12-6-2010

Antecedents and Outcomes of Information Privacy Concerns in Online Social Networking: A Theoretical Perspective

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

芽|Sprouts Working Papers on Information Systems ISSN 1535-6078

Antecedents and Outcomes of Information Privacy Concerns in Online Social Networking: A Theoretical Perspective

Burcu Bulgurcu
University of British Columbia, Canada

Abstract
This article attempts to contribute to the information privacy literature by providing a comprehensive theory on antecedents and outcomes of Online Social Network (OSN) usersâ information privacy concerns. Based on a review of existing literature on information privacy and considering the unique characteristics of OSN setting, this paper develops a conceptual model with 14 propositions. The goal of this theory is twofold: (1) to explicate OSN provider organizationâ s information practices that lead emergence of usersâ information privacy concerns and discuss the specific conditions under which these practices are perceived privacy issues, (2) to identify the behavioural and affective outcomes of usersâ perceived information privacy concerns.

Keywords: information privacy, online social networks, privacy concerns, coping theory, privacy paradox

Permanent URL: http://sprouts.aisnet.org/10-81

Reference: Bulgurcu, B. (2010). "Antecedents and Outcomes of Information Privacy Concerns in Online Social Networking: A Theoretical Perspective," Proceedings > Proceedings of JAIS Theory Development Workshop . *Sprouts: Working Papers on Information Systems*, 10(81). http://sprouts.aisnet.org/10-81

ANTECEDENTS AND OUTCOMES OF INFORMATION PRIVACY CONCERNS IN ONLINE SOCIAL NETWORKS: A THEORETICAL PERSPECTIVE

Abstract

This article attempts to contribute to the information privacy literature by providing a comprehensive theory on antecedents and outcomes of Online Social Network (OSN) users' information privacy concerns. Based on a review of existing literature on information privacy and considering the unique characteristics of OSN setting, this paper develops a conceptual model with 14 propositions. The goal of this theory is twofold: (1) to explicate OSN provider organization's information practices that lead emergence of users' information privacy concerns and discuss the specific conditions under which these practices are perceived privacy issues, (2) to identify the behavioural and affective outcomes of users' perceived information privacy concerns.

Keywords: *information privacy, online social networks, privacy concerns, coping theory, privacy paradox*

1. INTRODUCTION

Privacy of personal information is substantially important to technology users as firms' pervasive use of information technologies make it difficult to have control over information (Dinev and Hart ; Hui et al. 2007; Malhotra et al. 2004; Solove 2001). The extant literature on information privacy has predominantly focused on understanding antecedents and consequences of privacy issues as they relate to utilitarian technologies such as: **1)** electronic commerce and online shopping (e.g., Awad and Krishnan 2006; Dinev and Hart 2006; Hui et al. 2007; Van Slyke et al. 2006; Wirtz et al. 2007); **2)** offline shopping and direct marketing (e.g., Culnan 1993; Culnan and Armstrong 1999; Hine and Eve 1998; Nowak and Phelps 1992); **3)** general Internet use (e.g., Dinev and Hart 2004; Korzaan et al. 2009; Son and Kim 2008), **4)** electronic health (Angst and Agarwal 2009); **5)** financial portals (Hann et al. 2007); **6)** online and mobile advertising (Lwin et al. 2007; Okazaki et al. 2009); and **7)** online browsing and search engines (Egelman et al. 2009a; Hawkey 2007). While these studies have expanded our understanding of the topic area, we yet know little about the emerging issues of information privacy associated with the use of OSNs.

This study aims to contribute to the privacy literature by focusing on the unique and novel conditions of the OSN context and extend our knowledge by proposing a theory to identify the antecedents and outcomes of technology users' information privacy concerns. The proposed theory will attempt to address three main questions:

1. What are the drivers of information privacy concerns in OSN?
2. What are the specific conditions (e.g. individual, organizational) under which technology providers' information practices are perceived as privacy issues by users?
3. What are users' reactions to perceived privacy issues in OSN settings?

The next section presents the motivation and scope of the study. Next, I will present taxonomy of the triggers, enablers, and outcomes of information privacy concerns in OSNs. Finally, I will introduce a conceptual model that includes proposed constructs and present theoretical propositions concerning the relationships among them.

2. MOTIVATION AND SCOPE OF THE STUDY

This study aims to contribute to the literature on information privacy by focusing on OSN settings. The nature of privacy issues, their drivers and outcomes directly depend on a given context (Nissenbaum 2004); therefore, to have a complete understanding of user reactions to information privacy issues, users' privacy concerns should be studied considering the contextual differences (Malhotra et al. 2004). To the best of my knowledge, the issues of information privacy have not yet been systematically examined for OSN settings.

This paper identifies two types of widely utilized information technologies –*instrumental and expressive*—that can be associated with users' information privacy concerns. *Instrumental technologies* refer to technologies that are designed to serve a specific need; such as online shopping, web browsing, online banking etc. These technologies acquire user input in order to operate and provide value. *Expressive technologies*, on the other hand, are individuals' expressing themselves. The most common example is social networking which is defined as a social structure made of individuals (or organizations) that are connected by one or more specific types of interdependency, such as friendship, intellectual knowledge, financial exchange, professional relationships.

Although many similarities may exist between instrumental and expressive technologies in terms of users' information privacy concerns, OSN settings may constitute significant

differences in the way privacy concerns emerges due to its unique and novel characteristics. In the following, I will discuss several contextual differences that make expressive technologies a more fertile ground for privacy invasions compared to instrumental technologies.

Purpose of Technology Use: The purpose of using an instrumental technology is mostly receiving an extrinsic benefit; such as a service or good. For example, users' main goal in an e-commerce site is shopping, in an e-banking site is financial transactions, and in an electronic health record system is to enter or search for patience information. Therefore, in an instrumental setting, users disclose personal information in return for gaining a self benefit and/or maximizing their net utility. Users' primary purpose of using an expressive technology is socialization; such as – keeping in touch with friends, following social events, sharing parts of personal lives etc. Therefore, in an expressive setting, users disclose personal information only if they want to increase their level of socialization on the platform.

Purpose of Data Disclosure: In a utilitarian setting, users may or may not be willing to disclose their personal information; however, to receive the provided service or goods they are mostly required to do so. For example, users may be asked to disclose personal information to receive more personalized service or gain a financial incentive. However, in expressive settings, users disclose their personal information voluntarily, only if they are willing to enhance the level of their socialization on the platform.

Type of Information Exchange**:** The personal information at stake (that could be lost through a privacy breach) is different in the two contexts. In the utilitarian context, it is 'basic' personal information such as name, address, and credit card details, whereas in the expressive context is all types of personal information that one uses for self-representation. As the interaction is between the firm and the user in a utilitarian context, and personal data is not

openly disclosed through the platform, management of self-identity is not an issue. However, management of self-identity is important in expressive settings, as personal data is openly disclosed to different parties.

