interest across communities including OSN service providers, users, and scholars. Privacy has been dealt with in many contexts, including how to technically achieve it [14], breaches of information privacy [15], how users value privacy in online contexts [16, 17], and how to define professional responses that cater to all stakeholders, including to their respective privacy requirements [43,44,45,46]. To date, privacy on OSNs has been studied extensively not only from technical aspects [6], [11], [18,19,20,21] such as privacy-by-design, privacy management, and privacy control, but also from social aspects [3], [5], [12], [22] such as users’ behaviors, privacy concerns, and privacy attitudes. Several studies also point out a flaw in existing privacy policies as well as privacy settings [23,24,25,26,27]. Despite restrictive privacy settings, privacy conflicts can still arise when there is a difference in privacy practices or privacy management, especially in interconnected and dependent environments like OSNs.

Furthermore, OSNs have continuously updated privacy policies, often changed privacy settings, consistently developed and implemented new features, as well as accepted third-party applications. These on-going changes lead to other privacy-related issues and increase in privacy concerns. Alternatively, many works have denoted users’ privacy concern [5], [12], [28], [29] and discussed privacy-related issues [21], [30,31,32]. New privacy challenges are inevitable with the growth of ever-changing OSNs, which privacy is interdependent.

2.1 Privacy Interdependence

In such interconnected environments like OSNs, privacy is a complicated matter than just an individual importance. Privacy of individual users is bounded to activities by others and their behaviors, rather than just each user. This privacy interdependence affects not only users but also non-users. The term “interdependent privacy” was first coined in the study of Facebook gaming permission by Bicz´ok and Chia [10]. Other contexts of interdependent privacy are associated with as third-party applications, re-sharing content, tagging, or joining groups.

Interdependent privacy is not relatively new and has been inherent in OSNs. However, extensive studies have considered OSN privacy as independent, concerning at an individual level [3], [4], [7,8,9] whereas interdependent privacy is required more attention. To date, relatively limited research on interdependent privacy exists [6], [10], [33], particularly with respect to third-party applications. For example, Wang et al. [34] pointed out that installing a third-party application on Facebook like calendar would violate user’s global privacy settings and friends’ privacy. In similar line, Ahmadinejad and Fong [19] revealed that third-party applications can jeopardize a large number of users through Application Programming Interface (API) attacks with high success rate. The attacks can reveal information on users’ profiles as well as infer other information. Likewise, Heatherly et al. [6] reported that both political and religious affiliation could be inferred from others’ information available on OSNs, even when users are unwilling to disclose such information. Moreover, Ryu et al. [35] demonstrated that analysing link structures can extract the hidden attributes and reveal sensitive information. They also proposed three algorithms to detect privacy breaches from attribute inference, based on friendship links and group memberships.

Our work is different from those mentioned above as we has focused on another context of interdependent privacy. Despite users’ purposes and intentions, users may disclose not only their own information but also information about others through their online activities. Disclosures of information pose both information privacy and personal privacy at risks. While self-disclosures can be inhibited, disclosing information by others is beyond individual control.

2.2 Other-generated Disclosure

Other-generated disclosures, which reveal about others without consent, are not uncommon on OSN wall posts, comments, videos, links, and photos. These phenomena can be seen in forms of sharing on-behalf, sharing co-owned content, sharing multiple-owned content, re-sharing content, distributing, or tagging. The most trending other-generated disclosures deal with photo sharing on OSNs; for example, parents post or share photos of their children.

Other-generated disclosures can occur not only in one-hop relationships or multi-hop relationships, but also within same or different platforms. ‘Disclosers’ is users who disclose content such as friends, friend-of-friends, friend-of-friend-of-friends, or strangers whereas ‘Disclosed’ can be users or non-users.

Some cases of other-generated disclosure can be claimed for legal protection or compensation under privacy laws, depending on counties. For instance, Mr Madill downloaded 83 pictures of a nine-year-old girl from his friend's Facebook and then re-posted those pictures to a Russian child porn web site [40].

