Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2010 Proceedings

Americas Conference on Information Systems (AMCIS)

8-2010

Information Disclosure and Online Social Networks: From the Case of Facebook News Feed Controversy to a Theoretical Understanding

Heng Xu
The Pennsylvania State University, hxu@ist.psu.edu

Rachida Parks
The Pennsylvania State University, rfp127@ist.psu.edu

Chao-Hsien Chu
The Pennsylvania State University, chu@ist.psu.edu

Xiaolong (Luke) Zhang
The Pennsylvania State University, lzhang@ist.psu.edu

Information Disclosure and Online Social Networks: From the Case of Facebook News Feed Controversy to a Theoretical Understanding

Heng Xu
The Pennsylvania State University
hxu@ist.psu.edu

Rachida Parks
The Pennsylvania State University
rfp127@ist.psu.edu

Chao-Hsien Chu
The Pennsylvania State University
chu@ist.psu.edu

Xiaolong (Luke) Zhang
The Pennsylvania State University
lzhang@ist.psu.edu

ABSTRACT

Based on the insights learned from the case analysis of the Facebook News Feed outcry, we develop a theoretical understanding that identifies major drivers and impediments of information disclosure in Online Social Networks (OSNs). Research propositions are derived to highlight the roles of privacy behavioral responses, privacy concerns, perceived information control, trust in OSN providers, trust in social ties, and organizational privacy interventions. The synthesis of privacy literature, bounded rationality and trust theories provides a rich understanding of the adoption of OSNs that creates privacy and security vulnerabilities, and therefore, informs the privacy research in the context of OSNs. The findings are also potentially useful to privacy advocates, regulatory bodies, OSN providers, and marketers to help shape or justify their decisions concerning OSNs.

Keywords

Online Social Netwoks (OSNs), Privacy Concerns, Facebook, and Information Disclosure.

INTRODUCTION

The emergence of Web 2.0 has brought with it the concept of Online Social Networks (OSNs), a major technological phenomenon that has united hundreds of millions of participants around the world. Most OSNs permit members to define personal profiles and customize them as they wish to express themselves, socialize and interact with others. Through OSNs, users may interact with each other for a variety of purposes, including business, entertainment, and knowledge sharing. Such open availability of personal data potentially exposes users of OSNs to a number of security and privacy risks.

To address the critical and acute concerns for information privacy, we aim to develop a theoretical understanding that identifies major drivers and impediments of information disclosure in OSNs. Based on the insights learned from the case analysis of the Facebook News Feed outcry (Boyd 2008; Hoadley et al. 2010), we develop a theoretical model to explain users' privacy management strategies in OSNs. These propositions highlight the roles of perceived benefits in using OSNs, privacy concerns, perceived information control, trust in OSN providers, trust in social ties, and organizational privacy interventions in predicting information disclosure behavior.

Rather than drawing on a monolithic concept of privacy from a single theoretical lens, we try to build upon previous literature from multiple theoretical lenses to create a common understanding of the individual's information disclosure behavior. The study reported here is novel to the extent that existing privacy research has not examined this complex set of inter-related constructs in the context of OSNs. The synthesis of privacy literature, bounded rationality and trust theories may provide a rich understanding of the adoption of OSNs that creates privacy and security vulnerabilities, and therefore, inform adoption research in the Information Systems (IS) discipline. This research is also potentially useful to privacy advocates, regulatory bodies, OSN providers, and marketers to help shape or justify their decisions concerning OSNs.

In this paper, we first present the case of the Facebook News Feed privacy outcry, describing the background of this case, and discussing the emerging themes. Then we develop a research framework that models the individual privacy decision making through proposing the moderating role of perceived benefits and identifying major antecedents to privacy concerns. The paper concludes with a discussion of theoretical and practical implications, and directions for future research.

THE CASE OF FACEBOOK NEWSFEED OUTCRY

Facebook, a free online social networking website, provides its users with a wide range of services including but not limited to creating and updating their accounts, chatting, blogging, content sharing, and joining organized networks. In September 2006, Facebook released the News Feed feature, a homepage that delivers in headline-news format, a constantly updated list of their friends' Facebook activities. News Feed highlights information that includes profile changes, upcoming events, and conversations taking place between the walls of a user and their friends. Initially, Facebook promoted the News Feed feature as a convenience, with the promise that it would make new information easier to find. However, within a couple of days of News Feed implementation, users were very upset and protested this change. Their claim was that their personal information was being exposed and invaded (Boyd 2008).

Facebook's immediate response to this privacy outcry was an official apology from its CEO, and re-releasing News Feed feature with new privacy control features. In what follow we look into insights on 1) the cause of the privacy outcry and the users' behavioral responses to personal information disclosure on OSNs, and 2) the appropriate measures incorporated by organizations to handle these privacy outcries.

