Interdependent Privacy

Chutikulrungsee, Tharntip Tawnie
Charles Sturt University

Burmeister, Oliver Kisalay
Charles Sturt University

Corresponding Author: Tharntip Tawnie Chutikulrungsee,
tchutikulrungsee@csu.edu.au

Abstract

Sharing on online social networks (OSNs) has rapidly emerged as a global phenomenon. Information that users share about one another has great impacts on impression formation, but also poses risks to the privacy of both users and non-users. Particularly, information disclosed by others (other-generated disclosure) is less deceptive and more credible than self-disclosure, challenges one's desired self-presentation as well as self-image, and can cause face threats. So far, privacy literature on OSNs has focused on self-disclosure, and little attention has been paid to other-generated disclosure. Given this growing and increasingly important phenomenon, this present study explores other-generated disclosures, based on the lived experiences of adult Facebook users, to fill this gap. Using an online survey, results shows that Facebook users are likely to be exposed to other-generated disclosure not only through tags and photos but also posts and comments. Posts and comments are increasingly problematic. Not only will this study be useful for service providers in designing new features and improving privacy controls, but it also benefits organisations who take advantage of viral marketing and electronic word of mouth (eWOM), but in ways that seek to preserve the privacy of individuals. Furthermore, this study increases users' privacy awareness and promotes meaningful online privacy practices to preserve not only privacy of individuals, but also privacy of engaging parties, due to the domino effect of interdependent privacy.

Keywords: interdependent privacy, other-generated disclosure, online social networks (OSNs), Facebook

1 Introduction

Sharing on online social networks (OSNs) like Facebook, Instagram, and Twitter has rapidly become a global phenomenon and emerged as a so-called 'new social norm'(Matyszczyk, 2010)). According to Facebook, 510,000 comments are posted, 293,000 statuses are updated, and 136,000 photos are uploaded in every 60 seconds (Facebook, 2017). Additionally, 300 million photos are uploaded per day on Facebook

(Facebook, 2017). As OSNs empower users though self-generated content distributors' capabilities, users perceives additional controls in sharing and interacting to other people; so users reveal not only about themselves but also about others. Many people post a photos taken with family members, friends, peers, mutual friends, and so on, or make comments in Facebook groups. This disclosure pose risks or threats to users' privacy as well as privacy of others. Obviously, privacy on OSNs relies not only on individuals but on others as well (Chutikulrungsee, Burmeister, Al-Saggaf, & Bhattacharya, 2016).

Privacy on OSNs has been extensively studied in the literature ranging from privacy policies, privacy settings, access control, to privacy practices. So far, most considerable research has viewed OSN privacy as independent and controllable within the individual level. However, the concept of an interdependent privacy, which reflects the reality of OSN environments, is disregarded and is an area requiring more attention. Of particular concern is interdependent privacy associated with other-generated disclosure on OSNs.

Other-generated disclosure has a great impact on impression formation, one's desired self-presentation, identity, and personal privacy. Information provided by others, on one hand, is less deceptive and more credible than self-disclosure (Walther, Van Der Heide, Hamel, & Shulman, 2009). Disclosure by others (other-generated disclosure), on another hand, is beyond individual control whereas self-disclosure is within individual control and inhibited. Of special concern is a lack of control over other-generated disclosure, particularly outside users' profiles (Hu, Ahn, & Jorgensen, 2013).

Unfavourable or unpleasant disclosure by others jeopardises personal lives, poses face threats, causes harassment, results in opportunity loss (e.g. jobs, awards), sheds one's negative public image, ruins reputation, and so on. Even though some cases of other-generated disclosure can be claimed for legal protection or compensation under privacy laws, depending on the country involved, the damage has already been incurred and cannot be undone, particularly when content has gone viral on OSNs. For instance, Mr. Madill downloaded 83 pictures of a nine-year-old girl from his friend's Facebook account and then re-posted those pictures to a Russian child porn website ("Man steals pictures from Facebook," 2015).