Unfortunately, not all privacy-related issues respecting other-generated disclosures can be legally protected. Some cases are still beyond current scopes of legislation or in shadow of existing regulations such as "digital kidnapping".

Digital kidnapping is a pervasive privacy issue in the era of OSNs as well as a recent trending phenomenon, widely reported since 2014. As of 4 August 2015, news reported that hashtags involving digital kidnapping (#babyrp, #babyrpl, #adoptionrp, or #orphanrp) had yielded 57,000 results on Instagram [41]. This new phenomenon of "baby role play" [42] occurs when someone steals a child's photo available on OSNs, then posts that stolen photo on other websites for role-playing. In general, female digital kidnappers use the stolen photo to show others as if the child belongs to them. Nevertheless, some cases of digital kidnapping are much disturbing in communities when digital kidnappers use the stolen photos in sexual and abusive role-playing. Digital kidnapping is not a crime although it can lead to kidnapping in the real world where the worst case scenarios may cause harm to a child's life.

So far, research examining other-generated disclosures has been under-represented in the OSN privacy literature. Yet, no work has addressed an interdependent privacy with regards to other-generated disclosures in the similar context of this present study. The scope of this study is considered within current privacy management and existing tools at the stage of this study.

Not only can other-generated disclosures cause privacy turbulence, but it also affects impression formation as well as desired self-image. Face threats refer to "an incident or behavior that could create an impression inconsistent with one's desired self-image"[1], making people vulnerable and leading to awkwardness, embarrassment, or relationship breakdown. Recently, relatively few studies have focused on face-threatening from other-generated disclosures [36], [38]. While Litt et al. [38] focused on users' experiences and feelings towards face threats, Wohn and Spottwoods [36] were interested in users' strategies in response to face threats. In this case, Litt et al. [38] explored what Facebook users considered be other-generated face threats as well as how Facebook and Internet skills impacts these threats. Based on the survey of 150 Facebook users [38], the result reveals that face threats result from users' neglecting and misunderstanding a target's audience or self-presentation. Furthermore, Wohn and Spottwoods [36] presented four reactive strategies that users used in response to other-generated face threats on Facebook even though some of those strategies can deteriorate relationship between victims and offenders. Along similar line, Litt and Hargittai [37] report that 33.3% of students (online survey sample: N=547) experienced turbulence online whereas those with higher Internet skills are less likely to experience it. In comparison with our study, the similarity lie in an emphasis on other-generated disclosures, a platform of interest (Facebook), and a method (an online survey). However, our study is different in terms of subjects of interest (adult users),

[1] [37] p.187

a method (using semi-structured in-depth interviews in addition to an online survey), and objectives. Our study investigates both engaging parties ('discloser' and 'disclosed') in diverse aspects such as motivations, perceptions, contents, strategies, as well as online and offline impacts, as opposed to only strategies.

3 Methodology

This qualitative study is underpinned upon the interpretivist philosophy and designed using a phenomenology methodology. The purpose of this phenomenological research is to explore other-generated disclosures from users' lived experiences as well as to better understand the essence of the phenomena. To gain insiders' perspectives of the phenomena, the purposive sampling is most appropriate in recruiting suitable participants as per sampling criteria through an online survey.

This present study consists of two phases as shown in Fig. 1. Phase I used an online survey to recruit at least 300 qualified respondents according to the purposive sampling criteria as well as to categorize suitable respondents into two groups – the 'discloser' and the 'disclosed'. The preliminary online survey was launched on SurveyMonkey.com in December 2015. The invitation for an online preliminary survey was advertised on several OSNs including Facebook, LinkedIn, and Twitter. This online survey consists 31 questions, which take approximately 10 minutes to complete. By taking this online survey, there is no obligation for respondents to further participate in the next phase of this study. At this stage, our study is in Phase I.