THEORETICAL FOUNDATION

To better understand information disclosure and privacy in OSNs, we identified three streams of literature that incorporate different privacy conceptualizations: privacy calculus, trust, and information control. Each of these theoretical lenses looks at information privacy differently and therefore provides a valid basis upon which the factors influencing judgments about the degree of privacy concerns could be reasonably proposed. These theoretical lenses are presented as guiding propositions for future research.

Information Control Lens

In case of Facebook privacy outcry (Boyd 2008; Hoadley et al. 2010), users felt they lost control over how their information was being used. Although there is no secrecy about their profile updates or their wall posts, users perceived less control over their disclosed information when Facebook News Feed feature broadcasted updated information about one's activities to the entire network of friends (Boyd 2008). The exploratory survey by Hoadley et. al (2010) suggested that the perceptions of easier access to information (78%) through Facebook News Feed decrease users' perceptions of control over their information, which leads to users' perceptions of privacy invasions.

The linkage between information privacy and the notion of control has been frequently highlighted in prior work (Altman 1977; Johnson 1974; Laufer et al. 1973; Westin 1967), which contributed to and stimulated research on privacy as a control related concept. Wolfe and Laufer (1974) suggested that "the need and ability to exert control over self, objects, spaces, information and behavior is a critical element in any concept of privacy" (p. 3). This view of privacy as a control related concept is also found in a number of consumer privacy studies (e.g., Dinev and Hart 2004; Goodwin 1991; Nowak and Phelps 1997; Phelps et al. 2000; Sheehan and Hoy 2000). For instance, consumers perceive information disclosure as less privacy-invasive when, among other things, they believe that they will be able to control future use of the information (Culnan and Armstrong 1999). This control perspective of information privacy indicates that control should be one of the key factors which provides the greatest degree of explanation for privacy concern (Sheehan and Hoy 2000). The implications of these findings lead us to consider the role of perceived information control in our theoretical development.

Privacy Calculus Lens

The release of Facebook News Feed caused users to feel that their information is being exposed to everyone in their network regardless of whom it was intended to (Boyd 2008). As a response to these perceived risks, Facebook embedded some privacy enhancing technologies to provide users with features such as opt out, allowing them to personalize their privacy settings. Through these interventions, Facebook managed to convince its users with the benefits of the new architecture of information flow (Boyd 2008), and to continue their information disclosure with the perceived benefits outweighing the perceived risks of information disclosure. The implications of these findings lead us to consider the role of privacy calculus in our theoretical development.

One very important perspective views of information privacy in terms of a calculus whereby personal information is given in return for certain benefits (e.g., Klopfer & Rubenstein, 1977; Stone & Stone, 1990). According to this perspective, Klopfer and Rubenstein (1977), for instance, found that the concept of privacy is not absolute but, rather, can be interpreted in "economic terms" (p.64). That is, individuals often consider the nature of the benefit being offered in exchange for information when deciding whether an activity violates their privacy (Culnan 1993; Xu and Gupta 2009; Xu et al. 2010). Such benefit could have a specific financial value (such as a cash payment, product, or service), and in some cases, the value could be information based (such as access to information that is of interest) (Sheehan and Hoy 2000). Overall, such calculus perspective of information privacy suggests the importance of rewarding consumers with benefits in return for the disclosure of their personal information.

Social Contract Lens

It has been shown in Hoadley et. al (2010) that 55.5% of users were less willing to reveal information about themselves after the implementation of the News Feed. Consistent with this finding, Boyd (2008) indicated in her conceptual analysis that the changes imposed by Facebook News Feed shacked users' trust beliefs toward Facebook and thus decreased their willingness to disclose their personal information. Research has shown that trust has a strong direct effect on influencing willingness to provide personal information (Dinev and Hart 2006; Metzger 2004; Xu et al. 2005); and that privacy concerns influenced information disclosure intentions with strong negative effects, indirectly through trust (Malhotra et al. 2004).

The conceptual academic literature in consumer privacy indicates that the Integrative Social Contract Theory (ISCT) is particularly appropriate for understanding the tensions between firms and consumers over information privacy (Caudill and Murphy 2000; Culnan 1995; Milne and Gordon 1993). According to this ISCT perspective, "a social contract is initiated, therefore, when there are expectations of social norms (i.e., generally understood obligations) that govern the behavior of those involved" (Caudill and Murphy 2000). Thus, the social contract, dictating how corporations handle consumers' personal information in an implicit form (not in an economic or a legal form), involves unspecified obligations and requires consumers' trust on the corporation's compliance to this social contract (Caudill and Murphy 2000; Culnan and Bies 2003; Hoffman et al. 1999). Hence, the lack of consumer trust in customer-centric enterprises seems to be a critical barrier that hinders the efforts of these enterprises to collect personal information from consumers for the purpose of providing services. In sum, such social contract lens leads us to consider the role of trust in our theoretical development.