Yet, not all privacy-related issues respecting other-generated disclosures can be legally protected. Some cases are still beyond the scope of legislation or in the shadow of existing regulations such as digital kidnapping and cyber hijacking. The term 'Digital kidnapping' coined at the end of 2014 is a disturbing trend and a pervasive privacy issue on OSNs in recent years. This phenomenon is known that someone (either 'known' or 'unknown') steals children' photos and re-post those photos on other web sites for the purpose of parental role-playing. Nevertheless, the stolen photos are also exploited in other ways such as sexual or abusive role-playing, and fake identification. The impact of this phenomenon ranges from privacy disturbance and privacy invasion, to privacy threats in terms of identity theft. Evidences from news report reveal that the famous hashtags relating to digital kidnapping, such as #babyrp, #babyrpl, #adoptionrp, or #orphanrp, had yielded 57,000 results on Instagram as of 4 August 2015. For instance, Lindsey Paris found her toddler's photos on a new blog and as if the toddler were that

person's own child (Beck, 2015). Another case involves identity theft - a friend of the victim of digital kidnapping found that victim's photos on Instagram, with derogatory things concerning other Instagram members, so the friend was suspicious that it was not the victim's behaviour. Then they later found that victim's photo on dating websites (McGinty, 2016). Digital kidnapping for role-playing is creepy but not crime; however, it can lead to kidnapping in the real world, which in the worst-case scenarios may cause harm to a child's life.

Collaborative activities, such as co-owned or multi-owned content, also raise a new set of challenges to independent privacy. A decision on sharing or distributing multi-owned content can be made by just one person without a requirement for consensus agreements among co-owners. The lack of collaborative privacy management leads to distribution of content beyond intended audiences or information leakage to the public, regardless of individual awareness. Although perpetual modification offers users more benefits, on-going changes create additional privacy challenges. Particularly, new features and add-on applications entice users to continuously interact as well as frequently share more information not only about themselves but also about others.

The purpose of this present study was to explore interdependent privacy regarding other-generated disclosure in multi-dimensional aspects from insiders, based on lived experiences. In particular, this study examined adult Facebook users (25-70 years old) who have engaged in other-generated disclosures. This present study chose Facebook as a platform of interest because of its popularity, features, fine-grained privacy settings as well as restricted privacy control. This paper is part of a work-in-progress and reports a survey result and a preliminary interview results about Facebook users' experiences in other-generated disclosure.

This study, on one hand, draws attention from all related parties (individual users, organisations, scholars, and OSN service providers) to new privacy challenges on OSNs. On the other hand, this study makes contributions to the scant literature on OSN interdependent privacy, whereby the matter is beyond individual control as well as current privacy settings. First, this study raises users' awareness of privacy interdependence on OSNs. Second, it explores social strategies for handling privacy issues associated with other-generated disclosure. Third, it uncovers kinds of content for future research. Accordingly, it encourages further studies on discovering effective detection mechanisms in addition to preventive strategies to solve these privacy issues.

The remainder of this paper is organized as follows. Section 2 discusses the theoretical foundation for this study and presents relevant literature. Next, section 3 introduces the research method. Then section 4 reports our survey results and discusses the findings. Section 5 later points out limitations and suggests avenues for future research, following the conclusion in section 6.

2 Theoretical Background and Literature

OSNs like Facebook, Google+, and Twitter have brought about a revolution in our daily lives/ and also played important roles such as indispensable communication channels, self-presentation tools, online information repositories, life-books, personal dailies, uncensored mass media, marketing or political campaigns, or networking webs. Users not only instantaneously interact with others but also freely generate, publish, share, or distribute their thoughts, ideas, feelings, expressions, or even personal life matters to their circles of friends or others worldwide.

Furthermore, ubiquitous Internet and an emergence of smart devices like smartphones offer more convenience to people in term of 'always-connected' and 'share-as-you-go' accessibility to OSNs. OSNs have become increasingly embedded in daily activities. Many people feel more comfortable to share and more open online than offline, regardless of location, physical distant, and social ties. Several people share their personal lives, problems or even secrets with strangers rather than with loved ones like family or friends. Consequently, OSNs have become vast resources of user-contributed content, ranging from general, personal, private, to sensitive information. This abundance of valuable information is susceptible to any misuse, inferences, threats, or attacks at any time.

Disclosing information on OSNs pose risks to both information privacy and personal privacy. Even selectively shared information can propagate beyond intended audiences. Despite selective sharing and restrictive privacy controls, privacy conflicts and privacy-related issues still arise, particularly in the dynamic, ever-changing, and privacy-interdependent platforms like OSNs.

