PRIVACY IN ONLINE SOCIAL NETWORKING: APPLYING A PRIVACY CALCULUS MODEL

Janice C. Sipior, Villanova School of Business, Villanova University, PA, USA, janice.sipior@villanova.edu
Burke T. Ward, Villanova School of Business, Villanova University, PA, USA, burke.ward@villanova.edu
Regina Connolly, DCU Business School, Dublin City University, Dublin 9, Ireland, regina.connolly@dcu.ie
Labhras MacGabhann, Villanova School of Business, Villanova University, PA, USA, lrozan01@villanova.edu

Abstract

The penetration rate continues to grow for social networking sites where individuals join a virtual community to socialize, make connections, and share opinions with those who have similar interests, while revealing personal information. However, online social networking presents a unique context with distinct privacy challenges. To understand information disclosure behavior in this context, we apply the extended privacy calculus model, developed by Dinev and Hart (2006a), which addresses the trade-off between the expected costs of privacy risk beliefs and the benefits of confidence and placement beliefs on the willingness to provide personal information. We further extend this model to include specific types of personal information, based on our proposed taxonomy of information integral to social networking. To test our research model, a questionnaire will be administered to undergraduate students, drawn from the mid-Atlantic U.S. For hypothesis testing, structural equations modeling will be used. The completion of this research-in-progress study is expected to contribute to our understanding of the types of information revealed in online social networking.

Keywords: social networking, privacy calculus, trust, risk, taxonomy of personal information.
1 INTRODUCTION

The penetration rate continues to grow for social networking sites where individuals join a virtual community to socialize, make connections, and share opinions with those who have similar interests, while revealing personal information. The global audience for Facebook, for example, has grown to 964,368,120 as of 02 February 2013.\(^1\) However, this vast growth of online social networking (OSN) has brought increasing privacy concerns (Rizk et al. 2009). While OSN creates value for society in supporting connections among people, criticism abounds about privacy risks in disclosing personal information which is used for commercial purposes (Krasnova et al. 2009a). Since OSN is fee-free to users, user information is used for marketing purposes, an important source of revenues (Krasnova et al. 2009a; Krasnova et al. 2012).

The privacy controversy over collecting information on the Internet arises from the far-reaching unprecedented capability to collect more detailed information and disseminate greater quantities of information (Sipior et al. 2009). OSN presents a unique context with distinct privacy challenges (Bulgurcu et al. 2010; Krasnova et al. 2010; Xu et al. 2008). For users of OSN, information sharing has become even easier as users can simultaneously update personal information across multiple social networks, such as Facebook, Twitter, and LinkedIn. Rosenblum (2007) observed that OSN users seem to be comfortable sharing personal information, seemingly oblivious to the privacy risks. However, privacy concerns of Facebook users, for example, have been found to be prevalent (O’Brien & Torres 2012). The contradiction between disclosing personal information while holding concerns about privacy is called the privacy paradox (Jensen et al. 2005). When confronted with the privacy paradox, the decision to disclose personal information may entail a cost-benefit calculation, termed the privacy calculus (Culnan & Armstrong 1999). Information may be exchanged for some economic or social benefit, weighed against the risks of disclosure. The decision to disclose personal information results from the rational choice when the economic or social benefit outweighs the risks of disclosure.

We extend the privacy calculus to OSN, by building on the research of Dinev and Hart (2006a) who examined the balance between privacy risk beliefs and confidence and enticement beliefs which influence the intention to provide personal information required to conduct transactions on the Internet. Dinev and Hart (2006a) developed a theoretical model comprised of contrary factors representing elements of a privacy calculus for e-commerce transactions. We apply their extended privacy calculus model to assess the impact of privacy risk beliefs, and confidence and placement beliefs, on the willingness to provide personal information within the context of OSN. We further extend this model to include specific types of personal information, based on our proposed taxonomy of information integral to social networking.

---

\(^1\) www.checkfacebook.com 2013
This research-in-progress paper first summarizes previous privacy calculus research in the context of OSN. We then propose a taxonomy of information integral to social networking. Based on the review of previous research, we present our research model, followed by our hypotheses, and our research methodology. Finally, we discuss expected implications of our study for research and for practice.

2 BACKGROUND

2.1 Previous Privacy Calculus Research in the Context of Online Social Networking

Xu (2009) argues that privacy beliefs are influenced by situational and environmental cues which are indicative of the level of privacy protections in a specific context environment. Further, Xu et al. (2008) confirm that privacy related relationships vary across types of websites, including e-commerce, OSN, financial, and healthcare sites, indicative of information sensitivity in various contexts. The unique context of OSN in this regard has prompted an emergent stream of research within the information systems (IS) literature addressing the disclosure of personal information. To understand the privacy paradox, we take a privacy calculus research perspective. We reviewed the privacy calculus research within the context of OSN and present a summary of this research in Table 1.

