UNDERSTANDING EMERGENCE AND OUTCOMES OF INFORMATION PRIVACY CONCERNS: A CASE OF FACEBOOK

Burcu Bulgurcu  
*University of British Columbia, bulgurcu@bc.edu*

Hasan Cavusoglu  
*University of British Columbia, hasan.cavusoglu@sauder.ubc.ca*

Izak Benbasat  
*University of British Columbia, Canada, izak.benbasat@sauder.ubc.ca*

Follow this and additional works at: [http://aisel.aisnet.org/icis2010_submissions](http://aisel.aisnet.org/icis2010_submissions)

Recommended Citation

[http://aisel.aisnet.org/icis2010_submissions/230](http://aisel.aisnet.org/icis2010_submissions/230)

This material is brought to you by the International Conference on Information Systems (ICIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in ICIS 2010 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.
Understanding Emergence and Outcomes of Information Privacy Concerns: A Case of Facebook

Burcu Bulgurcu
University of British Columbia
Burcu.Bulgurcu@sauder.ubc.ca

Hasan Cavusoglu
University of British Columbia
Hasan.Cavusoglu@sauder.ubc.ca

Izak Benbasat
University of British Columbia
Izak.Benbasat@sauder.ubc.ca

Abstract

Drawing on content analysis of user responses to the revisions in the Facebook Privacy Policy, this study develops a process model to explain emergence and outcome processes of users’ information privacy concerns in an online social networking context. The first phase of the model proposes three broad categories of informational practices – collection and storage; processing and use; and dissemination of personal data—associated with users’ information privacy concerns. This phase also identifies the conditions under which proposed practices are attributed as privacy issues. The second phase of the model describes outcomes of perceived privacy issues by proposing users’ affective and behavioral responses. The findings provide evidence for, (1) the important role of trigger conditions in emergence of users’ information privacy concerns, (2) the gap between privacy issues that are perceived by users and identified by domain experts, (3) the uniqueness of online social networking context in providing distinct privacy challenges.

Keywords: Online social networks, information privacy, Facebook
Introduction

Privacy of information is substantially important to technology users, as firms’ pervasive use of information technologies make it difficult to have control over personal information (Dinev and Hart; Hui et al. 2007; Malhotra et al. 2004; Solove 2001). Despite the extant literature which acknowledges the importance of privacy, privacy issues have been growing in recent years as new information technologies limit people’s ability to protect personal information (Dinev and Hart 2006; Hui et al. 2007; Malhotra et al. 2004). The pervasive use of information technologies, powerful databases, and ubiquitous computing practices made it extremely challenging for individuals to have control over personal information Solove 2001. Firms are now able to collect immense amount of data about their customers by tracking consumers electronically on the Internet and make use of databases to store and process information collected about customers. As a result, technology users are exceedingly concerned about information privacy violations today than any epoch of the history (Solove 2008).

Previous studies on information privacy have identified a number of important concepts as antecedents and consequences of information concerns by dominantly focusing on a number of contexts; such as, electronic commerce and online shopping (Awad and Krishnan 2006; Dinev and Hart 2006; Hui et al. 2007; Van Slyke et al. 2006; Wirtz et al. 2007), offline shopping and direct marketing (Culnan 1993; Culnan and Armstrong 1999; Hine and Eve 1998; Nowak and Phelps 1992), and general Internet use (Dinev and Hart 2004; Korzaan et al. 2009; Son and Kim 2008). A few recent studies investigated online information privacy by focusing on other specific settings; such as, e-health (Angst and Agarwal 2009), financial portals (Hann et al. 2007), online and mobile advertising (Lwin et al. 2007; Okazaki et al. 2009), and online social networking (Debatin et al. 2009). While these studies have expanded our understanding from various perspectives, we yet know little about the emerging issues of information privacy associated with the use of online social networks (OSNs).

This study aims to contribute to the privacy literature by focusing on OSN context and proposing a process theory to explain emergence and outcome processes of users’ information privacy concerns. The goal of this theory will be to explicate the information practices of an OSN provider organization that may lead emergence of users’ information privacy concerns and discuss the conditions under which these practices are perceived as privacy issues. Results of this study will have both theoretical and practical implications. From a theoretical perspective, study will offer, to the best of our knowledge, the first comprehensive framework to the literature that help us understand the context specific issues of information privacy in OSN. From a practical perspective, the proposed research will provide important managerial guidance to practitioners to considerer user reactions to privacy issues and evaluate their information practices. Further, it will provide insights that will enable practitioners to develop and evaluate more effective information privacy policies and design appropriate and complete set of privacy protection tools for their users considering needs of OSN users.