2.1 Interpretation of Privacy

Privacy has been consistently discussed among scholars from a wide range of disciplines for over a century; unquestionably, it is also one of the most significant and much debatable matters in legal and moral philosophy. Particularly in the evolution of OSNs and advanced mobile computing, privacy has led to a renewed interest in not only offline but also online.
Online privacy has then become an ongoing public talk and raised a major public concern. Despite available privacy managements along with a considerable research in this area, online privacy issues are still pervasive and becoming aggravated. For example, Snowden disclosure (Wikipedia, 2017) is of great interest and striking worldwide attention to information privacy.

While the importance of privacy has been globally recognised, notions of privacy in the literature are still fragmented across diverse disciplines. Due to a lack of a universally standardised definition, privacy has been interpreted in various dimensions and described in several different terms, ranging from one-dimensional to multi-dimensional aspects. Privacy is regarded in a single aspect during earlier research such as a right or an entitlement, a claim, a personal space, a control, a secrecy, a limit in disclosure of personal information, a boundary, a liberty, an anonymity, to a solitude, and much more (Altman, 1975; Solove, 2006; Warren & Brandeis, 1980).

Later concepts of privacy have been transformed to more breadth in an advent of ever-changing technology and ubiquitous computing where a boundary between offline and online spheres is unclear. Subsequently, contemporary privacy concepts have been emerged. Notions of privacy are then presented in compound contexts and different classifications. For instance, privacy is viewed in six dimensions as (1) the right to be left alone; (2) limited access to the self; (3) secrecy; (4) control over personal information; (5) personhood; and (6) intimacy.

Regardless of the difference in definitions, a conformity among privacy concepts exists that privacy is elastic, volatile, multi-dimensional, discipline-dependent, context-dependent, and culture-dependent.

2.2 Communication Privacy Management (CPM) Theory

Based on the notion of privacy as an access control, some researchers view privacy as a personal process whereas other privacy theorists consider privacy as an interpersonal process. The latter perception of privacy leads to a discussion on how to selectively control an access and manage boundaries between parties such as Altman's privacy theory. Altman (1975) use a shift upon cell membrane permeability' as a metaphor to explain privacy as a selective and interpersonal control. Although Altman's theory is emerged from regulating social interactions in physical spaces or offline environments, it has been extended in a number of domains.

Extending this approach, a theory of communication privacy management (CPM) has been applied in both offline and online communication and is often discussed in OSN privacy literature. This theory addresses three key principles: privacy ownership, privacy control, and privacy turbulence to manage information disclosure. According to CPM theory, people own their private information as well as have the right to protect and control an access to that information. When individuals share private information with others, they grant co-ownership rights to others for the future management and control over that private information. In this case, collective privacy boundary is needed in negotiating rules to protect privacy among parties. However, privacy turbulence arises in case of a collapse in privacy management.

Both theories require a continuous negotiation and management between related parties to prevent privacy turbulence; however, Wisniewski, Lipford, & Wilson (2012) pointed that these principles are uncommonly applied in OSN interface designs. Consequently, privacy turbulence has been increasing seen on OSNs and become a major issue extensively studied in literature.

Guided by these two theories, this present study regards privacy as a dynamic and multi-dimensional process that needs collaborative privacy management, particular in the interrelated environments and mutual boundary relationships such as in OSNs.

2.3 Interdependent Privacy

Online privacy in such interconnected environments like OSNs is a complicated matter because of their 'persistence, searchability, replicability, and scalability' (boyd & Ellison, 2007) as well as boundless audiences. These common characteristics of OSNs encourage a pervasive social exchange and trigger a domino effect in privacy. Individual privacy preferences on OSNs is bound to affect privacy of others. Also, available information from a social exchange has an impact on either personal or informational privacy of users or non-users.

Although this concept of privacy interdependence is not relatively new and innate in OSNs, this concept is disregarded in a privacy settings in practices. The term "interdependent privacy" (Biczók & Chia, 2013) was firstly coined in the study of Facebook gaming. While extensive research on OSNs consider privacy as independent, predominantly focusing on self-disclosure (Zlatolas, Welzer, Heričko, & Hölbl, 2015), scarce attention has been paid to a view of interdependent privacy.