<table>
<thead>
<tr>
<th>Research Study</th>
<th>Objective</th>
<th>Conclusion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hugl 2011</td>
<td>Analysis of scholarly work on information privacy in the OSN context.</td>
<td>Adults are more concerned about privacy; the majority underestimate privacy risks; privacy approaches fall short. Call for research on privacy calculus and fair information practices.</td>
</tr>
<tr>
<td>Dinev et al. 2009</td>
<td>Investigate users’ privacy perceptions by integrating privacy values, beliefs, and attitudes into a theoretical framework.</td>
<td>Perceived control and vulnerability influence perception of privacy. Anonymity and secrecy control information. Information sensitivity and expectation of privacy impact perceived vulnerability.</td>
</tr>
<tr>
<td>Krasnova et al. 2009b</td>
<td>Examine the factors behind individual self-disclosure decisions.</td>
<td>Perceived enjoyment and privacy concerns impact information revelation. Users’ concerns are determined by perceived likelihood of a privacy violation, less than expected damage.</td>
</tr>
<tr>
<td>Krasnova et al. 2010</td>
<td>Develop a self-disclosure model.</td>
<td>Convenience of relationships and enjoyment motivates information disclosure. Privacy risks are a barrier to disclosure. Users’ perception of risk can be mitigated by trust in the provider and availability of controls.</td>
</tr>
<tr>
<td>Krasnova and Veltri 2010</td>
<td>Explore the differences in perceptions of disclosure-relevant determinants between German and US users.</td>
<td>German users expect more damage and attribute higher probability to privacy violations. US users show higher level of privacy concern, with more benefits, more trust in the provider and legal assurances, and perceive more control.</td>
</tr>
<tr>
<td>Krasnova et al. 2012</td>
<td>Explore the role of the two cultural dimensions of individualism and uncertainty avoidance in self-disclosure decisions.</td>
<td>Trusting beliefs are key in self-disclosure decisions of users from individualistic cultures, while uncertainty avoidance determines the impact of privacy concerns.</td>
</tr>
</tbody>
</table>
Table 1. Previous privacy calculus research in the context of online social networking.

<table>
<thead>
<tr>
<th>Study</th>
<th>Research Focus</th>
</tr>
</thead>
<tbody>
<tr>
<td>Li et al. 2011</td>
<td>Examine online information disclosure decision as a result of affective and cognitive reactions of consumers over several stages.</td>
</tr>
<tr>
<td>Li 2012</td>
<td>Develop a dual-calculus framework of trade-offs that influence information disclosure behavior: privacy calculus and risk calculus.</td>
</tr>
<tr>
<td>Wilson and Valacich 2012 (research-in-progress)</td>
<td>Develop a theoretical model of actual disclosure behavior and potential for irrational behavior induced by situational factors.</td>
</tr>
</tbody>
</table>

Table 2. Proposed Taxonomy of User Information Integral to Social Networking.