SPURRING DEVELOPMENT OF PROPOSITIONS

The literature reviews in above section presenting the importance of information privacy from the calculus, trust, and control theoretical lenses provide the insightful theoretical foundations for formulating propositions for this research. Based on the three theoretical lenses described above, below we introduce the conceptual model and present research propositions concerning the relationships among the constructs. Figure 1 presents the research model. The following sections describe this emergent model in further detail.

Privacy Calculus: Rational Choice and Bounded Rationality

According to the calculus lens of privacy, individuals can be expected to behave as if they are performing a privacy calculus in assessing the outcomes they will receive as a result of providing personal information to corporations (Culnan 2000; Culnan and Armstrong 1999; Culnan and Bies 2003; Goodwin 1991; Milne and Rohm 2000; Milne et al. 1999). Hence, individuals will exchange their personal information as long as they perceive adequate benefits will be received in return—that is, benefits which exceed risks of the information disclosure (Culnan and Bies 2003). Consistent with the core ideas of the privacy calculus, the rational choice theory may further help predict how individuals make decisions regarding the revelation of personal information. This theory suggests that all action is fundamentally 'rational' in character and that consumers calculate the likely costs and benefits of any action before making a decision (Von Neumann and Morgenstern 1947). Individuals tend to pursue outcomes that maximize positive valences, which can be directly enhanced by benefits provided, and minimize negative valences (Culnan and Bies 2003; Stone and Stone 1990). Along the line of rational choice theory, higher level of privacy concerns that viewed as the negative valences, would be expected to negatively influence a personal's information disclosure behavior.

However, according to the bounded rationality theory (Simon 1982), human agents are unable to have *absolute rationality* because of the potential impacts of information processing capacity limitations and psychological distortions on individual decision making. For example, individuals have a tendency to discount 'hyperbolically' future costs or benefits (O'Donoghue and Rabin 2001; Rabin and O'Donoghue 2000). In economic literature, hyperbolic discounting implies inconsistency of personal preference over time – future events may be discounted at different discount rates than near-term events (Acquisti

2004). Hyperbolic discounting may affect privacy decisions, since the benefits of disclosing personal information may be immediate (e.g., ease of contacting friends), but the risk of such information disclosure may be invisible or spread over future periods of time (e.g., identity theft) (Acquisti 2004). Individuals may genuinely want to protect their personal data, but because of bounded rationality, rather than carefully calculating long term risks of information disclosure, they may opt for immediate gratification instead (Acquisti 2004).

Therefore, with the availability of immediate benefits in terms of convenience, self-presentation, and relationship maintenance, users of OSNs are very likely to opt for immediate gratification by discounting the potential risks of information disclosure. Therefore, we propose that perceived benefits will moderate the relationship between privacy concerns and information disclosure behavior:

Proposition 1: *With the perceived benefits (in terms of convenience, self-presentation, and relationship maintenance) available, the negative influences of privacy concerns on information disclosure behavior should be weaker.*