Interdependent privacy on OSNs are associated in many contexts such as third-party applications, inferences, re-sharing, tagging, or group participations. When users grant permission to install third-party applications, these applications can access and modify pieces of information on users' profiles. Additionally, friends of users can share information on the profiles without expressed consent. Several studies on privacy shows that installing third-party applications would violate user's global privacy settings and friends' privacy (Wang, Xu, & Grossklags, 2011), pose risks from inference attacks to reveal information on users' profiles (Ahmadinejad & Fong, 2014), or breach privacy of revealing sensitive information by extracting hidden attributes (Ryu, Rong, Li, & Machanavajjhala, 2013).

Another research in the area of the privacy interdependence on OSNs address that third parties can infer not only personal identification information (PII) shared by other users or friends but also political or religious affiliation, even when users are unwilling to disclose such information (Heatherly, Kantarcioglu, & Thuraisingham, 2013).

2.4 Information Disclosure on OSNs

Information disclosure on OSNs pose risks to privacy and cause either minor or major damages, ranging from unpleasant experiences, embarrassment, harassment, humiliation, privacy turbulences, bad self-image, face-threats, distress, inflammation, identity theft, to stalking and much more. A result from domino effects can lead to an extreme end such as a suicide, for example, some people cannot cope with online or offline stalking as well as disgrace when their content are pervasive shared by others on SNSs.

Users may disclose information about others either on their own OSNs' virtual spaces ("profiles") or other users' profiles during their online interactions and activities. Alternatively, some people refrain from joining OSNs to preserve their privacy.

However, non-users still is inevitable from privacy issues regarding other-generated disclosure.

The phenomenon of revealing about others without consent (other-generated disclosure) is not uncommon on OSN wall posts, comments, videos, links, photos, and tags. It can be seen in forms of sharing on-behalf, sharing either co-owned or multiple-owned content, re-sharing content, or tagging. The most trending other-generated disclosure relates to photo sharing on OSNs. For example, Alex shares a photo of him and his friends in a farewell party to his Facebook friends. Another example from a news report is that Dr. Than from Rhode Island posted information about a trauma patient on her Facebook page without revealing the patient's name; however, the hospital board concluded that she had posted enough information for people who knew the patient can identify.

Previous research reported that other-generated disclosure by friends can cause embarrassment or at worst break up profile connections (unfriending) although that disclosure is in a playful way such as amusement, tease, or mock (Choi, Jiang, Xiao, & Kim, 2015).

While disclosing information about oneself (self-disclosure) can be inhibited, managed, and under control of individuals, disclosing information about others (other-generated disclosure) is beyond individual control. Despite long privacy policies and fine-grained privacy settings such in Facebook, these privacy managements and mechanisms offer users the control only within users' profiles or own online spaces. Yet, there is a lack of control outside users' own spaces or over other-generated disclosure. Moreover, an increase in collaborative activities in the recent year such as sharing joint-ownership content raises a new set of privacy challenges on other-generated disclosure.

This present study focused on different another context of interdependent privacy and differed from earlier research. Previous research mostly focused on static content such as information on individual profiles whereas this present study calls attention to dynamic content associating with other-generated disclosure.

2.5 Privacy Concerns on OSN Platforms

Privacy concerns deal with the worry or belief that one's privacy may be at risk or undesirable. A considerable research on OSN privacy has studied privacy concerns in various aspects, ranging from factors associating with privacy concerns, measures of privacy concerns, privacy concerns in e-commerce contexts, to relationships between privacy concerns and users' behaviours in relation to adoption of OSNs or information disclosure. For example, privacy concerns can lead OSN users to limit their profile visibility and discourage users from expanding their networks, but privacy concern do not refrain users from self-disclosure (Chen, Wenjie, Xu, & Tan, 2015).

Despite a large body of research addressing OSN privacy concerns as addressed above, most existing studies put emphasis on privacy concern over self-disclosure. Limited research on OSNs explores privacy concern associated with information disclosure by

others, particularly by insiders (friends, mutual friends, peers). A few work brings to light that OSN users concerned about information disclosed by their friends. (Choi et al., 2015; Wisniewski, Xu, Lipford, & Bello-Ogunu, 2015)

3 Methodology

To better understand interdependent privacy with regard to other-generated disclosure, this phenomenological study used an online survey on Survey Monkey platform to explore Facebook users' privacy concerns, privacy settings, and information disclosure. Then we conducted a semi-structured in-depth interview with suitable participants who have lived experiences in other-generated disclosure on Facebook.