Literature Review

Previous research has suggested several different dimensions and drivers for information privacy concerns. A privacy taxonomy by Solove (2008) proposed four types of harmful practices—information collection, information processing, information dissemination, and invasions—and also suggested forms of these activities, such as; surveillance, aggregation, insecurity, breach of confidentiality, blackmail etc. Smith et al. (1996) has identified four privacy concern dimensions—collection, unauthorized internal or external secondary use, improper access, and errors—and proposed their measures. Similarly, Malhotra et al. (2004) has proposed technology users’ information privacy concerns as a multi-dimensional construct, which is conceptualized as data collection, user control, and user awareness. Based on Solove’s taxonomy (2008), this paper will propose three types of information practices as dimensions of information privacy concerns: (1) Collection and Storage, (2) Processing and Use, (3) Dissemination. 

Collection and Storage: Data collection, which is proposed as a key dimension of information privacy concerns (Solove 2002), refers to the degree to which a person is concerned about the amount of data possessed by others relative to the value of benefits received (Malhotra et al. 2004; Okazaki et al. 2009; Smith et al. 1996; Stewart and Segars 2002; Van Slyke et al. 2006). In the domains of electronic commerce and direct marketing, it is reported that consumers’ concerns over data collection practices affect their intentions toward releasing personal information (Phelps et al. 2000), trust and risk beliefs (Malhotra et al. 2004; Okazaki et al. 2009), willingness to transact and purchasing decisions (Hine and Eve 1998; Van Slyke et al. 2006).
Processing and Use: In order to create value, the practice of data collection is often followed by data processing practices, which refers to the combination, storage, analysis, manipulation, and use of gathered data (Solove 2008). For example, Amazon uses aggregated data about a person’s buying history to recommend other products that the person might find of interest. Prior studies that focus on the contexts of online and offline commerce have mentioned several potential benefits of data processing to online companies (profiling user data and utilizing lower cost and more effective personalized/targeted/customized marketing (Awad and Krishnan 2006; Culnan 1993; Phelps et al. 2001; Tezinde et al. 2002), understanding users’ technology usage patterns (Debatin et al. 2009), as well as technology users; such as, using personalized and customized services (Chellappa and Sin 2005; Nowak and Phelps 1997b), convenience and time savings (Hann et al. 2007). In the online social networking context, data processing may result in increases in levels of user socialization as it helps online social network providers identify friendship networks and make friendship suggestions, run social games and applications, provide settings for social shopping and so on. Alongside these benefits, however, processing can cause negative outcomes in terms of technology use as processing practices can conflict with user expectations and create privacy concerns. The studies in the literature propose several privacy issues related to data processing; such as, receiving unsolicited e-mails (Cranor et al. 2000; Sheehan 2002; Sheehan and Hoy 1999), identification and losing anonymity (Solove 2002), internal and external secondary data use (Smith et al. 1996).

Dissemination: The practice of data dissemination refers to an online firm’s revealing and spreading personal information (Solove 2008). Dissemination of data was not proposed as a salient concern in the previous studies that investigated contexts of instrumental technologies (i.e. e-com, advertising). However, data dissemination emerges as a clear theme in online social networking setting. There are two main explanations for this phenomenon: (1) The interactions among parties were much less complex for instrumental technologies (usually one two-way interaction between the consumer and the firm) compared to online social networking (many types of interactions; such between the user and the firm, the user and his friends, the user and his friends of friends, the user and third parties, the user’s friends and third parties, the firm and the third parties). Users’ having control over personal data could be easier to manage using instrumental technologies, as the only involved parties are the user and the firm. While online firms selling data for financial gain (Nowak and Phelps 1997a), insecurities of stored data (Smith et al. 1996), aggregation of collected data from multiple sources (Solove 2008) are suggested as potential drivers of data dissemination, existence of clear information privacy statement is usually sufficient to reduce users’ privacy concerns and to induce them adopt the technology. However, the complex nature of interactions on online social networking sites increases the likelihood of data disclosure and makes the user more vulnerable to information privacy related risks compared to the risks of instrumental technologies. All the relevant parties can be a source of data disclosure (i.e. a friend using unsecure third party applications, a malicious third party applications adopted by the user, users’ friends of friends profile settings). (2) The purpose of technology use also makes users’ more vulnerable on OSNs. As the main purposes of using social networks are making relationships, sharing, and communicating users are more willing to disclose their personal information. As their disclosure also increases their socialization on the site, they may become less sensitive to perceiving potential privacy issues.