The Nature of Trade-off (Benefits and Costs)*:* Utilitarian technologies mostly provide extrinsic benefits; such as, convenience, personalization, and financial benefits; whereas, expressive technologies mostly provide intrinsic benefits; such as higher levels of socialization, enjoyment, and fun. The cost of technology use would be privacy concerns in both settings, even though the nature of cost could be slightly different. Although there would be emotional costs of privacy breaches in both contexts, the cost of a privacy breach could be higher in a social context because a loss of face would presumably have a bigger emotional impact than a loss of basic personal information. The problems associated with use of expressive technologies can also be more widespread than those in instrumental technologies, spanning from personal life problems (Justice 2007), to career liabilities (Jones and Soltren 2005; Rosenblum 2007), to reputation damage (Survey 2009). Thus, the nature of trade-off would be different in both settings, as in a utilitarian setting (extrinsic benefit - privacy tradeoff), the cost and benefit are qualitatively different (high in utilitarian benefit and low in emotional cost), whereas in an expressive setting (intrinsic benefit - privacy tradeoff), cost and benefit are qualitatively the same (high in emotional benefit and high in emotional cost).

Types of Interactions and Characteristics of Interacting Parties*:* In a utilitarian context, the interaction and information exchange is usually held in a two-way interaction, which is between the firm and the individual. In an e-commerce context, for example, even though third parties are involved in the process (i.e. intermediaries, transport companies, and producers) consumers are not involved in these interactions. In an expressive setting, the interaction and information

exchange is mostly in between users of the network. However, the technology provider firm usually has full control over exchanged information as the firm holds the service and designs the technology. The interactions are complex in an expressive setting, as there are multiple two-way interactions (i.e. between the user and the service provider firm, between the user and the third parties that run on the online platform, between the firm and the third parties that interact with users, and among platform users).

Ubiquity of the technologies, time and spatial flexibility: In a utilitarian context, such as e-commerce, consumers adopt the technology with a specific purpose and when they satisfy their need, they discontinue using the service. Thus, time to interact with the technology is usually limited. In expressive settings, however, technology is usually part of users' daily lives and interaction time is much broader. Also, mobile devices provide a spatial flexibility to use the service everywhere and technology use becomes more ubiquitous compared to utilitarian technologies.

3. PROPOSAL OF A THEORETICAL MODEL

Technology users' information privacy related trade-offs have been identified as the major drivers of information privacy concerns in the extant literature. Based on the expectancy theory (Vroom 1964), this literature suggests that individuals explicitly consider the trade-off by assessing the potential positive (perceived benefits, such as financial gains or convenience) and negative (perceived costs, such as privacy concerns or invasion) outcomes before disclosing personal information and behave to maximize their net gains (Culnan and Armstrong 1999; Dinev and Hart 2006; Laufer and Wolfe 1977). Therefore, most of the earlier empirical studies investigating technology users' information privacy behaviors suggested that perceived net gains of technology use determine users' adoption of the technology or their willingness to provide

personal information for transactions. Some of the constructs that were associated with the positive outcomes of users' privacy calculus are perceived importance of personalization (Awad and Krishnan 2006; Chellappa and Sin 2005), personal Internet interest (Dinev and Hart 2006), trust and trust building factors; such as, familiarity and experience (Chellappa and Sin 2005; Hine and Eve 1998), and direct benefits; such as, monetary gains (Hui et al. 2007) and convenience (Hann et al. 2007; Hui et al. 2007). On the other hand, privacy concerns and perceived privacy risks (Awad and Krishnan 2006; Chellappa and Sin 2005; Dinev and Hart 2006), previous online privacy invasion experience (Awad and Krishnan 2006), lack of information transparency (Awad and Krishnan 2006), and lack of a (clear) information privacy policy (Awad and Krishnan 2006; Hann et al. 2007; Hui et al. 2007) are the example variables that were associated with negative outcomes considered as part of users' privacy calculus.

Table 1: Summary of findings for studies that utilized the trade-off perspective

Studies	Independent Vars.	Dependent Vars.	Main Findings
Awad and Krishnan 2006 (E-Com)	▪ Perceived importance of information transparency ▪ Previous online privacy invasion ▪ Importance of privacy policies	▪ Willingness to be profiled online for personalized service ▪ Willingness to be profiled online for personalized advertising	Consumers were more willing to partake in online personalization (compared to advertising) even in the presence of privacy concerns or previous negative experience as they see a benefit in personalization.
Chellappa and Sin 2005 (E-Com)	▪ Value for personalization ▪ Trust building factors (familiarity and experience)	▪ Likelihood for using personalized services	▪ Trust building factors were found to be negatively correlated with privacy concerns. ▪ Personalization value had a significant positive effect on likelihood of using personalized services.
Hann et al. 2007 (Financial Portals)	▪ Offering privacy policies regarding the handling and use of personal information ▪ Offering benefits such as financial gains	▪ Registering with the website ▪ Providing personal information	▪ Privacy policies (assures appropriate secondary use, review of personal information for mistakes, prevention of improper access) were valued by users.

	or convenience		▪ Convenience – through personalization and lowering of frictional costs – helped mitigate privacy concerns. ▪ Financial incentives were persuasive means to elicit personal information.
Hui et al. 2007 (E-Com)	▪ Existence of privacy statement ▪ Monetary incentive	▪ Disclosure of personal information	▪ The existence of a privacy statement induced more people to disclose their personal information to a website. ▪ Monetary incentive had a positive influence on disclosure.

Based on the extant information privacy literature that adopts the expectancy value theory (Vroom 1964), this paper suggests that OSN users' perceived net gains determine their privacy related behavioral responses. Recently Krasnova and Veltri (2010) proposed that users' self-disclosure on social networking sites depends on their perceived net gains (defined as privacy calculus) and empirically investigated the impact of cultural factors on users' perceived benefits and costs. Similarly, this paper aims to extend the knowledge about users' privacy calculus on OSN sites and asks the trade-offs that are made by the users of OSN sites. While I believe that perceived costs of using an OSN site will be similar to those of using other technologies mentioned in the literature (i.e. privacy concerns, previous privacy invasions), perceived benefits will be different. The benefits gained by using other technologies (i.e. monetary incentives, convenience) cannot be the antecedents of social networking sites' use. Rather, socialization (i.e. creating and maintaining social connections, re-connecting with old friends, following and promoting social events), expression and promotion of self identity, keeping a life memory, and fun and entertainment (i.e. social setting, social games) are some of the most common causes of OSN use (Ellison et al. 2007). Hence, on the benefit side, users enjoy the online socialization offered by OSN sites. Yet, this benefit may be countermanded by the increased information

privacy risks associated with disclosing information online. In view of that, this study suggests two important trade-off factors: (1) perceived socialization (related to information practices) on a social networking site; and (2) perceived concerns for information privacy (CFIP) regarding the online company's information practices.