3.1 Survey Administration and Samples

The survey questionnaires were launched online through SurveyMonkey.com. Simultaneously the invitation for this online survey was advertised on several OSNs such as Facebook (author's profile, public groups, and private groups), Twitter, and CSU forum.
This step intended to attract a large number of OSN users as some users have multiple OSNs including Facebook.

The online survey consists of 31 questions divided into four main sections, beginning with demographic information (Section A), background (Section B), Facebook usage (Section C), and contact for a follow-up Interview (Section D). It eliminated the bias on gender by striking a balance between male and female in both groups. At the end of the online survey questionnaires, survey respondents could voluntarily provide their pseudonym as well as their e-mail address if they were interested to participate in a semi-structured in-depth interview.

3.2 Preliminary interview results

Semi-structured, in-depth interviews of Facebook users on their experience about other-generated disclosure are continuing. Early results are presented and discussed here. We asked participants how they manage their social circles, handle overlapping of social circles, personal disclosure, updates from others, participate in either public or closed group, and conflicts within OSNs. Participants were asked to base their responses on actual past experience as opposed to speculating what they would do given a particular scenario. This was to gain the lived experiences of insiders because pervious research found that privacy concerns do not reflect on their privacy behaviour, a so-called privacy paradox. A consent form and information package about this research project were attached to the invitation sent to each participant.

Exemplary quotations from four participants follow:

I usually don't publish anything that I wouldn't want people to know publicly. They will hear from me face to face but I have noticed that when I posted the messages on the public forums, then I searched my name through google or .pal; sometime that posts were actually showed up for people to see in the public way which I didn't expect. But my privacy setting was set to my friends only. But, like I said, I try not to post anything that I wouldn't say to somebody publicly.

I was asked to remove the group picture from my Facebook page due to some conflicts between friends. I don't mind so I remove it.

My Facebook account is private. I hide everything I could such as my personal, my education, my family, my relationships status, my albums, and others; I mean I chose the minimum exposure options on Facebook privacy settings such as a friend list, favourite movies, favourite music, visited places, and others. However, I was very surprised one day when someone found out about my relationship status.

I untagged from the photos my friend posted after our holidays trip. However, I found that photo was still been around in a circle of friends and even to someone I didn't really know, who I thought maybe they are friends of my friends. So I asked my friends to remove that picture from their Facebook pages.

4 Discussion and Contribution

There were 460 survey respondents. The majority of respondents (91.1%) 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 (59.43%) than male (40.57%) respondents. Most respondents (44.05%) reside in Australia, 13.22% in Indonesia, 12.33% in United States, and others in United Kingdom, China, Brazil, Finland, India, Italy, and Pakistan. Most respondents live in metropolitan (52.51%) rather than rural (35.95%) and remote area (11.55%).

The majority of respondents are working professionals (69.87%), students (22.27%) and 'others' (7.86%), who described themselves as either stay-at-home parents or job seekers. Most respondents (90.85%) had Facebook accounts more than three years whereas some have Facebook accounts between 2-3 years (2.9%), 1-2 years (3.13%) and less than 6 months (3.13%). The number of friends that respondents have vary such as 100-200 (17.91%), 201-300 (16.33%), 300 or more (45.35%); subsequently, these three groups are met a sampling criteria in terms of number of friends.

More than one-fourth of respondents requested their friends remove photos on OSNs after finding out about other-disclosure outside their profiles (Figure.1). Other-generated disclosure associated with tags, photos, posts, or comments is more problematic in that associated with videos and links (Figure. 2-4). The request to friends to remove tags are likely the same as to remove photos; similarly, the request to friends to remove posts are

likely the same as to remove comments (Figure.2). On the other hand, the request from friends to respondents for deleting photos are slightly more than that for removing tags (Figure.3). In the same line, the request from friends to respondents for deleting posts are slightly more than that for deleting comments (Figure.3)