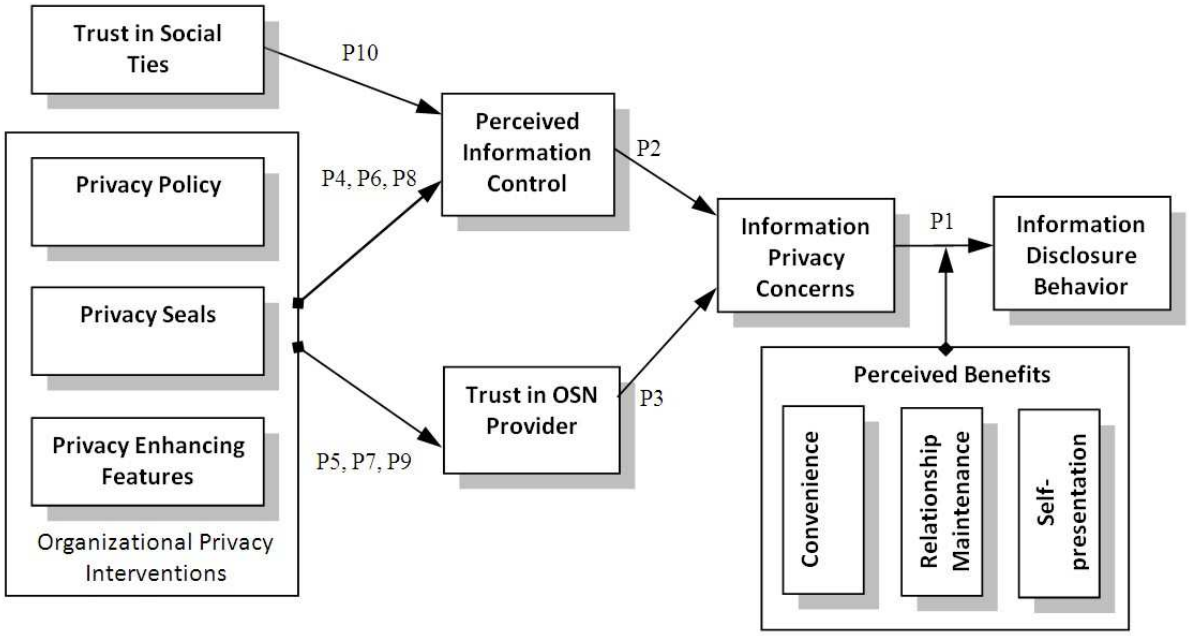

Figure 1. Research Framework

Determinants of Privacy Concerns

Perceived Information Control

As discussed above, the case of Facebook News Feed privacy outcry implies the important role of perceived information control in predicting privacy concerns. In fact, more frequently than not, the element of control is embedded in most privacy conceptual arguments and definitions and has been used to operationalize privacy in numerous measurement instruments (Altman 1975; Culnan 1993; Kelvin 1973; Margulis 1977; Smith et al. 1996; Westin 1967). In this research, "control" – defined as perceived control over information collection and use – is conceptualized as a related but separate variable from privacy concerns. Such conceptualization has been supported by Laufer and Wolfe (1977), who positioned control as a mediating variable in the privacy system. These considerations suggest that perceived control over disclosure and subsequent use of personal information is a separate construct from privacy concerns and that the two constructs are negatively related. Prior research has shown that, in general, individuals will have fewer privacy concerns when they have a greater sense that they control the disclosure and subsequent use of their information (Culnan 1993; Culnan and Armstrong 1999; Milne and Boza 1999; Stone and Stone 1990; Xu 2007). In other words, perceived information control is a contrary factor that is weighed against privacy concerns:

Proposition 2: *Perceived information control over OSNs negatively affects privacy concerns.*

Trust in OSN Provider

As discussed earlier, the social contract, dictating how corporations handle consumers' personal information in an implicit form (not in an economic or a legal form), involves unspecified obligations and requires consumers' trust on the corporation's compliance to this social contract (Caudill and Murphy 2000; Culnan and Bies 2003; Hoffman et al. 1999). The concept of social contract in the consumer privacy context means that consumers are willing to disclose personal information for certain benefits as long as they trust the corporation that it would uphold its side of social contract. Hence, the lack of consumer trust in customer-centric enterprises seems to be a critical barrier that hinders the efforts of these enterprises to collect personal information from consumers for the purpose of providing services. It is very likely that the customer-centric enterprises that are considered trustworthy by consumers may incur consumers' lower privacy concerns. In the context of OSNs, because of the absence of proven guarantees that the OSN providers will not engage in opportunistic behaviors in terms of information misuse, trust in an OSN provider is crucial in helping users overcome their perceptions of uncertainty. If the OSN provider is perceived to be caring about users' information privacy needs (trusting belief—benevolence), honest and consistent in its dealing with users' personal information (trusting belief—integrity), and capable of protecting their personal information (trusting belief—competence), the level of concerns over information privacy may be reduced. Therefore, we propose that:

> **Proposition 3:** *Trust in OSN provider negatively affects privacy concerns.*

Impacts of Organizational Privacy Interventions

Users' perceptions of the environment are formed by a set of institutional assurance variables, much as in the formation of the institution-based trust in the trust literature (e.g. McKnight et al. 2002). As in the case of the institution-based trust, organizational privacy interventions refers to an individual's perceptions of the institutional environment, in our case the OSN provider, and we will argue in the following paragraphs that it affects the individual's perceived information control and trust in PSN providers.

The integrative trust formation model developed by McKnight and Chervany (2002) in the e-commerce context includes the Web vendor interventions which are posited to have impacts on consumer trusting beliefs in the e-vendor. Web vendor interventions are defined as the actions a vendor may take to provide assurances to consumers about the vendor's site (McKnight and Chervany 2002). In the context of online markets, these interventions could include feedback mechanisms, escrow services, and credit card guarantees (Pavlou and Gefen 2004). The interventions assure consumers that this particular vendor site is safe in spite of whatever deficiencies exist in the overall Web environment. Following McKnight et al. (2002), this study defines OSN provider's privacy interventions as the interventions that a particular OSN provider takes to provide assurances to users about its efforts devoted to protect users' personal information. In particular, this study examines three types of interventions: (a) privacy policy, (b) third party privacy seals, and (c) privacy control features. Although not an exhaustive list of all privacy-related interventions in the context of OSNs, the proposed three factors represent the most popular market-driven and technology-driven privacy interventions. The following sub-sections describe these three privacy-related interventions in further detail.

