The Face-Off Between User Privacy and Information Exploitation in Online Social Networking

Jing Wang, University of New Hampshire, USA

ABSTRACT

This research examines the extent to which and the path through which privacy concerns may trigger negative consequences in Social Networking Sites (SNS). Contradicting conventional wisdom that privacy concerns could severely impede the adoption and diffusion of online social networking, the results indicate that privacy concerns and risk beliefs do not directly impact individuals’ willingness to share information through SNS. However, privacy concerns and risk beliefs do impede individuals’ willingness to be profiled by SNS for personalized services and advertisement. Privacy concerns also positively impact risk beliefs and negatively impact trusting beliefs. Trusting beliefs positively influence individuals’ willingness to share information through SNS and willingness to be profiled by SNS for personalized services and advertisement.

Keywords: Information Exploitation, Information Sharing, Privacy, Privacy Concerns, Risk, Social Networking, Trust

INTRODUCTION

While social networking sites (SNS) are rapidly growing in popularity, user privacy concerns on these sites have become an important issue for policymakers, trade groups, and user advocates. Information practices widely seen as endangering privacy continue to escalate within SNS. Popular SNS such as Facebook, Google Buzz, and Twitter have all come under fire for their privacy practices and suffered damage to their credibility, reputation, and brand. When Facebook launched its Beacon initiative in November 2007 and modified its terms of service without notifying its users in Spring 2010, the uproar was swift and fierce. Privacy advocates and frustrated users called on regulators to intervene, and the firm was eventually forced to backtrack. Google’s introduction of the auto-follow feature on Buzz, its social networking and messaging tool, represents another privacy nightmare that has heaped mounting criticism and outrage on the company. Since many SNS business models are built upon information collection and exploitation, the face-off between users’ privacy and the economic prerogatives of these sites becomes inevitable. Nevertheless,
contradicting conventional wisdom that privacy concerns could severely impede the adoption and diffusion of online social networking, new users continue to flock to SNS such as Facebook and Twitter and loyal users stick with them. By January 2011, Facebook had more than 500 million users who spent over 700 billion minutes per month on its website. Facebook is now the largest photo sharing website and first-choice for messaging and chatting. Consequently, this study poses an interesting research question of how online social networking sites can continue to succeed and thrive even in the presence of significant privacy concerns.

One explanation for the continual success of SNS in the presence of mounting privacy concerns may be that privacy concerns do not matter in the SNS context. Based on the literature, concerns over privacy vary significantly depending on the context. For instance, a person may be willing to submit his or her personal and credit card information for an online purchase because s/he may not perceive the payment procedure as invasive, but as a necessity to obtain the benefits of the product or service. However, s/he may feel uncomfortable if that information is then linked to other primary and secondary data such as browsing behavior on the Web site and demographic information (Hann, Hui, Lee, & Png, 2007). SNS distinguish themselves from traditional online transaction environments since the basic tenet of SNS is for people to voluntarily share their personal information. Given this voluntary nature, it is possible that privacy concerns do not matter in the SNS context, or at least not as much as in other online transaction environments. Thus, it would be unwise to assume that findings from other online transaction environments would automatically transfer to the SNS context and privacy concerns in SNS warrant further investigation. Currently, few studies have investigated information privacy in the context of social networking and most studies focus on the marketing (direct and online), digital medical records, and e-commerce contexts.

Further, while privacy concerns may trigger different consequences, extant research in this area largely focuses on users’ (un)willingness to provide personal information (Son & Kim, 2008). Considering that SNS business models are built on information collection and exploitation, another consequence that is of particular interest to an SNS site is individuals’ willingness to allow the site to profile them using the personal information they share on the site. Consequently, the objective of this research is to examine the extent to which and the path through which privacy concerns may trigger negative consequences in the SNS context. In addition to the (un)willingness to divulge information, this research investigates one other consequence that may be triggered by privacy concerns: (un)willingness to be profiled for personalized services and advertisements.

The paper begins with a review of relevant literature. It then presents the theoretical arguments followed by hypothesis development. Thereafter, the proposed hypotheses are empirically evaluated using survey data. Finally, the findings, implications, and limitations of this research are presented and suggestions for future research are discussed.

**LITERATURE REVIEW**

Given its multidimensional, contextually dependent, and dynamic nature, it is difficult to establish a single unified definition of privacy that can be operationalizable across disciplines. Many sociologists define privacy as the “the moral right of individuals to be left alone” (Laudon & Traver, 2001, p. 467). Information systems (IS) researchers have tailored the definition toward the informational aspect and define privacy as the right to control the collection, disclosure, and use of information about oneself (Awad & Krishnan, 2006; Dinev & Hart, 2006; Smith, Milberg, & Burke, 1996; Stone, Gueutal, Gardner, & McClure, 1983). Individuals’ information privacy concerns arise from the feeling that they are vulnerable in controlling the collection and use of their personal information (Dinev & Hart, 2004). Smith et al. (1996) identify four distinct yet
A Triangulation Approach to Understand Multi-Cultural College Students’ Technology Literacy in a Composition Classroom: Implications for Global Literacy Theory and Practices


[www.igi-global.com/chapter/a-triangulation-approach-to-understand-multi-cultural-college-students-technology-literacy-in-a-composition-classroom/96060?camid=4v1a](www.igi-global.com/chapter/a-triangulation-approach-to-understand-multi-cultural-college-students-technology-literacy-in-a-composition-classroom/96060?camid=4v1a)