While the practices of data collection, data processing, and data dissemination have been presented as drivers (or dimensions) of information privacy concerns in previous studies (Malhotra et al. 2004; Okazaki et al. 2009; Smith et al. 1996; Solove 2008), this paper argues that, depending on how users perceive them, information practices may indeed have two type of impacts for the context of OSNs—(1) positive impact: they may be influential in increasing users’ perceived level of socialization on the networking site, and (2) negative impact: they may be influential in increasing users’ information privacy concern. An OSN’s success entirely depends on its users’ participation and continuous activities on the site; such as, self-disclosure, communication, and information sharing (Ellison et al. 2007; Krasnova et al. 2008). To remain attractive to its users and provide a sustainable networking site, OSN provider organizations must be supporting and managing these processes by actively collecting, processing, and disseminating data. However, as previous studies suggested, these practices may also lead to the emergence of site users’ information privacy concerns. Thus, we mainly argue that, proposed frameworks remain at a very high level so they are not sufficient in providing necessary guidelines to understand specific and context dependent issues. In particular, these frameworks lack to explain how and why the proposed informational practices are perceived as privacy issues by technology users. While the proposed informational practices, such as collection, storage, and processing of personal information, can constitute potential harm to information privacy, they may well serve to the needs of technology users. For example, users who are registered to a website may enjoy the convenience of personalized contents. Therefore, it might be inappropriate to generalize that informational practices always create harm to information privacy. Furthermore, users may perceive some of the data collection methods (i.e. collection by online cookies) more important to information privacy than others (i.e. informed and direct questions). Thus, it is
essential to understand the trigger conditions under which an informational practice is perceived as a threat to information privacy. We believe that understanding these conditions would help not only enhance our theoretical understanding of information privacy but also design and develop better technological systems.

We also argue that, existing studies reflect the views of domain experts (i.e. academics, lawyers, privacy commissioners etc.), not those of users. However, some of the issues which are identified by the domain experts as important issues that could result in devastating consequences for people (i.e. aggregation of data from multiple sources for identification purposes) may not be perceived at all or at the same level by technology users. Hence, this study attempts to understand issues of information privacy from the perspective of technology users. In doing so, we aim to shed light on users’ vulnerabilities in regards to protecting their personal information by answering whether technology users are capable of perceiving all the informational practices that may create privacy challenges for them and whether some of the informational practices are more likely to be perceived as drivers of privacy issues. We believe that a better understanding of users’ perspective would allow us to develop appropriate training and awareness programs, better privacy protection tools, and better policies to protect their information privacy.

Based on all the discussion above, this our study aims to address the following questions in the context of online social networking sites: (1) What are users’ perceived privacy issues in an online social networking site?, (2) What triggers users’ attribution of an informational practice to a privacy issue?, (3) What are outcomes of users’ perceived privacy issues?

**Research Method**

The research questions of this study aims at understanding the emergence and outcomes of users’ information privacy concerns in an online social networking site. Qualitative analysis is well suited for the purpose of answering the research questions for a number of reasons. First, the concept of privacy and the context of online social networking are known to be a complex and variable phenomenon (Newman et al. 2006) that require in-depth understanding of an evolving and unfolding nature of events. Further, online social networking is a new phenomenon that needs further attention for a systematic understanding of information privacy issues it may create. Thus, our goal to generate and build a new theory in an area where little knowledge has been created can be achieved by employing a qualitative approach (Strauss and Corbin 1990). Finally, utilizing a qualitative approach is appropriate for this study as it aims to understand users’ perspectives about an issue (Strauss et al. 1994).