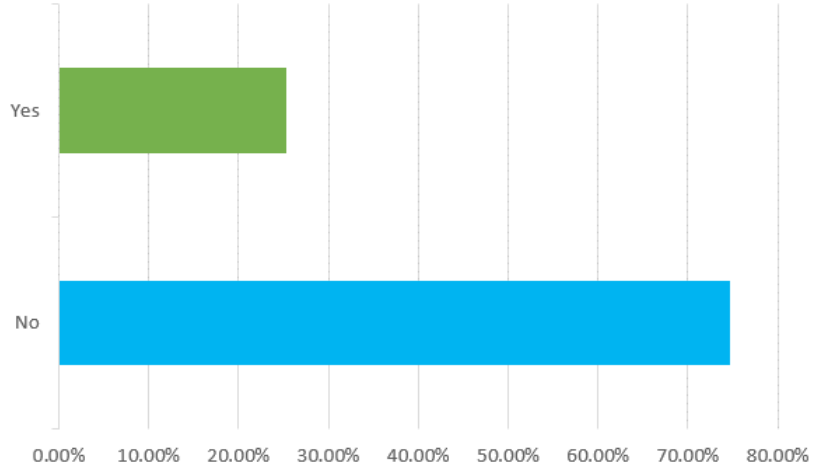

Figure.1 **Have you ever asked a Facebook friend to delete a group photos that includes you?**

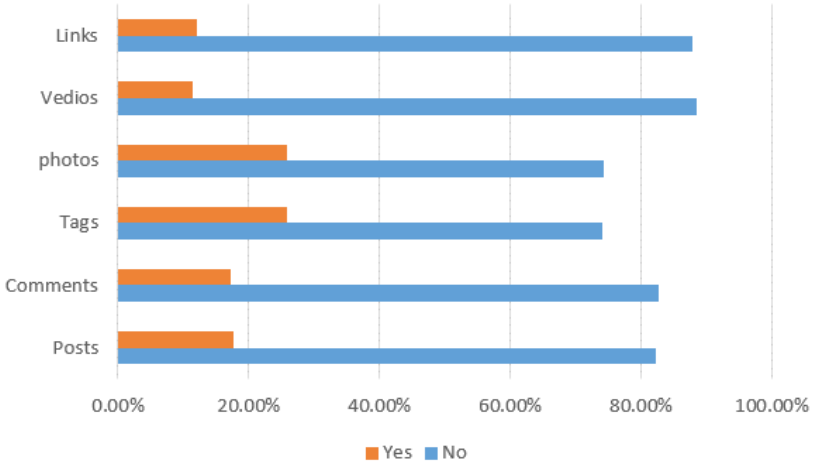

Figure.2 Have you ever asked others to remove/delete any of the following items from their profiles?

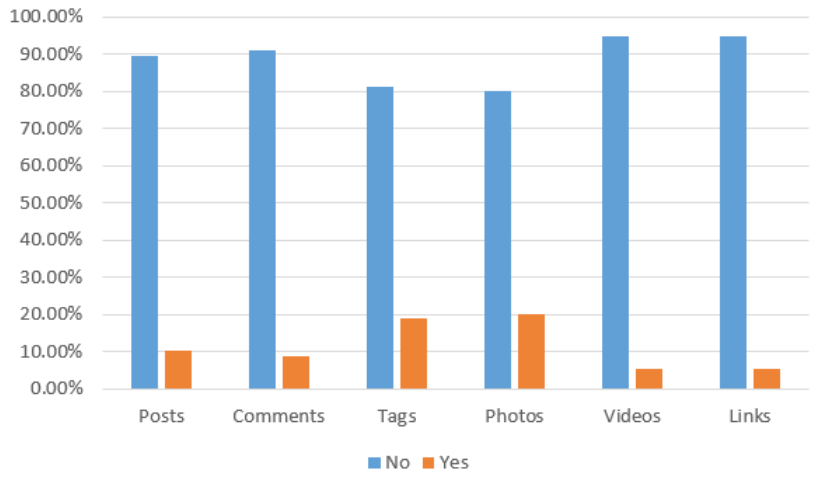

Figure.3 Have you ever been asked to remove/delete any of the following items from your profile?