Phase II uses a semi-structured, in-depth interview to extensively examine multi-dimensional aspects of other-generated disclosures ranging from motivations, perceptions, types of disclosed contents, actions, and impacts on to both online and offline relationships. The chief investigator will send an interviewinvitation, a consent form, and information package via e-mail to suitable respondents according to e-mail given at the end of the online survey (Phase I).

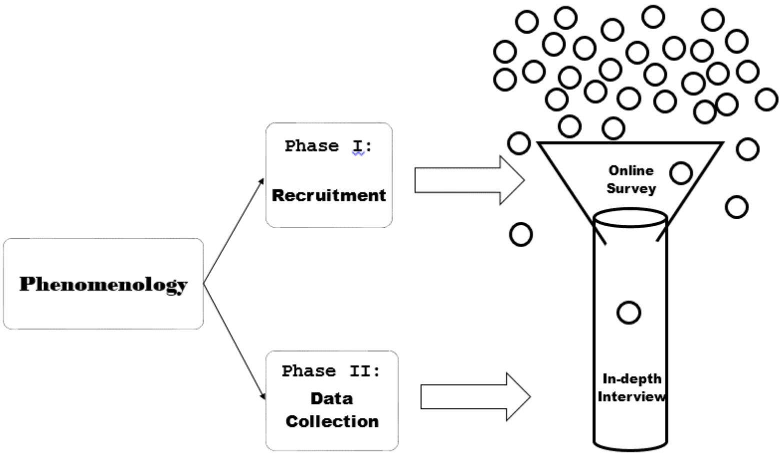

Fig. 1. Overview of research design

3.1 Sampling Criteria and Participants' Characteristics

This phenomenological study examines an OSN interdependent privacy, using Facebook as platform of interest because of its long existing popularity and influences. This present study focuses on adult users, rather than teenagers in many existing studies. The suitable participants must be active Facebook users (age 25-60 years old) for at least two years, have at least 100 Facebook friends, use Facebook (more than twice per week), upload and share photos regularly (at least once a week), make comments (at least once a week), post content (at least once per fortnight).

In the next phase of this current study (Phase II), the chief investigator will send an e-mail to invite qualified survey respondents for each semi-structured in-depth interview. Then data from in-depth interviews will be analysed according to the phenomenological analysis. The results from this phase will reveal multi-dimensional aspects of other-generated disclosure and its privacy, ranging from motivations, perceptions, types of content, actions as well as impacts on users in physical and virtual world.

4 Results and Discussion

At the time of writing, the survey is still being administered and hence only preliminary results are reported here. Currently, there are a total of 166 respondents consisting of Facebook users with a variety of ages and backgrounds. The majority of respondents (92.1%, N=166) are adult Facebook users who are older than 25 years (a group of interest) whereas the minority of respondents (7.83%) are under 25 years old.

There is a growing tendency towards more female (70.73%) than male (29.27%) respondents. A large proportion of respondents reside in Australia (51.2%) and Indonesia (33.73%) whereas the minority live in United States, United Kingdom, China, Brazil, Finland, India, Italy, and Pakistan. Location of respondents revealed: metropolitan (53.61%), rural (34.34%) and remote areas (12.05%).

The majority of respondents are working professionals (67.88%), which meets the sampling criteria for this study. Others are students (24.24%) and 'others' (7.88%), who described themselves as either stay-at-home parents or job seekers. Most respondents (89.02%) have Facebook accounts more than three years whereas some have Facebook accounts between 2-3 years (3.66%) and less than 2 years (7.32%). Accordingly, the first two groups are suitable participants for further in-depth interviews in Phase II as per the sampling criteria. The number of friends that respondents have vary such as 100-200 (16.88%), 201-300 (15.63%), 300 or more (50.63%); subsequently, these three groups are met a sampling criteria in terms of number of friends.