<table>
<thead>
<tr>
<th>Information Type</th>
<th>Data Source</th>
<th>User-in-Question’s Degree of Control</th>
<th>Parties that Can Access</th>
<th>Implicit or Explicit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service</td>
<td>User-in-Question</td>
<td>Low</td>
<td>User-in-Question, Service Provider</td>
<td>Explicit</td>
</tr>
<tr>
<td>Disclosed</td>
<td>User-in-Question</td>
<td>High</td>
<td>User-in-Question, Other Authorized Users Indicated by User-in-Question, Service Provider</td>
<td>Explicit</td>
</tr>
<tr>
<td>Entrusted</td>
<td>User-in-Question</td>
<td>Medium</td>
<td>User-in-Question, Entrusted User, Other Authorized Users Indicated by Entrusted User, Service Provider</td>
<td>Explicit</td>
</tr>
<tr>
<td>Incidental</td>
<td>All Other Users</td>
<td>Low</td>
<td>Incidental User, User-in-Question, Other Authorized Users Indicated by Incidental User, Service Provider</td>
<td>Implicit</td>
</tr>
<tr>
<td>Behavioral</td>
<td>User-in-Question</td>
<td>Low</td>
<td>Service Provider, Third Parties Authorized by Service Provider to Access Data</td>
<td>Implicit</td>
</tr>
<tr>
<td>Derived</td>
<td>User-in-Question, Other Users, Various Online Databases (in the case of cross-referenced or concatenated data)</td>
<td>Low</td>
<td>Party Responsible for Deriving Data, Other Authorized Users Designated by Party Responsible for Deriving Data</td>
<td>Implicit</td>
</tr>
</tbody>
</table>
Service information refers to the data that users must share in order to access a social network. It includes basic information such as a person’s name, date of birth, e-mail address, and – if the service is subscription based – a person’s debit or credit card number. Disclosed information refers to whatever data individuals make available to others through their online profiles, blogs, twitter feeds, and so forth. Entrusted information refers to what individual users post on other users’ profiles. It is similar to disclosed information in that it is generated by the user in question, but different in that once this data is turned over to an “entrusted” user it is no longer under the user-in-question’s direct control. Incidental information refers to data other users disclose about a user-in-question, either on their own or on the user-in-question’s profile. It differs from disclosed and entrusted information in that the user-in-question neither authored the data, nor has any control over it. Behavioral information refers to data a social networking site collects about users’ habits by recording what they do online. It includes things like the amount of time a user spends on a particular site, the sorts of online games a user plays, the frequency with which data regarding user is disclosed, the kinds of music a user listens to online, the sorts of articles a user reads via links embedded in a social networking site, and so forth. Finally, derived information refers to data that is derived from one or more of the above kinds of data. The “derivation” involved in this case can run the gamut from simple cognitive deduction – if, for example, 90% a user’s friends identify as Republicans, odds that user themselves is a Republican – to conclusions reached with the assistance of computers, algorithms or other kinds of assisted analytics.

Derived information is unlike the other five types of information in this taxonomy. It can include data derived from the activities of many users. For example, social analytic firm ListenLogic analyzes vast swaths of disclosed, entrusted, incidental, and behavioral data.

3 RESEARCH MODEL AND HYPOTHESES

In seeking to understand the willingness to provide personal information to social networking websites, the proposed research model presented in Figure 1 was developed based upon previous research on privacy concerns in the IS literature. Hugl (2011) has called for consideration of privacy calculus in research addressing information privacy in the OSN context. Specifically, we extend Dinev and Hart’s (2006a) extended privacy calculus model to the context of OSN. In investigating the privacy calculus, we seek to understand the disclosure of personal information weighed against the risks of disclosure. Important to the privacy calculus is the type of information under consideration for disclosure. We therefore further extend Dinev and Hart’s (2006a) extended privacy calculus model to include a taxonomy of information integral to social networking, based upon Schneier (2009). The constructs of our research are defined in Table 3.

![Figure 1. Proposed research model.](image-url)
Table 3. Constructs in the Extended Privacy Calculus Model for OSN (Based on and expanded from Dinev and Hart 2006a).

Our proposed research model identifies five constructs and the relationships between them. Based on the privacy calculus, it is hypothesized that behavioral intention will be influenced by the perceived costs and benefits. Behavioral intention, the dependent variable, is the willingness to provide personal information to social websites. Costs, an independent variable, are risk beliefs and privacy concerns. Benefits, an independent variable, are the confidence and enticement beliefs, which are trust and personal OSN interest, respectively. Each of these variables, and their hypothesized relationships, are discussed below. For hypothesis testing, structural equations modeling will be used.

3.1 Costs: Privacy Risk Beliefs and Privacy Concerns

Dinev and Hart (2006a) note that higher levels of privacy risk beliefs suggest user resistance to personal information disclosure. This observation was supported by their findings that a higher level of perceived Internet privacy risk is related to a lower level of willingness to provide personal information to transact on the Internet. Consistent results regarding users’ concerns about privacy risk have been attained in research on OSN. Krasnova et al. (2010) found privacy risk to be a critical barrier to personal information disclosure. However, this privacy risk was mitigated by the user’s trust in the social network provider and the availability of control options. Lo (2010) evaluated a trust-risk model of information disclosure which considered privacy concern to be a dispositional factor and an
antecedent of trust. The results revealed privacy concern significantly impacted perceived risk and thus personal information disclosure. Consistent with these findings, we hypothesize:

Hypothesis 1a-f. A higher level of perceived online social networking privacy risk (PR) is associated with a lower level of willingness to provide types of personal information in online social networking:

a. Service Information (Serv)
b. Disclosed Information (Disc)
c. Entrusted Information (Entr)
d. Incidental Information (Incid)
e. Behavioral Information (Behav)
f. Derived Information (Deriv)