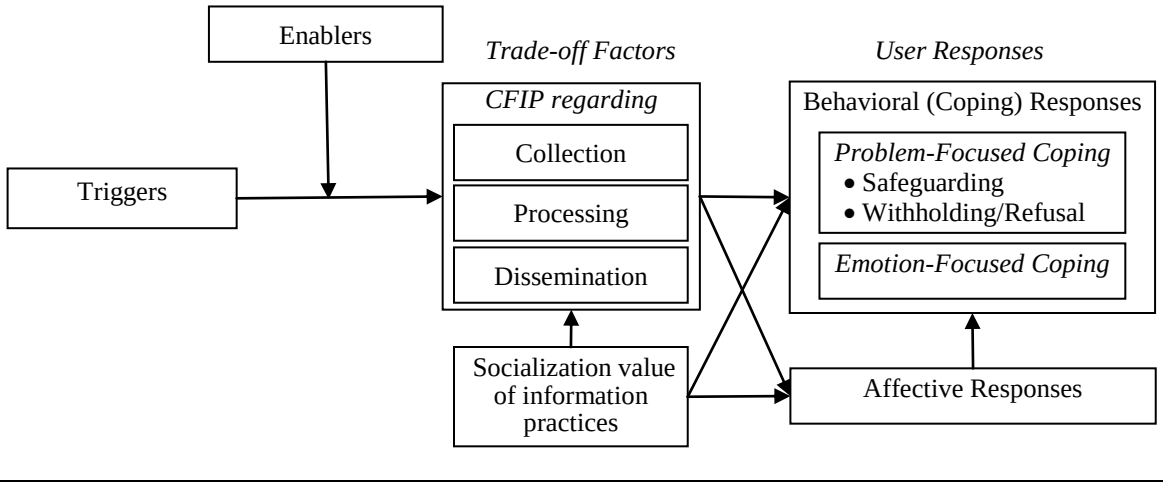

Figure 1: A Theory for Emergence and Outcomes of Information Privacy Concerns in Social Networking

3.1. Perceived privacy concerns regarding information practices

Previous research has suggested several different dimensions for information privacy concerns. Based on Solove's taxonomy (2008), this paper proposes three types of information practices as dimensions of information privacy concerns: (1) Collection, (2) Processing, (3) Dissemination.

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 online social networks—(1) they may be influential in increasing

users' perceived level of socialization on the networking site, and (2) they may be influential in increasing users' information privacy concern. An online social network'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, online social network 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, this paper introduces these practices not only as the source of information privacy concerns (negative trade-off factor), but also as the source of perceived of socialization (positive trade-off factor).

In the following, I will briefly explain these practices and how they are influential in increasing both benefit and cost perceptions of users' trade-offs.

3.1.1. Collection

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). While acknowledging these studies argument that collection of personal information is an important dimension of

privacy concerns, this paper also propose data collection as a necessary practice to increase perceived level of socialization on the OSN site.

3.1.2. Processing

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 OSN 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).

3.1.3. 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 OSN 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 OSN (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 OSN 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 online social networks. 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.

3.2. Perceived socialization on the social networking site

Socialization is central to the use of online social network site (Ellison et al. 2007). Enjoyment of socialization via self-representation and relationship maintenance are suggested as strong drivers of users' participation and self-disclosure to online social networks (Krasnova and Veltri 2010). Thus, I will propose the user's perceived socialization as the benefit factor in the trade-off. I believe that this construct strongly differentiates itself from other benefit factors of privacy calculus frameworks that were proposed in the extant literature, as it is unique to OSN setting.

Next, I will identify conditions that trigger users' information privacy concerns (*triggers*) and conditions that lead formation of them (*enablers*). Although each condition in a given set does not have to be present for emergence of a user's information privacy concern, I believe that, the existence of each would make its emergence incrementally likely. In the remainder of this section, I will first discuss the conditions that trigger information privacy concern and then those that enable emergence of it.

3.3. Trigger Conditions

I posit that existence of trigger conditions lead the user think about his information privacy when he uses the OSN site and thus, trigger user awareness about potential privacy issues. As a result, user will be more sensitive to privacy issues and more likely to perceive an information practice as a privacy issue. I believe that these conditions are particularly important for the context of OSN due to this setting's complexity.

3.3.1. Rapid changes in the legal framework (towards less privacy protective terms)

It is very common to observe online social network sites announcing a series of policy changes. There are a number of reasons for these revisions: (1) OSN platform involves more dynamic and complex processes compared to other platforms. According to rapid changes of business requirements, firms regularly update their privacy policy terms. For example, Facebook's recent introduction of social shopping (a mix of e-commerce and traditional shopping where consumers shop in a social networking environment) lets consumers swap ideas and share product reviews and discuss latest fashion trends with like-minded people before and after the decision making and purchasing processes. While this could be an extremely useful tool for users who like experience online shopping in a social context, the required policy changes for the introduction of this application may also introduce new privacy concerns. (2) It is also common that as the popularity of the platform increases, the firm that owns the OSN platform gains more power and enforce new policy terms that would be beneficial for their business. One of the significant examples of this is the evolution of Facebook's default privacy settings toward becoming a more open platform (McKeon 2010). (3) It is also possible the firm revises its policy according to the changing user needs.

However, when these revisions are too rapid, it gets extremely difficult to follow proposed changes for platform users. Further, it gets difficult for the online firm to inform all platform users about the changes and have their consent. In particular, when proposed policy changes shift from a better privacy protective option to a less protective one, users' information privacy concerns are likely to increase. For example, recently Facebook revised its privacy policy and acknowledged that the social network will store financial account information its users use to make purchases on its site unless you tell it not to (Facebook 2010). Such a

substantial change in the policy regarding users' opt-in/out preferences about their financial information resulted in emergence of general privacy concerns about the platform.

3.3.2. Lessened user controls

The ability of the user to control his personal information is an important antecedent of information privacy concerns as it helps the user perceive that potential risks and negative consequences are alleviated (Dinev and Hart 2004). Organizational procedures and technology based tools provided by the organizations allow the user to control the collection, processing, and dissemination of his personal information. It is known that when control is not allowed or when the future use of information is not known, individuals resist data disclosure or technology use (Culnan 1993; Dinev and Hart 2004; Malhotra et al. 2004; Phelps et al. 2000). I suggest that the user's losing necessary privacy controls which are previously available to protect his personal information could be a strong trigger factor. For example, Facebook is often criticized by its users and privacy experts for constantly removing previously available privacy controls and enforcing new settings. With the introduction of privacy policy revisions in 2009, Facebook users lost their control over their so called public information (previously they were called personal information) – name, profile picture, demographics, location, and friend list – and the new controls forced them to disclose their information to everybody rather than allowing them disclose their information according to their preferences (Facebook 2010). I suggest that losing previously available privacy controls is a critical factor that could trigger users' awareness on privacy and so result in emergence of privacy issues.