There is more problematic in tags, photos, posts, and comments, rather than videos and links. Respondents often deal with photos and tags on Facebook; 30.1% of respondents asked a Facebook friend to delete a group photo that includes them whereas 79.56% of respondents have tagged photos. While the majority of respondents (99.26%) were tagged on Facebook, 26.47% asked others to remove tags and 25.74%

asked others to remove photos (Table.1). In contrast, 16.65% were asked by other users to remove tags.

Table 1. Number of respondents asked others to remove or delete the following content from others' profile.

Content	Yes	No	Total
Posts	19.85% 27	80.15% 109	136
Comments	19.12% 26	80.88% 110	136
Tags	26.47% 36	73.53% 100	136
Photos	25.74% 35	74.26% 101	136
Videos	15.44% 21	84.56% 115	136

Besides tagging, re-sharing is another most popular activity of other-generated disclosures on Facebook. A description of a term "re-share" is noted on the question that "it means passing on content which is generated by others and shared with you". The majority of respondents re-share other-generated content (Table. 2). While the number of respondents re-sharing posts (84.78%) are almost equal to the number of respondents re-sharing links (85.5%), the remainders re-share photos (75.36%) and video (69.56%).

Table 2. Users' re-sharing activities

Re-share	Yes	No
Posts	117	21
Photos	104	34
Video	96	42
Links	118	20

Other-generated disclosure is beyond individual control when it occurs in another user's profile, rather than own profiles. In this case, users generally have to deal with this phenomenon offline by asking the 'discloser' to remove or delete those content. The number of respondents who have removed or deleted photos (23.53%) are relatively same as the number of respondents who have removed or deleted tags (23.13%), due to a friend's request. Similarly, the number of respondents who have removed or deleted posts (17.78%) are slightly different from the number of respondents who have removed or deleted comments (16.30%), due to a friend's request.

Users have involved in an argument on friends' profiles (34.81%), closed groups (28.89%), and public groups (25.74%) (Fig.2).

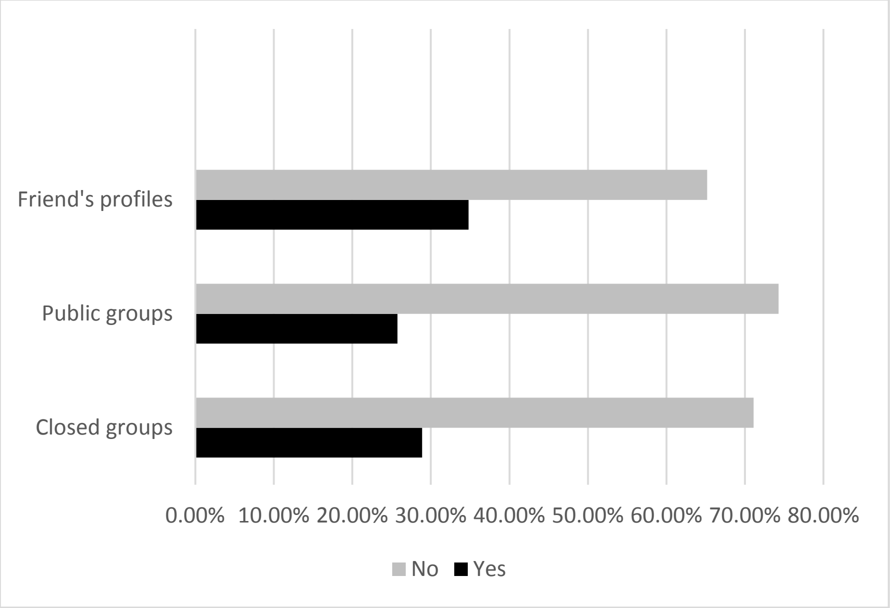

Fig. 2. Number of respondents engage in an argument

The reports from preliminary survey presented here have some limitations. First, the majority of respondents were female, professionals (63.16%), and adult Facebook users. This is expected to diminish as the sample sizes grow. Despite our attempt to have a balance of gender in the final survey results and two groups from purposive sampling, there is a possibility that the derivatives of this purposive sample may yield a disproportion between male and female population. Second, the data sets obtained from this survey were not a complete representation of the general human population, since the ages of participants from both groups are in between 25-60 years. Third, this preliminary online questionnaire involved self-reporting.