Privacy Policy

The organizational privacy interventions for privacy assurance are predicated on the assumption that OSN providers have an incentive to address privacy concerns of users because, if they fail to do so, they will suffer reputational losses. Privacy literature suggests that a firm's collection of personal information is perceived to be fair when the consumer is vested with notice and voice (Culnan and Bies 2003; Malhotra et al. 2004). In other words, consumers want to influence changes in firms' polices that they find to be objectionable (Malhotra et al. 2004). Privacy policy is essentially a self-regulated organizational mechanism where consumers can be informed about the choices available to them regarding how the collected information is used, the safeguards in place to protect the information from loss, misuse, or alteration, and how consumers can update or correct any inaccurate information. It has been suggested that the prescription of notification of and consent by consumers effectively exemplifies procedural fairness and thus increases consumers' perceived control over their personal information (Culnan and Bies 2003; Milne and Culnan 2004). In addition, a particular OSN provider's posting its privacy policy should may enable users to believe that the OSN provider cares about their information privacy needs (trusting belief—benevolence), and it is honest and consistent in its dealing with users' personal information (trusting belief—integrity). Therefore, we propose:

> **Proposition 4:** The OSN provider's interventions with regard to having privacy policy will increase users' perceived information control.

Proposition 5: The OSN provider's interventions with regard to having privacy policy will increase users' trust beliefs in OSN provider.

Privacy Seals

When applied to consumer privacy, ISCT suggests that a firm's collection of personal information is perceived to be fair when the consumer is vested with voice (Culnan and Bies 2003; Malhotra et al. 2004). Frequently, the organizational privacy assurance through privacy policy may need to be reinforced by having a trusted third party certify that the web sites indeed conform to the fair information practices they purport to (Culnan and Bies 2003). Such third-party certification typically comes in the form of seals of approval such as those given by Online Privacy Alliance or TRUSTe. These seal programs should enhance the consumer's perceived control and increase their trust in OSN providers because these institutional mechanisms could limit the firm's ability to behave in negative ways, allowing consumers to form and hold beliefs about expectations of positive outcomes (Johnson and Cullen 2002). As Gefen et al. (2003) explain for the case of trust, having a third party like the reputable TRUSTe to vouch for a firm's trustworthiness should build trust in that such third party assurances have typically been one of the primary methods of building trust in business. Empirical studies have shown that companies that conform to the privacy seal programs could foster consumers' perceptions of control over their personal information and enhance their trust perceptions in OSN providers (Culnan and Armstrong 1999). Therefore, we propose:

Proposition 6: The OSN provider's interventions with regard to joining third party privacy seal programs will increase users' perceived information control.

Proposition 7: The OSN provider's interventions with regard to joining third party privacy seal programs will increase users' trust beliefs in OSN provider.

Privacy Enhancing Features

To strengthen the bond of social contract between firms and consumers over information privacy, firms need to address the data collection issue in that marketers' collection of personal information would continue to be an important source of privacy concerns (Malhotra et al. 2004; Phelps et al. 2000). In the context of OSNs, OSN providers have been rolling out features that allow users to control who can access their personal information. Some social networking sites (e.g., Friendster.com) even embedded the privacy control features into the very use of various social networking functions and thus integrated privacy control as part of social networking functionality. With various features that support the functions of specifying privacy preferences for using different OSN applications, users are able to limit the amount of personal information disclosed on the OSNs. For example, Facebook users can specify their privacy preferences on who can see their profiles and personal information, who can search for them, how they can be contacted, what stories about them get published to their profiles, etc. These privacy enhancing features could provide users with the capabilities to limit information disclosure, and thus may reduce their privacy concerns. Empirical evidence supported that perceptions of privacy invasion are lower when the individuals are provided with the technical features to control their personal information disclosure (Eddy et al. 1999; Zweig and Webster 2002; Zweig and Webster 2003). Therefore, we propose:

Proposition 8: The OSN provider's interventions with regard to introducing privacy enhancing features will increase users' perceived information control.

Introducing privacy-enhancing features, therefore, should directly build users' trust beliefs toward an OSN provider because of the nontrivial investment of time and resources made by the OSN provider to design and implement these features. This action should be interpreted as a signal that the OSN provider is actively addressing users' privacy concerns and it will comply with the social contract by undertaking the responsibility to manage users' personal information properly. In other words, a particular OSN provider's introduction of the privacy enhancing features to users may enable them to believe that the OSN provider cares about their information privacy needs (trusting belief—benevolence), and it is capable of protecting their personal information (trusting belief—competence). Therefore, we propose:

Proposition 9: The OSN provider's interventions with regard to introducing privacy enhancing features will increase users' trust beliefs in OSN provider.