3.3.3. Perceived vulnerability of other users

One of the unique characteristics of OSN sites compared to other contexts is users' likelihood of observing others' (i.e. friends, strangers, and individuals in the same network) online profiles and assessing their vulnerabilities to privacy related risks. A recent study by Debatin et al. (2009) investigates user privacy attitudes and behaviors on Facebook and mentions two relevant constructs – negative incidents to oneself and those perceived by others. They find that Facebook users are more likely to perceive risks to others' privacy rather than to their own privacy. Therefore, I propose a user's perceived vulnerabilities of other OSN users as an important and novel construct and suggest that it would be significant in explaining the user's privacy concerns. In particular, I suggest that the user's perceived privacy vulnerabilities of other users will trigger his awareness on privacy issues and result in increases in his perceiving future privacy issues.

3.3.4. Perceived relevance of requested/disclosed data to the primary purpose of technology use

Perceived relevance refers to the user's perception that information being collected and used is relevant to the transaction context (Lwin et al. 2007) such that the data collector firm only collects and use the necessary data to serve the original purpose of transaction. When users perceive that the firm collects data that would directly serve his needs (i.e. required customization of service), they will be less likely to attribute the collection practice to a privacy issue (Graeff and Harmon 2002). Information privacy literature that focus on other settings discusses the perceived relevance construct in different forms; such as, perceived legitimacy of information requests (Hine and Eve 1998), perceived congruency of information to the interaction context (Lwin et al. 2007), consumer knowledge on relevance of collected data (Nowak and Phelps 1997a), the amount of information requests (Hui et al. 2007; Stewart and

Segars 2002), purpose of usage of the collected data (Sheehan 2002), and procedural fairness (Culnan and Armstrong 1999). These studies associated perceived relevance construct with an increase in privacy concerns and a decrease in online transactions and/or purchases. For the OSN context, these findings imply that a user would be less concerned about his information privacy when he perceives that the amount and the nature of information requests are congruent with his primary purpose of using the technology. For example, a third party application on Facebook (i.e. a birthday reminder application to remember friends' birthdays) may need to capture personal data from the user's profile to function. However, if the user perceives that such an application captures more information that it would need (i.e. location information), this would trigger emergence of his privacy concerns.

3.3.5. Type of requested/disclosed data (sensitive and user specific)

Previous research suggests the type of requested personal information as a contextual variable and propose its direct effect on an individual's risk beliefs and behavioral intentions (i.e. willingness for registration, disclosing information, transaction) (Chellappa and Sin 2005; Malhotra et al. 2004; Meinert et al. 2006; Phelps et al. 2000). As the technology user's perceived potential for loss or harm would directly dependent upon the type of information disclosed (Meinert et al. 2006), it might be reasonable to suggest that type of collected data would affect the user's information privacy concerns. Previous studies propose two constructs as types of data that could affect individuals' information privacy concerns – *data sensitivity* and *data specificity*. In particular, these studies argue that an individual's information privacy concerns are increased by his perceived level of sensitivity of the collected data (Cranor et al. 2000; Okazaki et al. 2009; Sheehan 2002; Sheehan and Hoy 2000) and his perceived level of specificity of information (i.e., the degree to which it was directly traceable to the individual, such as collection of individual vs.

group level data; anonymous vs. non-anonymous data) (Cranor et al. 2000; Nowak and Phelps 1992; Nowak and Phelps 1997a). The results of these studies suggest that the greatest potential threats to individuals' information privacy involve sensitive information that is directly associated with specific individuals (personally identifiable, non-anonymous data). A recent study by Lwin et al. (2007) investigates the moderating role of information sensitivity and finds that although a strong business policy is effective in reducing concern when companies collect low sensitivity data, it is insufficient in reducing concern for highly sensitive data.

3.3.6. Perceived responsibility of the firm

The power-responsibility equilibrium model suggests that power and responsibility should be in equilibrium (Davis et al. 1980). This model suggests that partner in a relationship with more power also has the responsibility to ensure an environment of trust and confidence. According to the model especially large and powerful firms should have ethical responsibilities to their customers; otherwise, selection of a strategy of greater power and less responsibility will be harmful to the company in the long run as consumers will take defensive action. A recent survey presents that individuals feel businesses and governments are not doing enough to protect their privacy (GILC 2010). Wirtz et al. (2007) proposed policy and regulation as two general categories of power-yielding influences reducing consumers' online privacy concerns and found that the greater the perceived responsibility of an organization concerning online privacy protection, the lower is the consumer's online privacy concern. The proposed link between perceived levels of firm's responsibility and users' information privacy concerns becomes more important for the context of OSN, as interactions among relevant parties are more complex. OSN users not only expect that the firm is responsible of its own actions but also the businesses that run under its platform (i.e. third party applications, advertisers, application and game

developers). Especially, the firm's allowance of malicious/inappropriate advertising and applications on its platform could trigger its users' privacy concerns as they feel that the firm should be responsible of all actions of third parties that run on its platform. For example, when the user's faces with the negative consequences of a phishing attack performed by a third party application that runs on Facebook, his likelihood to perceive future information practices as privacy issues will be increased.

Propositions: I propose the following propositions regarding the impacts of triggers:

Users will be likely to attribute an information practice to a perceived privacy issue when

(1) they perceive that the legal framework rapidly changes towards less protective terms,

(2) their perceived ability of controls are lessened,

(3) they perceive vulnerabilities of other users,

(4) they perceive that requested/disclosed data are irrelevant to the primary purpose of technology use,

(5) they perceive that requested/disclosed data are sensitive and/or user specific, and

(6) they perceive that the firm do not act responsibly to protect his data from risks that come from third parties that run on its platform.

3.4. Enabler Conditions

I will propose four enabler conditions and suggest that users' information privacy concerns could be strengthened with the lack of (or alleviated with the existence of) these conditions. Enabler conditions are different from triggers in the sense that they require the user's conscious awareness of the OSN site's information practices. Thus, these conditions are inherently firm specific and are mostly specified in privacy policies of OSN sites. While the impact of existence and/or effectiveness of privacy terms (i.e. privacy policies, privacy seals, legal frameworks) on

reducing privacy concerns was investigated by many studies (Awad and Krishnan 2006; Hann et al. 2007; Hui et al. 2007; Lwin et al. 2007; Meinert et al. 2006; Miyazaki and Krishnamurthy 2002; Moores 2005; Wirtz et al. 2007), this paper focuses on specific conditions that should be clarified within the privacy policies.