In particular, this study conducts a content analysis and investigates users’ comments posted on sections of proposed privacy policies. This method provided a good foundation to understand users’ privacy concerns in online social networking. First, the method allowed us to reach users who are sensitive in protecting their personal information and have some understanding on the privacy concept in general. Second, it helped us obtain a large data set. Third, it enabled us to reach very rich explanations about various informational practices of Facebook as they were specified in details in their policy. Last, but not least, it enabled us to gather users’ reactions to proposed policy as it is known that technology users are usually not aware of their needs but they are good at responding to a set of proposed terms. We believe analyzing users’ reactions to the policy by using a rich and novel dataset enabled us to better understand users’ privacy concerns in online social networking.

**Research Context**

This study was conducted with Facebook users. Facebook is a popular OSN site with more than four hundred million of active users connecting and communicating with their friends, sharing links, photos, or videos with their networks, creating and joining groups. It is reported that fifty percent of Facebook users log on to the site in any given day and people spend over five hundred billion minutes per month on average (Facebook 2010). Facebook’s popularity and extensive usage by people all over the world make its privacy policy susceptible to all criticisms. While Facebook founders and mainstream users argue that the social network actually offers a slew of privacy controls and security features which can help users protect their personal information, the site is often at the core of privacy criticisms related to social networking on press articles and mass media (The Globe and Mail 2010, CNN 2010). Facebook was selected as the platform for this study for a number of reasons. First, it enabled us to reach a larger user population due to Facebook’s popularity. Second, it allowed us to gather users’ perspectives as Facebook allows their users to comment on the revisions of the site’s privacy policy. Third, Facebook is a good representative example to investigate privacy issues surrounding social networking as the site possesses all the main characteristics
of new online social networking sites which are known to redefine the nature of social interaction on the Internet.

Fourth, Facebook users are likely to be more aware of the potential privacy issues on the site as Facebook is the focus of attention in the mass media in relation to information privacy challenges of social networks.

**Data Collection: Sample and Procedure**

Data collection was conducted in 2009 and 2010 right after the proposal and release of Facebook’s Privacy Policy and Statement of Rights and Responsibilities. After each release, Facebook asked its users to provide feedback on the proposed policy by posting comments on the sections of the policy within a seven day comment period. This study investigates the user comments on sections in 2009 and 2010 privacy policies. While Facebook provides each policy section in five different languages and lets its users comment in these languages, this study only includes the analysis of comments posted in English. Table 1 presents the number of user comments posted for each section of proposed privacy policies. Actual column represents the number of overall user comments that are available under each section of the policies, while analyzed column represents the number of comments that were included in our analysis. The comments were eliminated from the analysis because they were either written in a language other than English or short answers that were confirming or disconfirming the policy section without providing any specific explanation on perceived privacy concerns. The policy that was proposed in 2010 was quite similar to the one proposed in 2009, except the revisions in wordings and formatting of the document. While the recent policy includes a new section for “sharing information in Facebook”, the terms of this section were already available in the former policy under “information you share with third parties”.

<table>
<thead>
<tr>
<th>Policy Sections</th>
<th>October 29, 2009</th>
<th>March 26, 2010</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Actual</td>
<td>Analyzed</td>
</tr>
<tr>
<td>Introduction</td>
<td>238</td>
<td>233</td>
</tr>
<tr>
<td>Information we receive</td>
<td>131</td>
<td>130</td>
</tr>
<tr>
<td>Information you share with third parties</td>
<td>109</td>
<td>109</td>
</tr>
<tr>
<td>Sharing information on Facebook</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>How we use your information</td>
<td>56</td>
<td>51</td>
</tr>
<tr>
<td>How we share information</td>
<td>77</td>
<td>72</td>
</tr>
<tr>
<td>How you can view, change, or remove information</td>
<td>92</td>
<td>90</td>
</tr>
<tr>
<td>How we protect information</td>
<td>56</td>
<td>51</td>
</tr>
<tr>
<td>Other terms</td>
<td>113</td>
<td>112</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>872</strong></td>
<td><strong>848</strong></td>
</tr>
</tbody>
</table>

**Data Analysis**

Data analysis was conducted with a qualitative data analysis software package (NVivo v.8). While the data analysis is still in progress, the major stages that have been completed are as follows:

**Stage 1: Analysis of comments posted for Facebook 2009 Privacy Policy:** We coded and analyzed the user comments posted for the sections of the privacy policy proposed in 2009. The purpose was identifying informational practices that are associated with users’ perceived privacy issues. Thus, we have coded all user comments posted for 2009 Policy and identified a list of privacy issues. The results of the phase were a number of privacy concerns identified by Facebook users.