Impacts of Trust in Social Ties

Besides trust in the OSN provider (Facebook.com), Hoadley et. al (2010) also highlights the importance of trust in the social ties (e.g., friends, friends of friends on Facebook, and the university's Facebook users) in the case of Facebook News Feed privacy outcry. When a user disclose her personal information in OSNs, the personal information moves to a collective domain where the user and her friends in OSNs become co-owners with joint responsibilities for keeping the information safe

and private (Petronio 2002). Individuals/friends on the user's contact list usually have certain amount of information access to the user's profile and personal information thus may abuse it if the relationship changes. In addition, it has been recently reported that personal details of Facebook users could potentially be stolen due to their friends' adding applications (Kelly 2008). That is to say, even if some users think they have tight security settings, their personal information could be stolen due to their friends' ignorance of privacy and security (Kelly 2008). The need for trust in social ties arises due to the inability to monitor other members on the network and being uncertain about their behaviors. Trust in social ties, therefore could be an effective mechanism to reduce the complexity of human conduct in situations where people have to cope with uncertainty (Luhmann 1988). Such belief may enable users to believe that their personal information will be co-managed appropriately by their friends in OSNs. Therefore, we propose:

Proposition 10: Trust in the social ties positively affects perceived information control.

IMPLICATIONS AND CONCLUSION

In this paper, we used Facebook's privacy outcry case to identify major drivers and impediments of information disclosure in OSNs. The emergent model consists of factors such as perceived information control, social connectedness relates to trust, and concerns for information privacy, together with the notion of privacy attitude/behavior dichotomy. Drawing on the bounded rationality theory, we proposed the moderating effect of perceived benefits of using OSNs in influencing the relationship between privacy concerns and information disclosure behavior. We reasoned that, because of bounded rationality, rather than actually taking steps to protect their personal data, they may opt for immediate gratification brought by benefits of using OSNs, instead of carefully calculating long term risks of information disclosure such as identity theft. Furthermore, we discussed how the organizational privacy interventions and trust in social ties may alleviate privacy concerns through the mediating roles of trust in OSN providers and perceived information control.

We believe that the integrated theoretical framework enriches the information privacy literature by integrating rational choice, bounded rationality, trust and information control theoretical perspectives which will unpack the nature of information privacy in the context of OSNs. From a practical perspective, this research highlights that trust beliefs and perceived information control are the important factors in users' interactions with OSNs. In this aspect, this research provides some insights into the different approaches that could be used by an OSN provider to address privacy concerns by building trust and enhancing control perceptions. First, incorporating organization privacy interventions such as joining privacy seal programs or maintaining a good privacy policy into the management of information practices should be an important method for increasing users' trust beliefs and reducing their privacy concerns. Second, it is important for OSN providers to develop privacy enhancing features with user-friendly interfaces for specifying privacy preferences to counter privacy risk perceptions and enhance trust and control beliefs. To the extent that perceived control is a key factor influencing privacy concern, application developers should pay close attention to those measures that can increase the perceptions of information control. We would not have seen so much of a public outcry related to privacy had Facebook released News Feed together with control features such as opt-out and access control. Third, given the potential vulnerabilities caused by friends' ignorance of privacy and security, mechanisms for promoting collective information control between users and their friends should help build trust in social ties in OSNs.

Trust and user control could play primary roles in addressing privacy concerns pertaining to OSNs, especially in the absence of well-established legal resources. Having highlighted the roles of some market-driven and technology-driven mechanisms in trust building and privacy risk reduction, this study provides a preliminary understanding of the privacy issues in OSNs by integrating rational choice, bounded rationality and social contract theories into a theoretical framework. Using the groundwork laid down in this study, further empirical work validating this research framework could contribute significantly to extending our theoretical understanding and practical ability to foster the diffusion of OSNs.

ACKNOWLEDGMENTS

This research is partially supported by the National Science Foundation under Grant No NSF-CNS 0716646. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author and do not necessarily reflect the views of the National Science Foundation (NSF).

REFERENCES

Acquisti, A. "Privacy in Electronic Commerce and the Economics of Immediate Gratification," Proceedings of the 5th ACM Electronic Commerce Conference, ACM Press, New York, NY, 2004, pp. 21-29.

Altman, I. *The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding*, Brooks/Cole Publishing, Monterey, CA, 1975.

Altman, I. "Privacy Regulation: Culturally Universal or Culturally Specific?," *Journal of Social Issues* (33:3) 1977, pp 66-84.

Boyd, D. "Facebook Privacy Trainwreck: Exposure, Invasion and Social Convergence.," *Convergence: the international Journal of Research into New Media Technologies* (14:1) 2008, pp 13-20.

Caudill, M.E., and Murphy, E.P. "Consumer Online Privacy: Legal and Ethical Issues," *Journal of Public Policy & Marketing* (19:1) 2000, pp 7-19.