In calculating privacy risk, user assesses the likelihood of negative consequences and the perceived severity of these consequences with the disclosure of personal information (Xu et al. 2011). Previous empirical research in e-commerce has revealed a positive relationship between risk perception and privacy concerns (Dinev & Hart 2006a). Consistent with the previous privacy calculus research of Dinev and Hart (2006a), Dinev and Hart (2006b), Dinev et al. (2006), and Xu et al. (2011), we assess privacy risks as antecedent to privacy concerns:

Hypothesis 2. A higher level of perceived online social networking privacy risk (PR) is associated with a higher level of online social networking privacy concerns (PC):

We concur with Xu et al. (2011) about the “complexity of and inconsistencies in defining and measuring privacy” (p. 800) and adopt the movement they noted within the field of IS to consider privacy “concerns” as the central construct to capture “beliefs,” “attitudes,” and “perceptions” of privacy. Previous research has examined privacy concerns as an antecedent to behavior, including willingness to disclose personal information (Chellappa & Sin 2005), intention to transact (Dinev & Hart 2006b), and willingness to disclose personal information to transact. The empirical findings of Dinev and Hart (2006a) support a negative relationship, as we hypothesize, between privacy concerns and revealing personal information:

Hypothesis 3a-f. A higher level of online social networking privacy concerns (PC) is associated with a lower level of willingness to provide types of personal information in online social networking:

a. Service Information (Serv)
b. Disclosed Information (Disc)
c. Entrusted Information (Entr)
d. Incidental Information (Incid)
e. Behavioral Information (Behav)
f. Derived Information (Deriv)

3.2 Benefits: Trust and Personal Interest

Trust is regarded as a central aspect in the acceptance of technology (Gefen 2002). For example, consumer satisfaction with an online firm is based upon trust and credibility (Schoenbachler & Gordon 2002). Gross and Acquisti (2005) noted that privacy may be conducive to and necessary for intimacy, but trust may decrease within an OSN. However, Dinev and Hart (2006a) found that higher OSN trust was associated with willingness to provide personal information. We therefore hypothesize that:

Hypothesis 4a-f. A higher level of online social networking trust (T) is associated with a higher level of willingness to provide types of personal information in online social networking:

a. Service Information (Serv)
b. Disclosed Information (Disc)
c. Entrusted Information (Entr)
d. Incidental Information (Incid)
e. Behavioral Information (Behav)
f. Derived Information (Deriv)
Consistent with Dinev and Hart (2006a), who found a negative relationship between privacy risk and trust, we assess privacy risks as antecedent to trust in OSN:

Hypothesis 5. A lower level of perceived online social networking privacy risk (PR) is associated with a higher level of online social networking trust (T).

In accordance with (Dinev & Hart 2006a), we consider personal interest to be an intrinsic motivation based on a belief that engaging in an activity provides self-fulfilling satisfaction, which is captured by the degree of cognitive attraction in computer interactions (Dinev & Hart 2006a). Their empirical findings provide support for a positive relationship between personal interest and the users’ willingness to provide personal information:

Hypothesis 6a-f. A higher level of personal online social networking Interest (PI) is associated with a higher level of willingness to provide types of personal information in online social networking:

a. Service Information (Serv)
b. Disclosed Information (Disc)
c. Entrusted Information (Entr)
d. Incidental Information (Incid)
e. Behavioral Information (Behav)
f. Derived Information (Deriv)

4 RESEARCH METHODOLOGY

A questionnaire administered to undergraduate students will be utilized for this study because this methodology increases generalisability, facilitates replicability, and provides statistical power (Dooley 2001). The use of students as subjects is appropriate because they are, as high volume users of both the Internet and OSN, appropriate for the context. We acknowledge the limitation of the use of a convenience sample, collected from a specific geographic location (i.e., a private university located in the mid-Atlantic U.S.), for this study.

4.1 Measures

Questionnaire items, based on previous research, will be used to measure the research variables. The questionnaire will also capture demographic information. All variables will be measured using multiple items, with the exception of demographics.

4.2 Procedure

The questionnaire was reviewed by three colleagues who have expertise in both methodology and in the subject area resulting in very minor corrections. Additionally, we undertook a pilot test to confirm that the questions were worded properly and are appropriate for our sample. As was done for the pilot study, we will distribute our questionnaire through a systematic email accompanied by clear instructions for completing the questionnaire. The questionnaire will be administered through the web-based survey tool Survey Monkey, to present a clear layout and instructions for the questions.

5 RESEARCH CONTRIBUTION

We expect our study to contribute to the nascent body of research addressing the privacy calculus in the context of OSN by extending the extended privacy calculus model for e-commerce transactions, developed by Dinev and Hart (2006a), to this realm. We also expect our study to have practical implications for online vendors regarding privacy concerns about types of information users disclose.
References