3.4.1. Perceived Transparency: Awareness and notice principle

Transparency refers to the data collector firm's explicit disclosure of its information practices (i.e. data collection, processing, and use) before taking any action regarding users' data (FCT 2000). Transparency inherently refers to *notice and awareness principle*, one of the most important recommended principles of privacy policies (Jamal et al. 2003), which suggests that users should explicitly be informed about the firm's information practices regarding collection, processing, and dissemination of his personal data. Some of the important information practices of the firm that are expected to be disclosed are as follows: (1) Types of information collected through the website – what kind of information is the firm collecting about the user?, (2) Methods of data collection (i.e. direct questions, ubiquitous methods such as tracking the user with cookies over a period of time) – how and when is the firm collecting my data?, (3) Purpose of data collection– why is the firm collecting this particular data about me?, (4) Data processing and dissemination practices – what is the firm doing with my personal data that are collected? Would my data be used for identification purposes? Are there any undisclosed practices regarding processing and dissemination of my data?, (5) Duration of data storage – How long the firm will retain collected data in its database?, (6) Aggregation principles with data obtained from third parties – Are my personal data be sold to third parties for aggregation purposes? Is the firm aggregating the collected data with others coming from other sources for identification

purposes?, (7) Third parties who collect data on the Web site – Who else can collect, reach, and/or use my data collected through this particular platform?.

There are many studies in the privacy literature that investigate the transparency construct (sometimes by proposing slightly different variables). For example, a study by Awad and Krishnan (2006) focuses on whether information transparency features have an effect on consumer willingness to be profiled online and finds that consumers who rate information transparency as important are more cautious of sharing personal information and therefore less willing to participate in online profiling. Another recent study (Pavlou et al. 2007) suggests that website informativeness, which is defined as the degree to which buyers perceive that a website provides them with resourceful and helpful information, can overcome the information asymmetries created by the spatial and temporal separation of the online environment and solve the problem of hidden information by enabling buyers to learn more about the seller's characteristics, products, and information practices and thus, mitigate different types of uncertainties. They found that website informativeness strongly mitigated buyers' information privacy concerns, along with other proposed buyer concerns. A survey study by Cranor et al. (2000) revealed that the lack of transparency of the utilized data collection methods is strongly associated with increases in Internet users' information concerns. For example, web sites' collecting email addresses from visitors without consent to compile email marketing lists and tracking their visit and using that information improperly are suggested as serious privacy issues. Another study by Hine and Eve (1998) showed that, in the absence of straightforward explanations on the purposes of data collection, people were attributing unfavorable organizational motivations to the data collector organization. They suggested that clear and readily available explanations might alleviate some of the unfavorable speculations regarding

organizations' information practices. Similarly, other studies by Nowak and Phelps (1997a) and Sheehan (2002) focus on marketing context and suggest that privacy concerns could be alleviated by ensuring appearance of the marketing firm's information practices and data collection method, requiring consumer consent, and/or requiring voluntary consumer participation.

3.4.2. Perceived Procedural Control: Choice and consent principle

Control refers to the ability of the user to control his personal information, especially against undesired information practices and their negative consequences (Altman 1975; Dinev and Hart 2004). Control of personal information requires that an individual manages the outflow of information as well as the subsequent disclosure of that information to third parties (Hann et al. 2007). Control also refers an important recommended privacy policy principle, so called *choice and consent* (Jamal et al. 2003). Choice and consent principle suggests that technology users must be given options with respect to (1) whether and (2) how personal information collected from them may be used for purposes beyond those for which the information was provided (FTC 2000). Some of the required controls are: (1) Availability of explicit opt-in and/or comprehensive opt-out options; (2) Availability of option to restrict the use of personal information collected.

Many studies in online and offline marketing reported that technology users perceive privacy concerns when they are not granted sufficient control on the collection, storage, use, and disclosure of their personal information (Culnan 1993; Dinev and Hart 2004; Malhotra et al. 2004; Phelps et al. 2000), and such perception deter them from disclosing their personal information and/or utilizing these technologies. (Phelps et al. 2001). Milne (2000) suggests that privacy is enhanced when consumers are aware of information practices and are given a choice

over information provision and use. Companies' not providing a choice to the user regarding the secondary use of his personal data (i.e. sharing personal information with other companies without receiving authorization from the user who provided the information) was also found to be a significant information privacy concern dimension (Stewart and Segars 2002).

3.4.3. Access

Access refers to (1) the user's ability to view and contest the accuracy and completeness of data collected about him and (2), if he finds it necessary, his ability to remove the data from the company's database (Cranor et al. 2000). Access is proposed as an important factors to contribute to the perceived fairness of information practices (FTC 2000) and expected to alleviate users' information privacy concerns (Culnan 2000).

3.4.4. Security

Lack of security refers to the users' perceived insecurities regarding the company's data collection and storage practices and his perception that the company will fail to protect his personal data from internal or external access. Data collectors' failure to assure that users' personal information is protected and secure from unauthorized internal and external use would increase users' information privacy concerns (Stewart and Segars 2002).

Propositions: I propose the following propositions regarding the impacts of enablers:

(7) Transparency, (8) Procedural control, (9) Access, and (10) Perceived security reduce attribution of an information practice to a privacy issue.

3.5. User Responses

In this section, I will first list the important consequences (outcome variables) of users' information privacy concerns proposed in the extant literature of privacy along with the contexts

investigated. Table 3 presents this summary. The variables are found to be negatively affected by privacy concerns unless otherwise indicated. Then, I will propose my taxonomy for outcomes of information privacy concerns that are relevant to the context of OSN.

Table 2: Summary of privacy related outcome variables in the literature

Studies	Contexts	Outcome Variables
Angst and Agarwal 2009	E-Health	Opt-in Intention for e-health record use
Awad and Krishnan 2006	E-Com	Willingness to be profiled online for personalization
Chellappa and Sin 2005	E-Com	Likelihood for using personalized services
Culnan 1993	Direct marketing	Attitude toward secondary information use
Culnan and Armstrong 1999	Offline consumer transactions	The firm's attracting and retaining customers
Debatin et al. 2009	Online social networking	Change in privacy settings
Dinev and Hart 2006 Hann et al. 2007 Hui et al. 2007 Meinert et al. 2006 Malhotra et al. 2004	▪ E-Com ▪ Financial portals	Registering with a website Disclosure of personal information (willingness/intention)
Dinev and Hart 2005 Hine and Eve 1998 Pavlou et al. 2007 Phelps et al. 2001 Van Slyke et al. 2006	▪ E-Com ▪ Offline Commerce	Transaction (or purchase) intention
Miyazaki and Fernandez 2001	Online shopping	Willingness to pay for privacy Online purchasing rate
Egelman et al. 2009b	E-com	Willingness to examine multiple websites to find a better privacy protective option
Korzaan et al. 2009	Internet use	*Behavioural intentions* ▪ refuse to give information, ▪ take action to remove name, ▪ refuse to purchase
Lwin et al. 2007 Wirtz et al. 2007	Online Advertising	*Individual Responses* ▪ *Fabricate*: Misrepresentation of personal information ▪ *Protection*: Adoption of privacy protection technologies ▪ *Withhold*: Refusal to purchase from (or register to) a web site
Malhotra et al. 2004	▪ E-Com	▪ Trusting beliefs

Okazaki et al. 2009	▪ Mobile Advertising	▪ Risk beliefs
Pavlou et al. 2007	E-Com	▪ Perceived Uncertainty
Sheehan and Hoy 1999 Sheehan 2002	Online Advertising	▪ Notifying ISP about unsolicited e-mail ▪ Requesting removal from maligning list ▪ Flaming senders of unsolicited e-mail ▪ Registering for web sites ▪ Providing incomplete data during registration ▪ Providing inaccurate data during registration
Son and Kim 2008	Internet Use	▪ Refusal (information provision) ▪ Removal (private action) ▪ Negative word-of-mouth (private action) ▪ Complaining directly to online companies (public action) ▪ Complaining directly to 3rd party organizations (Public action)

Considering the summary table, I will propose two types of outcomes for information privacy concerns: *Affective* and *Behavioral (Coping) Responses.*

3.5.1. Affective Outcomes

Several affective outcome variables that were proposed in the privacy literature could be applicable to social networking.