Culnan, M.J. "'How Did They Get My Name'? An Exploratory Investigation of Consumer Attitudes toward Secondary Information Use," *MIS Quarterly* (17:3) 1993, pp 341-364.

Culnan, M.J. "Consumer Awareness of Name Removal Procedures: Implication for Direct Marketing," *Journal of Interactive Marketing* (9), Spring 1995, pp 10-19.

Culnan, M.J. "Protecting Privacy Online: Is Self-Regulation Working?," *Journal of Public Policy & Marketing* (19:1) 2000, pp 20-26.

Culnan, M.J., and Armstrong, P.K. "Information Privacy Concerns, Procedural Fairness and Impersonal Trust: An Empirical Investigation," *Organization Science* (10:1), Jan-Feb 1999, pp 104-115.

Culnan, M.J., and Bies, J.R. "Consumer Privacy: Balancing Economic and Justice Considerations," *Journal of Social Issues* (59:2) 2003, pp 323-342.

Dinev, T., and Hart, P. "Internet Privacy Concerns and Their Antecedents - Measurement Validity and a Regression Model," *Behavior and Information Technology* (23:6) 2004, pp 413-423.

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

Eddy, R.E., Stone, L.D., and Stone-Romero, F.E. "The Effects of Information Management Polices on Reactions to Human Resource Information Systems: An Integration of Privacy and Procedural Justice Perspectives," *Personnel Psychology* (52) 1999, pp 335-358.

Gefen, D., Karahanna, E., and Straub, D.W. "Trust and TAM in online shopping: an integrated model," *MIS Quarterly* (27:1), March 2003, pp 51-90.

Goodwin, C. "Privacy: Recognition of a Consumer Right," *Journal of Public Policy and Marketing* (10:1) 1991, pp 149-166.

Hoadley, M.C., Xu, H., Lee, J., and Rosson, M.B. "Privacy as Information Access and Illusory Control: The Case of the Facebook News Feed Privacy Outcry,," *Electronic Commerce Research and Applications.* (Vol. 9:No. 1) 2010, pp 50-60.

Hoffman, D.L., Novak, T., and Peralta, M.A. "Information Privacy in the Marketspace: Implications for the Commercial Uses of Anonymity on the Web," *Information Society* (15:2) 1999, pp 129-139.

Johnson, C.A. "Privacy as Personal Control," in: *Man-Environment Interactions: Evaluations and Applications: Part 2,* D.H. Carson (ed.), Environmental Design Research Association, Washington, D.C., 1974, pp. 83-100.

Johnson, L.J., and Cullen, B.J. "Trust in Cross-Cultural relationships," in: *The Blackwell Handbook of Cross-Cultural Management,* M.J. Gannon and K.L. Newman (eds.), Blackwell, Oxford, UK, Malden, Mass, 2002, pp. 335-360.

Kelly, S. "Identity 'at risk' on Facebook," in: *BBC News*, 2008.

Kelvin, P. "A social psychological examination of privacy.," *British Journal of Social and Clinical Psychology* (12) 1973, pp 248-261.

Klopfer, P.H., and Rubenstein, D.L. "The concept privacy and its biological basis," *Journal of social Issues* (33) 1977, pp 52-65.

Laufer, R.S., Proshansky, H.M., and Wolfe, M. "Some Analytic Dimensions of Privacy," Paper presented at the meeting of the Third International Architectural Psychology Conference, Lund, Sweden, 1973.

Laufer, R.S., and Wolfe, M. "Privacy as a Concept and a Social Issue - Multidimensional Developmental Theory," *Journal of Social Issues* (33:3) 1977, pp 22-42.

Luhmann, N. "Familiarity, Confidence, Trust: Problems and Alternatives," in: *Trust,* D. Gambetta, G. (ed.), Basil Blackwell, New York, 1988, pp. 94-107.

Malhotra, N.K., Kim, S.S., and Agarwal, J. "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model," *Information Systems Research* (15:4), December 2004, pp 336-355.

Margulis, S.T. "Conceptions of Privacy - Current Status and Next Steps," *Journal of Social Issues* (33:3) 1977, pp 5-21.

McKnight, D.H., and Chervany, N.L. "What trust means in e-commerce customer relationships: an interdisciplinary conceptual typology," *International Journal of Electronic Commerce* (6:2) 2002, pp 35-59.

McKnight, D.H., Choudhury, V., and Kacmar, C. "Developing and Validating Trust Measures for E-Commerce: An Integrative Typology," *Information Systems Research* (13:3) 2002, pp 334-359.

Metzger, M.J. "Privacy, Trust, and Disclosure: Exploring Barriers to Electronic Commerce," *Journal of Computer-Mediated Communication* (9:4) 2004.