The final survey result of this project will engage larger sample size. In the next phase, the qualitative findings from a semi-structured in-depth interview will reveal multi-dimensional aspects of the phenomena from insiders' perspective based upon their lived experiences.

This area of research could also expand beyond behaviors of Facebook users to that of other OSNs such as Twitter, Instagram and Snapchat. So far little attention has focused on other-generated disclosures on OSNs such as Instagram, WhatApps, and Xing.

5 Conclusion

Interdependent privacy on OSNs regarding other-generated disclosures is beyond individual control and in need more attention. As of this writing, no work has yet explored an interdependent privacy regarding other-generated disclosures in the multi-dimensional aspects from OSN insiders' perspectives (the 'discloser' and the 'disclosed'). This paper presents a preliminary results based upon an online survey, which is Phase I in this current study.

Other-generated disclosures on OSNs is an inevitable phenomena, which can occur to either users or non-users. To date, existing studies on privacy management cannot fully resolve these problems as well as current tools are inadequate to mitigate this privacy related issues. New designs of privacy management and policy are in need to protect personal and information privacy. In addition, future detection mechanisms or tools would be helpful to mitigate privacy risks. The preliminary survey findings will increase users' awareness as well as call for scholars' attention to tackle these privacy challenges in the right direction.

5.1 Acknowledgement

We would like to thank Gail Fuller for help in SurveyMonkey and thank survey respondents for their contribution and support to this current study.

References

1. Fodor, M., Brem, A.: Do privacy concerns matter for Millennials? Results from an empirical analysis of Location-Based Services adoption in Germany. Computers in Human Behavior. 53, 344–353 (2015)
2. Patsakis, C., Zigomitros, A., Papageorgiou, A., Galván-López, E.: Distributing privacy policies over multimedia content across multiple online social networks. Computer Networks. 75, 531–543 (2014)
3. Al-Saggaf, Y., Nielsen, S.: Self-disclosure on Facebook among female users and its relationship to feelings of loneliness. Computers in Human Behavior. 36(0) 460–468 (2014)
4. Zlatolas, L. N., Welzer, T., Heričko, M., Hölbl, M.: Privacy antecedents for SNS self-disclosure: The case of Facebook. Computers in Human Behavior. 45, 158–167 (2015)
5. Taddicken, M.: The "Privacy Paradox" in the Social Web: The Impact of Privacy Concerns, Individual Characteristics, and the Perceived Social Relevance on Different Forms of Self-Disclosure. Journal of Computer-Mediated Communication. 19(2), 248–273 (2014)
6. Heatherly, R., Kantarcioglu, M., Thuraisingham, B.: Preventing Private Information Inference Attacks on Social Networks. IEEE Transactions on Knowledge and Data Engineering. 25(8), 1849–1862 (2013)
7. Kwak, K. T., Choi, S. K., Lee, B. G.: SNS flow, SNS self-disclosure and post hoc interpersonal relations change: Focused on Korean Facebook user. Computers in Human Behavior. 31(0), 294–304 (2014)