**Stage 2: Review of existing taxonomies of privacy concerns in the literature:** In this stage, we have thoroughly reviewed the existing taxonomies and theories of privacy in order to identify the potential contributions of the findings of the first stage to the literature. Considering what we have learned in the first stage, we have identified the strengths and the weaknesses of the existing theories and taxonomies in the literature and proposed the important and novel concepts that came out in the first phase. Finally, we have revised the research questions according to what we have learned in these two stages. As the main conclusions of this stage, (1) we have decided to adapt Solove’s (2008) taxonomy as a guideline for categorizing broad informational practices and included data collection and storage, data processing and use, and data dissemination as the main categories or informational practices; (2)
we have decided to focus on understanding the trigger conditions under which any given informational policy would be perceived as a privacy issue from the perspective of users; (3) we have noted that data also includes outcomes of privacy issues so we have decided to code outcomes of privacy issues in later stages.

Stage 3: Re-coding of Facebook 2009 Privacy Policy: In this stage, we have re-coded findings of the first stage considering Solove’s (2008) taxonomy. We have also coded the outcomes of perceived privacy issues.

Stage 4: Analysis of comments posted for Facebook 2010 Privacy Policy and Theory Development: We compared the terms in 2009 and 2010 policies and realized that there were not any major differences in their terms. We plan to continue with coding the comments posted for 2010 policy and use results of this stage as a confirmation to the findings of the third stage. Finally, we plan to focus on theory development and review our coding to identify the relationships among the constructs. Based on the results, we will develop a theoretical model that explains the emergence and outcomes of a privacy issue in an online social networking site from the users’ perspective.

**Preliminary Findings**

This study attempts to explain emergence and outcomes of a privacy issue as a process from the perspective of users of an online social networking site. The proposed model, which is presented in Figure 1, defines two sequential processes: (1) Emergence of a Privacy Issue and (2) Outcomes of a Privacy Issue. Findings of each section of the privacy policy will be explained in detail below.

**Phase 1: Emergence of a Privacy Issue**

The paper proposes three informational practices that could potentially be attributed as a privacy issue by users. The analysis revealed that there exist different sets of trigger conditions for each informational practice.

**Collection and Storage of Information** refers to an online social networking site’s acquisition and retention of personal information from its users. According to our data, data collection and storage are held by two parties on this social networking site: Facebook and the third party applications that run on the Facebook platform.

**Data collection and storage by Facebook:** We have identified two types of privacy issues – interrogation and surveillance—that are associated with data collection and storage practices of Facebook. Interrogation refers to direct acquisition of personal information from users by asking relevant questions in a direct manner. These questions aim to collect two types of information: profile information and personal information. Profile information includes the name, e-mail address, birthday, gender, location information and users must provide the required information in order to obtain an account to use the service. Personal information, on the other hand, is not
Data collection and storage by third party applications: We have identified two privacy issues that are associated with the data collection and storage of third party applications. The first privacy issue is “friends’ applications’ access to personal data” and it refers to third party applications’ (which are signed up by connected friends on Facebook platform) ability to access all personal information that are visible to this particular friend. The second issue identified is “automatic data collection by pre-approved third parties” which refers to pre-approved third party applications’ (which are selected and approved by Facebook) ability to automatically collect personal information from all users. We have identified four trigger conditions under which information collection and storage by third party applications have been perceived as a privacy issue: 1) Perceived irrelevance of collected or stored data to the functioning of the application, 2) Perceived lack of transparency about what is collected or stored, 3) Perceived lack of transparency about how and when data is collected and stored, 4) Perceived vulnerability of other users in terms of their data collection by third parties.

Processing and Use of Information refers to an online social networking site’s use and manipulation of data that has been collected. Information processing does not involve the collection of data; rather, it concerns how already-collected data is handled (Solove 2008). Processing and use of information are held by two parties on this social networking site: Facebook and the third party applications that run on the Facebook platform.

Processing and Use by Facebook: Users perceived two issues that are associated with use of personal information by Facebook. Facebook uses personal information to increase the use of their platform: 1) by using personal information of a user (i.e. name, profile picture, profile link etc.), Facebook offers friendship suggestions to other users who are in that user’s close network. 2) by using a user’s personal information and his/her connection history, Facebook offers re-connection suggestions. The conditions that trigger users’ perception of these privacy issues are identified as use of personal information without informed consent and perceived vulnerability of others. Users argue that they do not have any control over the use of their personal information as they have no option of opting-out and are not asked for any consent. Also, they are usually not aware of how their personal information is used but they observe the other users’ being used in such a way that they can also suspect that their data is being used in the same way.