- Perceived distrust to the company
- Perceived dissatisfaction
- Perceived uncertainty
- Perceived insecurity

3.5.2. Behavioral Outcomes

Attempting to understand human behavior under IT threats, Liang and Xue (2009) propose two types of coping behaviors – *emotion based coping* and *problem based coping*. They suggest the following: *"Problem-focused coping refers to adaptive behaviors that take a problem-solving approach to attempt to change objective reality. It deals directly with the source of the threat by*

taking safeguarding measures (e.g., installing safeguarding IT, disabling cookies, updating passwords regularly). After the measures take effect, users' perception of their current state is further away from the undesired end state, thus reducing the threat. In contrast, emotion-focused coping is oriented toward creating a false perception of the environment without actually changing it or adjusting one's desires or importance of desires so that negative emotions related to threat (e.g., fear and stress) are mitigated. This coping reduces perceived threat or motivation of coping with the threat without changing objective reality."

Based on coping theory (Lazarus 1966; Lazarus and Folkman 1984), they propose two cognitive processes that users are involved: threat (primary) appraisal and coping (secondary) appraisal in their proposed theory of technology threat avoidance. This theory posits that users' threat perception leads to coping appraisal, in which users assess the degree to which the IT threat can be avoided by taking safeguarding measures based on perceived effectiveness and costs of the safeguarding measure and self-efficacy of taking the safeguarding measure. When users' are motivated to avoid malicious IT when they perceive a threat and believe that the threat is avoidable by taking safeguarding measures (problem-focused coping); if users believe that the threat cannot be fully avoided by taking safeguarding measures, they would engage in emotion-focused coping.

Based on the technology threat avoidance theory (Liang and Xue 2009), I propose that a user's privacy concern will lead to two types of behavioral responses: problem-focused and emotion-focus coping. As an extension to their theory, I suggest two types of problem-based coping responses: *safeguarding* and *withholding*. In parallel with the technology threat avoidance theory, I suggest that users of an OSN platform can perform problem-focused coping,

emotion-focused coping, or both. Several mechanisms can play role in users' selection of their coping behavior. I will articulate each coping mechanism in the following sub-sections:

Problem focused coping – Safeguarding responses: If users identify a safeguarding option that is likely to reduce the threat of malicious IT, they will try problem-focused coping first (Liang and Xue 2009), as adopting safeguarding options can bring them the most valued outcome (Vroom 1964). Thus, I suggest that adopting safeguards towards protecting his personal information would be the best option for the rational OSN user, as this strategy not only be helpful in objectively reducing his privacy concerns but also allow him continue enjoying the OSN platform without any limitations. This strategy requires the user's adoption and effective use of privacy protective technologies, such as:

- Adopting privacy controls on the platform
- Adopting additional protection tools offered by third parties (i.e. software to check privacy settings)
- Adoption of privacy controls outside the platform (i.e. private browsing, turn-off location information of mobile device)

Problem focused coping – Withholding/Refusal responses: Another problem-focused coping that users would commonly intend could be withholding/refusal. This type of coping involves the user's full or partial refutation of the service. Liang and Xue (2009) suggest two antecedents for threat avoidance motivation-- perceived threat (i.e. severity and susceptibility) and perceived avoidability (i.e. perceived effectiveness, perceived costs, and self-efficacy) and suggest avoidance motivation as the direct driver of avoidance behavior. Considering their argument, I believe that the user's withholding/refusal responses would particularly occur when his

perceived threat is high and perceived avoidability of the threat is low. For example, when the user perceives that the threat could be critically harmful to his information privacy but perceives that his efficacy is not commensurate to effectively using technological controls and prevent the potential threat or he perceived that the cost of his prevention attempt will be too high, he may decide to withhold/refute using the service. This strategy would not be as useful as the previous one, as he has to either fully or partially trade-off his enjoyment of using the service, even though it may be effective in preventing the potential threats. Some of the examples are:

- *Refusing to register and release information*: Willingness to register and release information is one of the important dependent variables that are investigated in the extant privacy literature (Dinev and Hart 2006; Hann et al. 2007; Hui et al. 2007; Meinert et al. 2006; Malhotra et al. 2004; Son and Kim 2008). I believe that it can also be an important outcome variable for social networking context.
- *Quitting the platform*: Removal of personal information (Smith et al. 1996; Son and Kim 2008) and quitting the online platform could be a strong private response. For example, sixty percent of respondents to a survey say they are considering quitting Facebook due to privacy fears (Sophos Poll 2010).
- *Withholding information release*: As the less extreme alternative of quitting the platform, Facebook users' are often advised to disclose the minimum required personal information to continue using the service if they need to stay available to friends using its service.
- *Quit third party applications*: Third party applications that run on the social networking platform are deemed to be a significant driver of user's privacy concerns. Users who are particularly sensitive about third party applications' information practices could resign from using their services.

- *Limiting socialization*: Users' privacy concerns may also result in their limiting socializations on the platform. For example, the user who is concerned about his communication privacy and who does not like his communication scripts to be available to all friends may choose not to use friends' walls or completely remove his wall to prevent his friends' connecting him with public messages.
- *Terminating connections*: Friend's privacy settings may affect a user's information privacy through third party applications. For example on Facebook, the user may decide to disclose certain information to a particular his friend. However, if the friend utilizes a malicious third party application without setting privacy controls to determine the data that could be accessible by that application, it is possible that application could reach all the data that is made accessible to the friend. Thus, the user may perceive certain friendship connections harmful to his privacy and may decide to terminate them. Similarly, Facebook's making its users' "Fan Pages" and "Networks" data public to everyone in 2009 resulted in many users terminating their connections with those pages or networks.
- *Misrepresentation of personal information*: Another common coping strategy on social networks could be fabrication of information (by providing inaccurate or incomplete information), which has also been mentioned by previous studies (Lwin et al. 2007; Son and Kim 2008; Wirtz et al. 2007). For example, Facebook enforced certain profile information (i.e. name, profile picture, location etc.) to be publicly available to everyone in 2009. Most users, who were not satisfied about losing control over their personal data, either removed this type of information from their profile or fabricated them because certain information was required to be released to use the service (i.e. birthday).