8. Utz, S.: The function of self-disclosure on social network sites: Not only intimate, but also positive and entertaining self-disclosures increase the feeling of connection. Computers in Human Behavior. 45(0), 1–10 (2015)
9. Chang, C.: Self-construal and Facebook activities: Exploring differences in social interaction orientation. Computers in Human Behavior. 53, 91–101 (2015)
10. Biczók, G., Chia, P. H.:Interdependent Privacy: Let Me Share Your Data. In: Financial Cryptography and Data Security, vol. 7859, pp. 338–353. Springer Berlin Heidelberg (2013)
11. Jin, L., Joshi, J. B. D., Anwar, M.: Mutual-friend based attacks in social network systems. Computers & Security. 37, 15–30 (2013)
12. Chen, J., Ping, J. W., Xu, Y. C., Tan, B. C.: Information Privacy Concern About Peer Disclosure in Online Social Networks. IEEE Transactions on Engineering Management. 62(3), 311–324 (2015)
13. Boyd, D. M., Ellison, N. B.: Social Network Sites: Definition, History, and Scholarship. Journal of Computer-Mediated Communication. 13(1), 210–230 (2007)
14. Burmeister, O. K., Islam, M. Z., Dayhew, M., Crichton, M.: Enhancing client welfare through better communication of private mental health data between rural service providers. Australasian Journal of Information Systems. 19, 1–14 (2015)
15. Bernoth, M., Dietsch, E., Burmeister, O. K., Schwartz, M.: Information Management in Aged Care: Cases of Confidentiality and Elder Abuse. Journal of Business Ethics. 122(3), 453–460 (2014)
16. Burmeister, O. K.: What Seniors Value About Online Community. The Journal of Community Informatics. 8(1), 1–12 (2012)
17. Burmeister, O. K.: Websites for seniors : Cognitive accessibility. International Journal of Emerging Technologies and Society. 8(2), 99–113 (2010)
18. Conti, M., Poovendran, R., Secchiero, M.: FakeBook: Detecting Fake Profiles in On-Line Social Networks. In: Proceedings of the International Conference on Advances in Social Networks Analysis and Mining (ASONAM). pp.1071-1078. IEEE Computer Society (2012)
19. Ahmadinejad, S. H., Fong, P. W.: Unintended disclosure of information: Inference attacks by third-party extensions to Social Network Systems. Computers & Security. 44, 75–91 (2014)
20. Squicciarini, A., Karumanchi, S., Lin, D., DeSisto, N.: Identifying hidden social circles for advanced privacy configuration. Computers & Security. 41(0), 40–51 (2014)
21. Squicciarini, A. C., Xu, H., Zhang, X.: CoPE: Enabling collaborative privacy management in online social networks. Journal of the American Society for Information Science and Technology. 62(3), 521–534 (2011)
22. Acquisti, A., Brandimarte, L., Loewenstein, G.: Privacy and human behavior in the age of information. Science. Science. 347(6221), 509–514 (2015)
23. Liu, Y., Gummadi, K. P., Krishnamurthy, B., Mislove, A.: Analyzing facebook privacy settings: user expectations vs. reality. In: Proceedings of ACM SIGCOMM Conference on Internet measurement conference. ACM, Berlin, Germany (2011)
24. Madejski, M., Johnson, M. L., Bellovin, S. M.: The failure of online social network privacy settings. 1–20 (2011)
25. Masoumzadeh, A., Joshi, J.: Privacy settings in social networking systems: what you cannot control. In Proceedings of the 8th ACM symposium on Information, computer and communications security (SIGSAC). pp. 149-154 (2013).