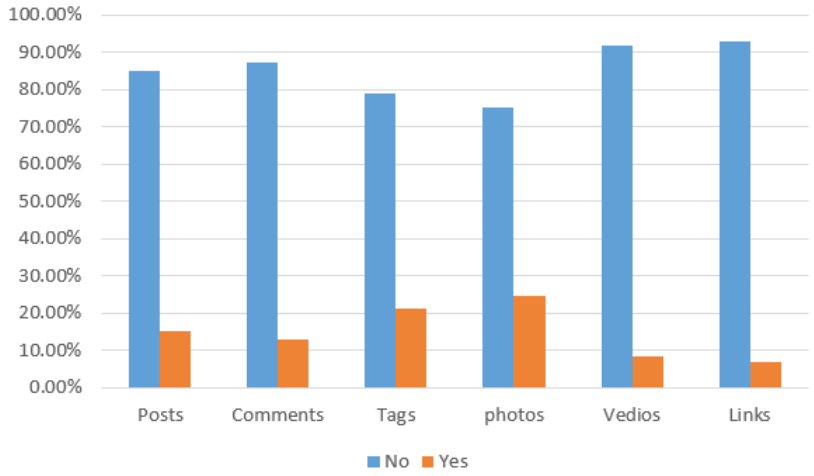

Figure.4 Have you ever removed/deleted any of the following items from your profile due to friends' requests?

According to interviews with Facebook users, they had experienced other-generated disclosure on Facebook. Participants revealed was unexpected, as some restrict their Facebook privacy settings as "friend-only" although some are less restrictive. Most participants agree that they didn't see any reasons to worry about information disclosure by others, especially from outsiders because they are carefree about disclosures by strangers and Facebook privacy settings are sufficient enough to prevent privacy related issues from strangers. However, they were concerned about disclosure from insiders such as family, colleagues, and friends but they assumed that it is unlikely to happen. From the preliminary results, most disclosure by friends are through photos and comments. Regardless of intention, other-generated disclosure by friends can arise even though users restrict their privacy settings.

5 Limitations and Future Research

Firstly, our findings are based on the Facebook platform; alternatively, future studies could investigate the interdependent privacy on different OSNs such as Google+, Twitter, and Xing, to confirm the generalizability of our results. Second, using an online survey may be viewed as a limitation in terms of access availability as it is aimed at people who have internet access. Third, a number of methodological limitations have to be taken into account when interpreting the results of this study. By using an online survey, the data from this present study are based on self-reports. Self-reports require a reconstruction of attitudes, feelings, or behaviours from memory and can subsequently be biased. Future research can find an alternative by tracking or logging actual behaviours.

6 Conclusion

Interdependent privacy issues associated with other-generated disclosure are increasingly common in social media. Other-generated disclosure on OSNs is inevitable even with non-users and is beyond individual control. In this paper, we addressed the privacy issues associated with this phenomenon from the perspective of adult Facebook users. Our results show that Facebook users are likely to expose to other-generated disclosure not only through tags and photos but also through posts and comments. Posts and comments are increasingly problematic because no existing effective privacy control currently exists to mitigate this risks. These results serve as a basis for future development in the area of information privacy and yield valuable insights that can guide practice in this important, new area of privacy.

This study will increase users' awareness as well as call for scholars' attention to pay more attention to other-generated disclosure, especially from the insiders. Furthermore, it is a call to future research to examine privacy control mechanisms and design privacy settings which tackle privacy issues with regard to other-generated disclosure associated with posts and comments, rather than focusing on photos.

Acknowledgements

We would like to thank all survey respondents for their participations and contributions to this study. Thanks to the senior editor, associate editor, and two anonymous reviewers for their comments and suggestions, which significantly improved the quality of this paper. We are very grateful to Yeslam Al-Saggaf for his guidance in research design, his feedback and comments, and his support in this research project. We also thank Maureen Minielli for her great support in this study.

References

Ahmadinejad, S. H., & Fong, P. W. L. (2014). Unintended disclosure of information: Inference attacks by third-party extensions to Social Network Systems. Computers & Security, 44, 75–91. https://doi.org/10.1016/j.cose.2014.04.004

Altman, I. (1975). The Environment and Social Behavior: Privacy, Personal Space, Territory, Crowding. Brooks/Cole Publishing Company.

Beck, C. (2015, February 18). Digital kidnappers steal kids' online pictures. Retrieved July 22, 2017, from http://www.wusa9.com/news/nation-now/digital-kidnappers-steal-kids-online-pictures/203578781

Biczók, G., & Chia, P. H. (2013). Interdependent Privacy: Let Me Share Your Data. In Financial Cryptography and Data Security (pp. 338–353). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-39884-1_29

boyd, danah m., & Ellison, N. B. (2007). Social Network Sites: Definition, History, and Scholarship. Journal of Computer-Mediated Communication, 13(1), 210–230. https://doi.org/10.1111/j.1083-6101.2007.00393.x