Emotion focused coping: Liang and Xue (2009) suggest that creating emotion focused coping creates false perception of the environment without actually changing it or adjusting one's desires or importance of desires. While it may not be a direct solution to their problem, it may be helpful in mitigating users' negative emotions (e.g., fear and stress) related to their concerns.

- *Joining online communities*: It is very common that users join online communities to share their negative experiences and feelings, inform other users with the insight they gained, or sometimes to gain power for public action. There are many websites on the Internet used for this purpose. For example, a website called quitfacebookday.com accuses Facebook of being inconsiderate about users' personal data and helps the site visitors to quit the platform.
- *Complaining to others (negative word-of-month)*: Another form of coping could be users' negative word-of-mouth communication—sharing negative experiences with friends and relatives—to damage the company's reputation (Son and Kim 2008), which could be a strong tool with today's communication technologies.
- *Complaining directly to online companies:* The user who is concerned about his privacy can directly connect to the online company (Son and Kim 2008). In Facebook example, users can communicate with the company through the official Facebook page of the company and also post comments to the terms of a released privacy policy within a time period.
- *Complaining indirectly to third-party organizations:* The user can also complain to independent third-party privacy groups (i.e. TRUSTe, Privacy Commissioner of Canada) or engage in privacy litigation (Son and Kim 2008). While the user's action may not be directly influential on reducing his privacy concern in the short term, third-party organizations may be quite influential on information practices of online companies in the long term. For example, for a number of critical issues, Privacy Commissioner of Canada was successful in enforcing

its proposed changes to Facebook's privacy practices and ensuring the company policy's compliance with Canadian law.

Propositions: I propose the following propositions regarding user responses:

(11) Users may employ either problem- focused or emotion-focused coping to reduce their information privacy related concerns.

(12) When users have the ability, they perform safeguarding-based problem-focused coping to mitigate the negative consequences of privacy issues and continue using the OSN platform.

(13) When users do not have the ability, they perform withholding/refusal-based problem-focused coping to mitigate the negative consequences of privacy issues and limit or discontinue using the OSN platform.

(14) Users perform emotion-focused coping to subjectively reduce their privacy concerns.

4. CONCLUDING REMARKS

In this paper, I first discussed the unique conditions of online social networks compared to other technologies. Then, I developed a theory base on users' privacy-socialization trade-offs and presented a set of theory-based propositions concerning the drivers and outcomes of users' information privacy concerns in OSN settings. The propositions provide answers to the three research questions that initially motivated the paper. In particular, I suggested several factors that impact users' information privacy concerns in OSN settings—rapid changes in the framework, lessened user controls, perceived vulnerability of other users, perceived relevance of disclosed data, type of disclosed data, and perceived responsibility of the firm. I also categorised user responses based on coping theory (i.e. behavioural and affective responses), and suggested several user reactions to perceived privacy invasions. The answers should be of interest to

academic researchers, designers, and current or potential providers of OSN service provider organizations. From the theoretical perspective, the proposed theory attempts to be the first comprehensive study in the literature to help understand the context specific and novel issues of information privacy for the context of OSN. From the practitioner perspective, the proposed theory aims to provide managerial guidance to practitioners in evaluating their information practices according to OSN users' responses to privacy issues, developing and evaluating more effective information privacy policies, and designing necessary privacy protection tools.

5. REFERENCES

Altman I. 1975. The environment and social behavior. Monterey, CA: Brooks/Cole.

Angst CM, and Agarwal R. 2009. Adoption of Electronic Health Records in The Presence Of Privacy Concerns: The Elaboration Likelihood Model and Individual Persuasion. MIS Quarterly 33(2):339-370.

Awad NF, and Krishnan MS. 2006. The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to Be Profiled Online for Personalization. MIS Quarterly 30(1):13-28.

Chellappa R, and Sin R. 2005. Personalization versus Privacy: An Empirical Examination of the Online Consumer's Dilemma. Information Technology & Management 6:181-202.

Cranor LF, Reagle J, and Ackerman MS. 2000. Beyond concern: Understanding net users' attitudes about online privacy. In: Vogelsang I, and Compaine BM, editors. The Internet Upheaval: Raising Questions, Seeking Answers in Communications Policy The MIT Press. p 47-70.

Culnan MJ. 1993. "How Did They Get My Name?": An Exploratory Investigation of Consumer Attitudes Toward Secondary Information Use. MIS Quarterly 17(3):341-363.

Culnan MJ. 2000. Protecting Privacy Online: Is Self-Regulation Working? Journal of Public Policy & Marketing 19(1):20-26.

Culnan MJ, and Armstrong PK. 1999. Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. Organization Science 10(1):104-115.

Davis K, Frederick WC, and Blomstrom RL. 1980. Business and Society. New York, NY.: McGraw-Hill,.

Debatin B, Lovejoy JP, Horn A-K, and Hughes BN. 2009. Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences. Journal of Computer-Mediated Communication 15(1):83-108.

Dinev T, and Hart P. 2004. Internet privacy concerns and their antecedents - measurement validity and a regression model. Behaviour & Information Technology 23(6):413-422.

Dinev T, and Hart P. 2005. Internet Privacy Concerns and Social Awareness as Determinants of Intention to Transact. International Journal of Electronic Commerce 10(2):7-29.

Dinev T, and Hart P. 2006. An Extended Privacy Calculus Model for E-Commerce Transactions. Information Systems Research 17(1):61-80.

Egelman S, Tsai J, Cranor LF, and Acquisti A. 2009a. Timing is Everything? The Effects of Timing and Placement of Online Privacy Indicators. 27th international conference on human factors in computing systems. New York, NY, USA: ACM.

Egelman S, Tsai J, and Cranor LFA, Alessandro. 2009b. Timing is Everything? The Effects of Timing and Placement of Online Privacy Indicators. 27th international conference on human factors in computing systems. New York, NY, USA: ACM.

Ellison NB, Steinfield C, and Lampe C. 2007. The Benefits of Facebook "Friends:" Social Capital and College Students' Use of Online Social Network Sites. Journal of Computer-Mediated Communication 12(4):1143-1168.

Facebook. 2010. Facebook's Privacy Policy.

FTC. 2000. Privacy Online: Fair Information Practices in the Electronic Marketplace: Report to Congress.

GILC. 2010. An International Survey of Privacy Laws and Practice.

Graeff TR, and Harmon S. 2002. Collecting and using personal data: Consumers' awareness and concerns. The Journal of Consumer Marketing 19(4/5):302-319.

Hann I-H, Hui K-L, Lee S-YT, and Png IPL. 2007. Overcoming Online Information Privacy Concerns: An Information-Processing Theory Approach. Journal of Management Information Systems 24(2):13-42.

Hawkey K. 2007. Managing the Visual Privacy of Incidental Information in Web Browsers. Halifax, Nova Scotia: Dalhousie University.

Hine C, and Eve J. 1998. Privacy in the Marketplace. Information Society 14(4):253-262.

