Computers in Human Behavior 33 (2014) 153–162

Contents lists available at ScienceDirect

Computers in Human Behavior

journal homepage: www.elsevier.com/locate/comphumbeh

Teens' concern for privacy when using social networking sites: An analysis of socialization agents and relationships with privacy-protecting behaviors

Yang Feng [a,*], Wenjing Xie [b]

[a] College of Mass Communication and Media Arts, Southern Illinois University Carbondale, Carbondale, IL 62901, United States
[b] School of Journalism, Southern Illinois University Carbondale, Carbondale, IL 62901, United States

ARTICLE INFO

Article history:
Available online 11 February 2014

Keywords:
Privacy-protecting behaviors
Parental influence
Social networking site (SNS) use
Privacy concern
Teen

ABSTRACT

U.S. teens are spending substantial time on social networking sites (SNSs). Yet, only a few studies have documented teens' privacy-protecting behaviors on SNSs. Using data of Facebook teen users and their parents in the U.S. from the Pew Internet's Teens & Privacy Management Survey ($N = 622$), this study investigated the socialization agents of teens' level of online privacy concern, and the relationship between teens' level of online privacy concern and their privacy-protecting behaviors on SNSs. Based on path analysis results, this study identified parents and SNS use as the two significant socialization agents. In particular, this study revealed the role of parents' privacy concern and the role of SNS use in motivating teens to increase online privacy concern, which, in turn, drives teens to adopt various privacy-setting strategies on SNSs and to set their Facebook profiles to private. Implications for policy-makers and educators were discussed.

1. Introduction

With the increasing popularity of social networking sites (SNSs) among teens, Lenhart et al. (2011) reported that Facebook has become the dominant social networking site among U.S. teens aged 12–17 and that 93 percent of teen SNS users have established a Facebook account. Considering the extent of teens' use of SNSs such as Facebook, privacy advocates have raised concerns about teens' vulnerability to privacy risks (Schonberger, 2005). Such concerns may not be in a vacuum. Survey from Pew Internet Research suggested that teens face potential risks associated with online life: while 43 percent of teen SNS users have been contacted online by strangers, 17 percent of teen SNS users have become "friends" with whom they have never personally met (Lenhart & Madden, 2007).

With the increasing use of SNSs among teens, online marketers try to reach more teens through social media and SNSs have become an important venue for them to collect teen consumers' information (Boveda-Lambie & Hair, 2012). For example, Facebook is sponsored by advertising revenue. Its privacy policy clearly states that "Facebook is a free service supported primarily by advertising. We will not share your information with advertisers without your consent. We allow advertisers to select characteristics of users they want to show their advertisements to and we use the information users share with us to serve those advertisements... We (Facebook) take steps to ensure that others use information that you share on Facebook in a manner consistent with your privacy settings" (Facebook., 2009).

Regarding marketers' collection of information that teens share online, government regulations such as the Children's Online Privacy Protection Act (COPPA) require marketers to seek verifiable parental consent before collecting information from children under the age of 13 (Sheehan, 2004). However, teens above the age of 13 are not protected by COPPA. Moreover, existing regulations mainly focus on restricting online marketers' active collection of children's information, and children's and teens' voluntary information disclosure online are rarely covered. Since SNS users are motivated to share information in the virtual community and teens are not aware of online privacy as much as adults are (Lenhart & Madden, 2007), it would be especially hard to restrict teens to disclose information on SNSs. The inability to curb teens' voluntary information disclosure online, along with the increasing information sharing among teens, raises both public and parental concerns about online risks resulting from teen privacy loss (Willard, 2007). For instance, one online risk stemming from online marketers' attempts to collect personal information from teens is identity fraud (Schonberger, 2005). Another online risk is the bombardment

[*] Corresponding author. Tel.: +1 614 256 0063.
E-mail addresses: fengyang29@live.com (Y. Feng), wxie@siu.edu (W. Xie).

http://dx.doi.org/10.1016/j.chb.2014.01.009
0747-5632/© 2014 Elsevier Ltd. All rights reserved.

of unwanted commercial e-mails caused by teens' disclosure of personal information on SNSs (Grant, 2006; Liau, Khoo, & Ang, 2005). Regarding these online risks that teens face, it is necessary to explore the factors that increase teens' privacy concern and that encourage teens to take control of privacy settings on SNSs.

This study attempts to add to our knowledge by examining the privacy-protecting behaviors of teens aged 12–17, and the role of their parents and SNS usage in their privacy-protecting behaviors on SNSs. Our first aim is to examine the important socialization agents that influence teens' online privacy concern. The second aim is to explore the relationship between teens' level of online privacy concern and teens' privacy-protecting behaviors on SNSs, including their implementation of various privacy-setting strategies on SNSs and profile visibility on Facebook. The third aim is to investigate the demographic influence on the two socialization agents (parents' level of privacy concern, teens' level of SNS use), on teens' level of privacy concern, and on teens' privacy-protecting behaviors on SNSs.