Chen, J., Ping, J. W., Xu, Y. C., & Tan, B. C. Y. (2015). Information Privacy Concern About Peer Disclosure in Online Social Networks. IEEE Transactions on Engineering Management, 62(3), 311–324. https://doi.org/10.1109/TEM.2015.2432117

Choi, B. C. F., Jiang, Z. (Jack), Xiao, B., & Kim, S. S. (2015). Embarrassing Exposures in Online Social Networks: An Integrated Perspective of Privacy Invasion and Relationship Bonding. Information Systems Research, 26(4), 675–694. https://doi.org/10.1287/isre.2015.0602

Chutikulrungsee, T. T., Burmeister, O. K., Al-Saggaf, Y., & Bhattacharya, M. (2016). Denial of Choice: Group Level Disclosure of Private Information. In Technology and Intimacy: Choice or Coercion (pp. 229–240). Springer, Cham. https://doi.org/10.1007/978-3-319-44805-3_19

Emerson, R. (2011, October 18). 13 Controversial Facebook Firings: Palace Guards, Doctors, Teachers And More. Huffington Post. Retrieved from http://www.huffingtonpost.com/2011/10/17/facebook-firings_n_1003789.html

Heatherly, R., Kantarcioglu, M., & Thuraisingham, B. (2013). Preventing Private Information Inference Attacks on Social Networks. IEEE Transactions on Knowledge and Data Engineering, 25(8), 1849–1862. https://doi.org/10.1109/TKDE.2012.120

Hu, H., Ahn, G.-J., & Jorgensen, J. (2013). Multiparty Access Control for Online Social Networks: Model and Mechanisms. IEEE Transactions on Knowledge and Data Engineering, 25(7), 1614–1627. https://doi.org/10.1109/TKDE.2012.97

Matyszczyk, C. (2010, January 11). Zuckerberg: I know that people don't want privacy. Retrieved July 22, 2017, from https://www.cnet.com/au/news/zuckerberg-i-know-that-people-dont-want-privacy/

McGinty, B. (2016, April 11). Digital kidnappers steal your identity. Retrieved July 22, 2017, from http://www.wcnc.com/tech/digital-kidnappers-steal-your-identity/128904472

Ryu, E., Rong, Y., Li, J., & Machanavajjhala, A. (2013). Curso: protect yourself from curse of attribute inference: a social network privacy-analyzer (pp. 13–18). ACM Press. https://doi.org/10.1145/2484702.2484706

Solove, D. J. (2008). Understanding privacy (First Harvard University Press paperback edition). Cambridge, Massachusetts London, England: Harvard University Press.

Walther, J. B., Van Der Heide, B., Hamel, L. M., & Shulman, H. C. (2009). Self-Generated Versus Other-Generated Statements and Impressions in Computer-Mediated Communication: A Test of Warranting Theory Using Facebook. Communication Research, 36(2), 229–253. https://doi.org/10.1177/0093650208330251

Wang, N., Xu, H., & Grossklags, J. (2011). Third-party apps on Facebook: privacy and the illusion of control (pp. 1–10). ACM Press. https://doi.org/10.1145/2076444.2076448

Warren, S. D., & Brandeis, L. D. (1890). The Right to Privacy. Harvard Law Review, 4(5), 193–220.

Wikipedia. (2017, June 30). Commentary on Edward Snowden's disclosure. In Wikipedia. Retrieved from https://en.wikipedia.org/w/index.php?title=Commentary_on_Edward_Snowden%27s_disclosure&oldid=788341174

Wisniewski, P., Lipford, H., & Wilson, D. (2012). Fighting for my space: coping mechanisms for sns boundary regulation. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 609–618). ACM Press. https://doi.org/10.1145/2207676.2207761

Wisniewski, P., Xu, H., Lipford, H., & Bello-Ogunu, E. (2015). Facebook apps and tagging: The trade-off between personal privacy and engaging with friends: 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. https://doi.org/10.1002/asi.23299

Zephoria. (2017, July 6). Top 20 Facebook Statistics - Updated July 2017. Retrieved July 22, 2017, from https://zephoria.com/top-15-valuable-facebook-statistics/

Zlatolas, L., Nemec, Welzer, T., Heričko, M., & Hölbl, M. (2015). Privacy antecedents for SNS self-disclosure: The case of Facebook. Computers in Human Behavior, 45, 158–167. https://doi.org/10.1016/j.chb.2014.12.012