Processing and Use by Third Party Applications: The only privacy issue regarding processing and use of information by third party applications was targeted advertising, which refers to types of advertisements that are placed to reach consumers based on various traits such as their demographics, purchase history, or observed behavior. The conditions that trigger targeted advertising perceived as a privacy issue are personal information being used inappropriately or for manipulative or malicious purposes by third parties.

Dissemination of Data refers to data holders’ transfer or disclosure of the information to others. The only data holder that transfers or discloses information to others is identified as Facebook. Two methods of disclosure identified are 1) Facebook’s disclosure on its own platform, and 2) Facebook’s disclosure to third parties. Even though third parties are identified as data collectors, their possible dissemination of data was not identified as a privacy issue based on the analyzed data.

Facebook’s data disclosure on its own platform: Facebook discloses personal data through its own platform and the identified privacy issues are as follows: 1) Disclosure of general information (i.e. profile picture, name, fan pages, location information) to everyone. Users’ are not allowed to change their privacy settings for their general information. 2) Disclosure of friends list to friends. Users have to show all their friends to other friends even if they want to hide a group of (or all of) their friends from other friends. 3) Disclosure of tagged photos and videos to friends of friends. A user has no control over being tagged in a photo (other than removing the tag after it is posted). When a friend tags a user in one of his photos; all friends of this friend are able to see this photo. 4)
Disclosure of entire photo album [when a friend is tagged, comments on a photo etc.] to friends of friends. When a user tags a friend in one of his photos, all friends of this friend are able to see the entire photo album posted by the user. 5) Disclosure of all personal actions to friends. Personal actions are all disclosed to friends without users’ having an option of changing the privacy settings. Trigger conditions are identified as follows: 1) Enforced privacy settings, 2) Perceived insufficiency (or unavailability) privacy protection tools, 3) Changes in privacy settings without asking for informed consent, 4) Changes in privacy protection tools from a better protective option to a less protective one, 5) Perceived vulnerability of others in terms of their data disclosure on Facebook platform.

Phase 2: Outcomes of a Privacy Issue

We have identified two groups of outcome variables: Affective and Behavioral Reactions. Users’ behavioral reactions to a perceived privacy issue are identified as intention to quit the platform, intention to quit third party applications, intention limit socialization, intention to terminate connections (i.e. online connections with friends, fan pages, groups etc.), intention to give false information, intention to search for additional protection tools. Users’ affective reactions are identified as perceived distrust to the platform, perceived insecurity during the interactions with the platform, perceived unfairness of informational practices and privacy terms, perceived discomfort in using the platform and its services, and perceived dissatisfaction. While data provides evidence that perceived affective outcomes are associated with behavioral outcomes, further research is required to better explain this relationship.

Discussion, Implications, and Future Research

Theoretical Implications

This study makes important theoretical contributions to the emerging literature on information privacy in online social networking. To the best of our knowledge; this is the first study that investigates information privacy in the context of online social networking. This study shows that the context of online social networking has different dynamics that may result in arousal of unique privacy challenges. Results indicate that users’ interactions with different parties; such as, the technology platform, third party applications, friends, and other social communities creates several novel privacy issues that cannot be generalized to all contexts. Second, while the extant literature has proposed theories to define and conceptualize information privacy, this study is the first to propose a process model to explain emergence and outcomes of privacy issues as a process. Further, existing theories of information privacy reflects expert views, however, the proposed theory in this study attempts to reflect the process from users’ perspective. While theories reflecting expert views help us understand the potential privacy issues in detail, they cannot explain users’ weaknesses. Hence, they are not sufficient in providing guidelines that could help lessen users’ perceived vulnerabilities, develop necessary protection mechanisms to alleviate potential privacy issues. Understanding the emergence and outcomes of a privacy issue as a process from users’ perspective is important to understand users’ needs and help them accordingly. Third, this study is, to the best of our knowledge, the first to investigate the issues of privacy by utilizing a content analysis. The selected method helped us explore the research questions from a novel perspective and identify new constructs that would complement the existing literature. In addition, utilization of a qualitative method resulted in identifying unique variables that are specific to the selected context.