26. Netter, M., Riesner, M., Weber, M., Pernul, G.: Privacy Settings in Online Social Networks--Preferences, Perception, and Reality. In: Proceedings of the 46th Hawaii International Conference on System Sciences (HICSS). pp. 3219–3228 (2013)
27. Anthonysamy, P., Rashid, A., Greenwood, P.: Do the Privacy Policies Reflect the Privacy Controls on Social Networks? In Privacy, Security, Risk and Trust (PASSAT) and 2011 IEEE Third International Conference on Social Computing (SocialCom). pp. 1155–1158 (2011)
28. Baek, Y. M., Kim, E., Bae, Y.: My privacy is okay, but theirs is endangered: Why comparative optimism matters in online privacy concerns. Computers in Human Behavior. 31, 48–56 (2014)
29. Staddon, J., Huffaker, D., Brown, L., Sedley, A.: Are privacy concerns a turn-off?: engagement and privacy in social networks. In: Proceedings of the 8th Symposium on Usable Privacy and Security (SOUP). pp.1-13. ACM, Washington, D.C. (2012)
30. Parra-Arnau, J., Perego, A., Ferrari, E., Forne, J., Rebollo-Monedero, D.: Privacy-Preserving Enhanced Collaborative Tagging. IEEE Transactions on nowledge and Data Engineering. 26(1), 180–193 (2014)
31. Lang, C., Barton, H.: Just untag it: Exploring the management of undesirable Facebook photos. Computers in Human Behavior 43. 147–155 (2015)
32. Hu, H., Ahn, G.-J., Jorgensen, J.: Detecting and resolving privacy conflicts for collaborative data sharing in online social networks. In: Proceedings of the 27th Annual Computer Security Applications Conference. ACM, Orlando, Florida, USA (2011)
33. Wisniewski, P., Xu, H., Lipford, H., Bello-Ogunu, E.: Facebook apps and tagging: The trade-off between personal privacy and engaging with friends. Journal of the Association for Information Science and Technology. 66(9), 1883–1896 (2015)
34. Wang, N., Xu, H., Grossklags, J.: Third-party apps on Facebook: privacy and the illusion of control. In: Proceedings of the 5th ACM Symposium on Computer Human Interaction for Management of Information Technology (ACM CHIMIT 2011). pp.1-10. ACM, Cambridge, Massachusetts (2011)
35. Ryu, E., Rong, Y., Li, J., Machanavajjhala, A.: curso: protect yourself from curse of attribute inference: a social network privacy-analyzer. In: Proceedings of the ACM SIGMOD Workshop on Databases and Social Networks. pp.13-18. ACM, New York (2013)
36. Wohn, D. Y., Spottswood, E. L.: Reactions to other-generated face threats on Facebook and their relational consequences. Computers in Human Behavior. 57, 187–194 (2016)
37. Litt, E., Hargittai, E.: A bumpy ride on the information superhighway: Exploring turbulence online. Computers in Human Behavior. 36, 520–529 (2014)
38. Litt, E., Spottswood, E., Birnholtz, J., Hancock, J. T., Smith, M. E., Reynolds, L.: Awkward encounters of an “other” kind: collective self-presentation and face threat on facebook. In: Proceedings of the 17th ACM conference on Computer Supported Cooperative Work and Social Computing (CSCW). pp. 449-460. ACM, Baltimore, Maryland, USA (2014)
39. Company Info | Facebook newsroom. February 4, (2004). http://newsroom.fb.com/company-info/ [January 15, 2016]
40. He took the innocence and made it disgusting. February 3, (2015). http://www.news.com.au/technology/online/man-steals-pictures-from-facebook-posts-them-to-child-porn-website/story-fnjwnhzf-1227208112703 [October 29, 2015]
41. Chang, L.: Baby role-play, or virtual kidnapping, is the most disturbing Instagram hashtag ever, http://www.digitaltrends.com/mobile/baby-role-play-virtual-kidnapping/ [August 4, 2015]

42. Beware: Digital kidnappers of children are lurking. March 4, (2015). http://www.kidspot.com.au/could-digital-kidnappers-steal-images-of-your-child/ [January 29, 2016]
43. Burmeister, O.K.: Applying the ACS code of ethics. Journal of Research and Practice in Information Technology. 32(2), 107-120 (2000)
44. Burmeister, O.K. and Weckert, J.: Applying the new software engineering code of ethics to usability engineering: A study of 4 cases. Journal of Information, Communication & Ethics in Society. 3(3), 119-132 (2003)
45. Bowern, M., Burmeister, O., Gotterbarn, D., and Weckert, J.: ICT Integrity: Bringing the ACS Code of Ethics up to date. Australasian Journal of Information Systems. 13(2), 168-181 (2006)
46. Burmeister, O.K.: Achieving the goal of a global computing code of ethics through an international-localisation hybrid. Ethical Space: The International Journal of Communication Ethics. 10(4), 25-32 (2013)