Milne, G.R., and Boza, M.-E. "Trust and Concern in Consumers' Perceptions of Marketing Information Management Practices," *Journal of Interactive Marketing* (13:1) 1999, pp 5-24.

Milne, G.R., and Culnan, M.J. "Strategies for reducing online privacy risks: Why consumers read(or don't read) online privacy notices," *Journal of Interactive Marketing* (18:3) 2004, pp 15-29.

Milne, G.R., and Gordon, E.M. "Direct Mail Privacy-Efficiency Trade-Offs Within an Implied Social Contract Framework," *Journal of Public Policy and Marketing* (12:2), Fall 1993, pp 206-215.

Milne, G.R., and Rohm, A. "Consumer Privacy and Name Removal Across Direct Marketing Channels: Exploring Opt-in and Opt-out Alternatives," *Journal of Public Policy and Marketing* (19:2), Fall 2000, pp 238-249.

Milne, G.R., Rohm, A., and Boza, M.-E. "Trust Has to Be Earned," in: *Frontiers of Direct Marketing,* J. Phelps (ed.), Direct Marketing Educational Foundation, New York, 1999, pp. 31-41.

Nowak, J.G., and Phelps, J. "Direct Marketing and the Use of Individual-Level Consumer Information: Determining How and When "Privacy" Matters,," *Journal of Direct Marketing* (11:4), Fall 1997, pp 94-108.

O'Donoghue, T., and Rabin, M. "Choice and procrastination," *Quartely Journal of Economics* (116) 2001, pp 121-160.

Pavlou, P.A., and Gefen, D. "Building Effective Online Marketplaces with Institution-Based Trust," *Information Systems Research* (15:1) 2004, pp 37-59.

Petronio, S.S. *Boundaries of privacy : dialectics of disclosure*, State University of New York Press, Albany, 2002, pp. xix, 268 p.

Phelps, J., Nowak, G., and Ferrell, E. "Privacy Concerns and Consumer Willingness to Provide Personal Information," *Journal of Public Policy and Marketing* (19:1) 2000, pp 27-41.

Rabin, M., and O'Donoghue, T. "The economics of immediate gratification," *Journal of Behavioral Decision Making* (13) 2000, pp 233-250.

Sheehan, K.B., and Hoy, G.M. "Dimensions of Privacy Concern among Online Consumers," *Journal of Public Policy and Marketing* (19:1) 2000, pp 62-73.

Simon, H.A. *Models of bounded rationality*, The MIT Press, Cambridge, MA, 1982.

Smith, H.J., Milberg, J.S., and Burke, J.S. "Information Privacy: Measuring Individuals' Concerns About Organizational Practices," *MIS Quarterly* (20:2), June 1996, pp 167-196.

Stone, E.F., and Stone, D.L. "Privacy in Organizations: Theoretical Issues, Research Findings, and Protection Mechanisms," *Research in Personnel and Human Resources Management* (8:3) 1990, pp 349-411.

Von Neumann, J., and Morgenstern, O. *Theory of Games and Economic Behavior*, (2nd ed.) Princeton University Press, Princeton, 1947.

Westin, A.F. *Privacy and Freedom*, Atheneum, New York, 1967.

Wolfe, M., and Laufer, R.S. "The Concept of Privacy in Childhood and Adolescence," in: *Privacy as a Behavioral Phenomenon, Symposium Presented at the Meeting of the Environmental Design Research Association,* S.T. Margulis (ed.), Milwaukee, 1974.

Xu, H. "The Effects of Self-Construal and Perceived Control on Privacy Concerns," Proceedings of the 28th Annual International Conference on Information Systems (ICIS 2007), Montréal, Canada, 2007.

Xu, H., and Gupta, S. "The Effects of Privacy Concerns and Personal Innovativeness on Potential and Experienced Customers' Adoption of Location-Based Services " *Electronic Markets – The International Journal on Networked Business* (19:2) 2009, pp 137-140.

Xu, H., Teo, H.H., and Tan, B.C.Y. "Predicting the Adoption of Location-Based Services: The Roles of Trust and Privacy Risk," Proceedings of 26th Annual International Conference on Information Systems (ICIS 2005), Las Vegas, NV, 2005, pp. 897-910.

Xu, H., Teo, H.H., Tan, B.C.Y., and Agarwal, R. "The Role of Push-Pull Technology in Privacy Calculus: The Case of Location-Based Services," *Journal of Management Information Systems* (26:3) 2010, pp 137-176.

Zweig, D., and Webster, J. "Where is the Line between Benign and Invasive? An Examination of Psychological Barriers to the Acceptance of Awareness Monitoring Systems," *Journal of Organizational Behavior* (23) 2002, pp 605-633.

Zweig, D., and Webster, J. "Personality as a Moderator of Monitoring Acceptance," *Computers in Human Behavior* (19) 2003, pp 479-493.