2. Literature review

2.1. Concept of privacy and privacy settings on SNSs

Before discussing teens' privacy concern and privacy-protecting behaviors on SNSs, we will first explain the concept of privacy to provide a conceptual foundation about what privacy means and how the concept of privacy is applied in the context of SNSs. We will operationalize one of the dependent variables of this study – privacy-setting strategies – on the basis of the concept of privacy. We will also discuss the privacy options and settings on Facebook, which provides the operationalization of another dependent variable of this study – Facebook profile visibility.

As Palen and Dourish (2003) pointed out, privacy is a concept with multidimensional aspects and there is no consensus about a universally accepted definition of privacy (Wildemuth, 2008). Some scholars identified four distinct concepts of privacy (Introna, 1997), two of which have been regarded as directly related to technology use (Taraszow, Aristodemou, Shitta, Laouris, & Arsoy, 2010). One of the concepts of privacy is based on Westin (1967)'s idea that privacy is one's control over his or her own personal information. Westin (1967) defined privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (p. 7). Westin (1967, 2003)'s concept of privacy relies heavily on the impacts of information and communication technologies. According to Westin (2003), when information-technology developments were very limited, there was high public trust in and public comfort with the information collection and use activities by government and other agencies. Advances in physical, psychological, and data surveillance technologies such as mainframe computers in the 1960s started to make people recognize the dark side of new technologies regarding privacy intrusion. For example, a national survey in 1978 showed that 64% of the public were concerned about threats to personal privacy, up from 34% in 1970 (Westin, 2002). The rise of the Internet and the arrival of ubiquitous wireless communication devices such as the cell phone raised the privacy issue to be a first-level social issue in the U.S. (Westin, 2003). By virtue of these technologies, advertisers and business industries can use web site cookies to identify visitors, document and track their usage, and deliver advertisements or marketing messages based on consumers' private and personal information, which drew increased consumer annoyance (Garfinkel, 2000; Westin, 2002).

Westin (1967, 2003)'s concept of privacy is related to information and communication technology in general, and can be applied in the context of SNS use in particular. With the feature to connect people, SNSs encourage or even require a user to reveal his/her real name, email, school, location and other identities when he/she registers for personal accounts, which leaves privacy a big concern (Lewis, Kaufman, & Christakis, 2008). Meanwhile, SNSs such as Facebook can provide large-scale data that people have never seen on previous types of media (Lohr, 2012). The development of data-mining technologies and applications, which was envisioned by Westin (2003), made it possible for advertisers or other third parties to obtain in-depth characteristics and personal interest of the consumers by tracking their privacy and personal information disclosed on SNSs (Lohr, 2012).

Another concept of privacy focuses on the "monitored" and "searchable" part of anyone's life (Lessing, 1998), which is also applicable in the context of SNS use. Lessing (1998) defined privacy as the part "which is left after one subtracts, as it were, the monitored, and the searchable, from the balance of social life" (p. 1). The monitored means the part of the life that is watched by the public in a regular way. For instance, in a small community, people's behaviors such as coming and leaving, buying in the local market, and talking with other people, can be observed and monitored by neighbors. The searchable means a person leaves letters, diaries, footprint, and other stuff or information in the environment through which other people can find, notice, or trace him/her. Lessing (1998) argued that under the traditional monitoring system such as a small community, data collected and monitored were transient and had high cost. For example, what people said and did was very easy to be forgotten or disregarded by their neighbors. However, crude modern technologies such as emails and telephone records made the data permanent and more searchable.

Looking at SNSs such as Facebook, users' behaviors and information are also monitored and searchable. People can disclose demographic information, update status, share emotions and thoughts, post photos and videos, and share personal interest on SNS, which makes advertisers easily observe and monitor their behaviors. Moreover, SNS users' names and profile photos appear in their friends' friend list. They can also leave comments on friends' timeline, photos, and videos and be tagged in others' news feeds, photos, and posts, through which they leave a footprint or record that is searchable and traceable by others, including advertisers and other third parties. Hence, Lessing (1998)'s concept of privacy is highly relevant for the discussion and research of privacy in SNSs. In this study, we will adopt Lessing (1998)'s concept of privacy and examine if teens have deleted or modified their monitored or searchable information on Facebook such as name, age, location, tags, comments, posts, friends, or even have deactivated their profiles or accounts, to protect their privacy.

Even though there were privacy concerns regarding SNS use, Facebook did not have the privacy-setting function until the beginning of 2008. Before that, Facebook had been criticized for its invasion of privacy and its potential commercial exploitation by third parties (Debatin, Lovejoy, Horn, & Hughes, 2009). Advertisers and online marketers can access Facebook users' personal information such as age, gender, location, hometown, photos, and personal interest without permission or authorization. They can also use Facebook for data tracking, phishing, and other malicious purposes, which can be considered as unethical or even illegal use of users' property (Guo, 2010). Research showed that the information disclosed on Facebook can be sufficient for third parties to identify a single user, even with the name removed (Felt & Evans, 2008). Other concerns also have been raised about the links between Facebook and its use by other agencies (Debatin et al., 2009). For example, the Patriot Act (2006) permits state agencies to disregard the privacy settings on Facebook to look up employees' information.