Hui K-L, Hock Hai T, and Sang-Yong Tom L. 2007. The Value of Privacy Assurance: An Exploratory Field Experiment. MIS Quarterly 31(1):19-33.

Interactive H, and Westin AF. 2002. The Harris Poll: #46 (2002). New York.

Jamal K, Maier M, and Sunder S. 2003. Privacy in E-Commerce: Development of Reporting Standards, Disclosure, and Assurance Services in an Unregulated Market. Journal of Accounting Research 41(2):285-309.

Jones H, and Soltren JH. 2005. Facebook: Threats to Privacy.

Justice E. 2007. Facebook Suicide: The End of a Virtual Life.

Korzaan M, Brooks N, and Greer T. 2009. Demystifying Personality and Privacy: An Empirical Investigation into Antecedents of Concerns for Information Privacy. Journal of Behavioral Studies in Business 1:1-17.

Krasnova H, Hildebrand T, Günther O, Kovrigin S, and Nowobilska A. 2008. Why Participate In An Online Social Network: An Empirical Analysis. European Conference on Information Systems. Galway.

Krasnova H, and Veltri NF. 2010. Privacy Calculus on Social Networking Sites: Explorative Evidence from Germany and USA. In: Natasha FV, editor. p 1-10.

Laufer RS, and Wolfe M. 1977. Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory. Journal of Social Issues 33(3):22-42.

Liang H, and Xue Y. 2009. Avoidance of Information Technology Threats: A Theoretical Perspective. MIS Quarterly 33(1):71-90.

Lwin M, Wirtz J, and Williams JD. 2007. Consumer online privacy concerns and responses: a power-responsibility equilibrium perspective. Journal of the Academy of Marketing Science 35(4):572-585.

Malhotra NK, Sung SK, and Agarwal J. 2004. Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. Information Systems Research 15(4):336-355.
McKeon M. 2010. The Evolution of Privacy on Facebook.
Meinert DB, Peterson DK, Criswell JR, and Crossland MD. 2006. Privacy Policy Statements and Consumer Willingness to Provide Personal Information. Journal of Electronic Commerce in Organizations 4(1):1-17.
Milne GR. 2000. Privacy and Ethical Issues in Database/Interactive Marketing and Public Policy: A Research Framework and Overview of the Special Issue. Journal of Public Policy & Marketing 19(1):1-6.
Milne GR, and Rohm AJ. 2000. Consumer Privacy and Name Removal Across Direct Marketing Channels: Exploring Opt-In and Opt-Out Alternatives. Journal of Public Policy & Marketing 19(2):238-249.
Miyazaki AD, and Fernandez A. 2001. Consumer Perceptions of Privacy and Security Risks for Online Shopping. Journal of Consumer Affairs 35(1):27.
Miyazaki AD, and Krishnamurthy S. 2002. Internet Seals of Approval: Effects on Online Privacy Policies and Consumer Perceptions. Journal of Consumer Affairs 36(1):28.
Moores T. 2005. Do Consumers Understand the Role of Privacy Seals in E-Commerce? Communications of the ACM 48(3):86-91.
Nissenbaum H. 2004. Privacy as contextual integrity. Washington Law Review 79:119-158.
Nowak GJ, and Phelps J. 1992. Understanding privacy concerns. An assessment of consumers' information-related knowledge and beliefs. Journal of Direct Marketing 6(4):28-39.
Nowak GJ, and Phelps J. 1997a. Direct marketing and the use of individual-level consumer information: Determining how and when. Journal of Direct Marketing 11(4):94-108.
Nowak GJ, and Phelps J. 1997b. Direct marketing and the use of individual-level consumer information: Determining how and when "Privacy" matters. Journal of Direct Marketing 11(4):94-108.
Okazaki S, Li H, and Hirose M. 2009. Consumer Privacy Concerns and Preference for Degree of Regulatory Control. Journal of Advertising 38(4):63-77.
Pavlou PA, Huigang L, and Yajiong X. 2007. Understanding and Mitigating Uncertainty in Online Exchange Relationships: A Principal--Agent Perspective. MIS Quarterly 31(1):105-136.
Phelps J, Nowak G, and Ferrell E. 2000. Privacy concerns and consumer willingness to provide personal information. Journal of Public Policy and Marketing 19(1):27-41.
Phelps JE, D'Souza G, and Nowak GJ. 2001. Antecedents and Consequences of Consumer Privacy Concerns: An Empirical Investigation. Journal of Interactive Marketing (John Wiley & Sons) 15(4):2-17.
Poll S. 2010. 60% of Facebook users consider quitting over privacy.
Rosenblum D. 2007. What Can Anyone Know: The Privacy Risk of Social Networking Sites. IEEE Security and Privacy 5(3):40-49.
Sheehan KB. 2002. Toward a Typology of Internet Users and Online Privacy Concerns. Information Society 18(1):21-32.
Sheehan KB, and Hoy MG. 1999. Flaming, Complaining, Abstaining: How Online Users Respond to Privacy Concerns. Journal of Advertising 28(3):37-51.
Sheehan KB, and Hoy MG. 2000. Dimensions of Privacy Concern Among Online Consumers. Journal of Public Policy & Marketing 19(1):62-73.

Smith HJ, Milberg SJ, and Burke SJ. 1996. Information Privacy: Measuring Individuals' Concerns About Organizational Practices. MIS Quarterly 20(2):167-196.
Solove DJ. 2001. Privacy and Power: Computer Databases and Metaphors for Information Privacy. Stanford Law Review 53(6):1393-1462.
Solove DJ. 2002. Conceptualizing Privacy. California Law Review 90:1087-1156.
Solove DJ. 2008. Understanding Privacy. Cambridge, Massachusetts: Harvard University Press.
Son J-Y, and Kim SS. 2008. Internet Users' Information Privacy-Protective Responses: A Taxonomy and a Nomological Model. MIS Quarterly 32(3):503-529.
Stewart KA, and Segars AH. 2002. An Empirical Examination of the Concern for Information Privacy Instrument. Information Systems Research 13(1):36-49.
Survey D. 2009. Social Networking And Reputational Risk In The Workplace.
Tezinde T, Smith B, and Murphy J. 2002. Getting Permission: Exploring Factors Affecting Permission Marketing. Journal of Interactive Marketing (John Wiley & Sons) 16(4):28-36.
Van Slyke C, Shim JT, Johnson R, and Jiang J. 2006. Concern for Information Privacy and Online Consumer Purchasing. Journal of the Association for Information Systems 7(6):415-443.
Vroom VH. 1964. Work and Motivation. New York: Wiley.
Wirtz J, Lwin MO, and Williams JD. 2007. Causes and consequences of consumer online privacy concern. International Journal of Service Industry Management 18(4):326-348.

芽|Sprouts

Working Papers on Information Systems | ISSN 1535-6078

Office:
Sprouts
University of Amsterdam
Roetersstraat 11, Room E 2.74
1018 WB Amsterdam, Netherlands
Email: admin@sprouts.aisnet.org

芽|Sprouts