While this study includes informational practices in the proposed model, it also argues that proposed informational practices would not be sufficient in explaining emergence of privacy issues alone. As a key theoretical contribution, this study proposes the trigger conditions under which any given informational practices would be perceived as a privacy issue. Thus, rather than proposing informational practices as sources of privacy concerns, this study suggests that future studies should aim to focus on the underlying trigger mechanisms that are associated with emergence of users’ privacy issues. Lastly, while existing theories of privacy are helpful in understanding the concept of information privacy in general terms, based on the findings of this study, we suggest that future studies should go beyond this high level conceptualizations by designing studies for specific context and attempt to understand the conditions that are associated with the emergence of privacy concerns.
Practical Implications

The results of this study offer important practical implications for privacy practitioners of social networking sites. The findings provide evidence that there exist trigger conditions under which an informational practice can be perceived as a privacy issue from a social networking site’s users’ perspective. Therefore, this study suggests that practitioners should strive to eliminate the trigger conditions to lessen their users’ perceived information privacy issues. Further, since users’ perceived lack of self-efficacy and lack of usability of privacy protection tools are shown to be significant trigger conditions, practitioners can design and propose privacy training and awareness programs to enhance their users’ perceived efficacy as well as to train them to be more effective users of provided privacy protection tools. Practitioners should also work on designing and providing more user-friendly protection tools. Another finding of the study is that technology users may not be capable of perceiving all the practices that may create harm to their information privacy. This finding suggests that protecting information privacy may not be solely left to the responsibility of users. As technology users cannot perceive the entire set of privacy issues and their vulnerabilities, government agencies (e.g., Office of the Privacy Commissioner of Canada), industry leaders (e.g., Facebook, Twitter, MySpace etc.), and consumer organizations (e.g., Privacy Rights Clearinghouse) not only should promote awareness of the potential privacy issues and their vulnerabilities among users but also should establish guidelines for good business practices for online companies and propose and enforce necessary legislations to protect technology users.

Limitations and Future Research Directions

One limitation of this study relates to the data analyzed in this study. Although the selected data collection method provided a very large sample size and a rich dataset to analyze, we did not have any control over the acquired data. The data set helped us understand this complex phenomenon, particularly identifying the privacy issues and triggers conditions. However, as a result of data limitations, relationships discovered among the constructs still have some weaknesses. To unveil the relationships and identify the causal links among the constructs, future research should interview the participants of social networking sites to collect more relevant data. Another important limitation of the study is regarding the generalizability of our results beyond the Facebook domain. While Facebook resembles important characteristics of OSNs, future studies should focus on other OSN services that offer unique socialization features and assess generalizability and/or uniqueness of findings.

Analyzing the user reactions to the terms of a particular privacy policy may have created a bias in explaining the emergence and outcomes of privacy issues in more general terms. Future research can complement the results of this study by utilizing different data collection methods; such as, observing a group of random Facebook users for a period of time and interviewing them in predetermined intervals to understand their use of technology in regards to protecting their information privacy. As some of the privacy issues may also arise during technology uses, such longitudinal studies can be helpful in understanding whether the issues identified in this study were particularly unique reactions to what were written in the privacy policy.

Another research direction can be contacting the Facebook users’ who have participated in this study by posting comments on the privacy policies and understanding the conditions that made them be more cautious about protecting their personal information. Furthermore, as their posting these comments for the attention of Facebook can be considered as a coping mechanism to deal with the perceived privacy issues (Liang and Xue 2009), a fruitful research direction can be to investigate the other mechanisms of coping and how these mechanisms helped them to deal with their perceived privacy concerns.

The results of this study suggest that Facebook users’ may be more successful in identifying some of the informational practices as the source of their privacy problems than others. Similarly, some of the perceived privacy issues are more salient according to the results of this study. Another extension of the research along this line can investigate whether the identified salience effects can be found in other contexts and if so, explain the reasons why some issues are perceived more easily than others by technology users.

Lastly, this study only analyzed the comments posted in English; however, other comments written in other languages remain to be analyzed in other languages. Therefore, future studies can also analyze this data for confirmation purposes. Analysis done with data in other languages may also help us understand cross cultural differences in regards to technology users’ privacy protection behaviours.
References


