Information & Management 52 (2015) 882–891

Contents lists available at ScienceDirect

Information & Management

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

An empirical analysis of users' privacy disclosure behaviors on social network sites

Kai Li [a], Zhangxi Lin [b], Xiaowen Wang [c,*]

[a] Business School, Nankai University, 94, Weijin Road, Tianjin 300071, China
[b] Center for Advanced Analytics and Business Intelligence, Texas Tech University, Lubbock, TX 79409, United States
[c] School of Economics, Nankai University, 94, Weijin Road, Tianjin 300071, China

ARTICLE INFO

Article history:
Received 15 September 2014
Received in revised form 27 June 2015
Accepted 9 July 2015
Available online 17 July 2015

Keywords:
Privacy disclosure
Social media
Social network sites
Generalized linear model

ABSTRACT

Users' privacy on social network sites is one of the most important and urgent issues in both industry and academic fields. This paper is intended to investigate the effect of users' demographics, social network site experience, personal social network size, and blogging productivity on privacy disclosure behaviors by analyzing the data collected from social network sites. Based on two levels of disclosed privacy sensitivity information, the textual information of a user's blog postings can be converted into a 4-tuple to represent their privacy disclosure patterns, containing the breadth and depth of disclosure, and frequencies of highly and less sensitive disclosures. Collections of a user's privacy disclosure patterns in social network sites can effectively reflect the user's privacy disclosure behaviors. Applying the general linear modeling approach to blogging data converted with a coding scheme, we find that males and females have significantly differentiated privacy disclosure patterns in dimensions related to the breadth and depth of disclosure. In addition, age has a significant negative relationship with the breadth and depth of disclosure, as well as with highly sensitive disclosure. We also find that social network site experience, personal social network size, and blog length are not significantly related to users' privacy disclosure patterns, while blog number always has positive associations with privacy disclosure patterns.

© 2015 Elsevier B.V. All rights reserved.

1. Introduction

Social media are a group of Internet and mobile based applications build on Web 2.0 technologies in which people can create, share, or exchange user-generated content. Currently, social media is becoming increasingly important in our daily life and has received substantial scholarly attention [46]. Social media outlets rely on the Internet and mobile technologies to provide interactive platforms for information dissemination, content generation, and interactive communications [65]. An array of Internet and mobile-based applications define the way social media functions. Examples include weblogs, microblogs, online forums, wikis, podcasts, life streams, social bookmarks, web communities, social networking, and avatar-based virtual reality [2,18,69]. Based on these applications, social network sites (SNS) have gained tremendous momentum, revolutionizing the way individuals build and maintain interpersonal relationships [1,70].

Because people are increasingly incorporating SNS as a part of their routine social activities, the number of SNS users has grown exponentially in recent years. Every minute, terabytes of user-generated content are posted by millions of users on various social network sites, such as LinkedIn, Facebook, Twitter, QQ, etc. In this way, SNS, underpinned by social media, become versatile resources for both industry stakeholders and scholars to study the enriched and dynamic data contributed by a wide range of users in the social network sphere [34].

In the past decade, research has focused largely on the adoption and usage of SNS [33,71], as well as the management of social relationships on SNS [17]. Limited work has covered the topic of privacy disclosure. In fact, privacy disclosure on SNS is becoming one of the most important and active research issues in the information systems arena [25], as the influx of user-generated content into various SNS has resulted in major concerns over the misuse of these data. Meanwhile, the Web 2.0 era demands data openness for all kinds of innovative online businesses, and as a

* Corresponding author. Tel.: +86 13821691316.
E-mail addresses: edu.cn">likai@nankai.?edu.cn (K. Li), zhangxi.lin@ttu.edu (Z. Lin), edu.cn">wangxw@nankai.?edu.cn (X. Wang).

http://dx.doi.org/10.1016/j.im.2015.07.006
0378-7206/© 2015 Elsevier B.V. All rights reserved.

result, increasing privacy information disclosure. Openness would essentially help to reduce the uncertainty of interactions, legitimate access to a person in an online group, and ultimately promote online business [39,62].

Personal information exchange between users on social network sites allows these people to maintain relationships with friends, develop new friendships, and find support and information [62]. Privacy disclosure on SNS has a negative side, however; greater disclosure may correspond also to information theft, trafficking, and privacy invasion. Gross and Acquisti [21] found that users effectively place themselves at a greater risk for cyber and physical stalking, identity theft, and surveillance when they disclose personal information on SNS. As such, concern over the negative effects of privacy disclosure has a major influence in users' adoption and routine use of SNS [71]. Therefore, this paper is intended to examine the predictability of privacy disclosure behaviors on SNS in terms of the privacy sensitivity levels of information to be disclosed (in short, we will use "sensitivity levels of information" implying the context of privacy). We will investigate the differences between users' disclosure of highly sensitive information and less sensitive information in relation to SNS structure and mechanisms. These are particularly important questions for SNS industry service providers; hence providing insight into this theme can prove useful in practical applications such as interface design and SNS privacy policy.

Our study contributes to the literature by focusing on predictors of SNS privacy disclosure. Communication Privacy Management theory is introduced as a framework to clarify the influence of users' gender, age, social network site experience, personal social network size, and blogging productivity on their privacy disclosure behaviors. Specifically, privacy disclosure is divided into two dimensions: breadth and depth. Highly sensitive disclosure and less sensitive disclosure are also distinguished in the study. To test these models, we collected practical data from one of the most popular social network sites. The results clarified various predictors of SNS privacy disclosure and offered insights into the social implications of SNS.

The remainder of this paper is structured as follows. Related literature about privacy disclosure on social network sites is reviewed to provide the theoretical background and foundation for our study in Section 2. We describe the research methodology of this paper in Section 3, including data, variables, and models. Empirical results are presented in Section 4. Finally, we conclude the paper and suggest future research directions.

2. Literature review

2.1. Privacy disclosure on social network sites

Information privacy has been considered one of the most important "ethical issues of the information age" [38,56,57]. As a philosophical, psychological, sociological, and legal concept, it has been studied extensively across multiple disciplines in the social sciences [58]. Generally, information privacy refers to an individual's control over the release of personal information [7,8], including its collection, unauthorized use, improper access, and errors [57]. Researchers from various academic disciplines view information privacy as different concepts. In the information systems (IS) domain, privacy is usually studied based on two definitions. The first is the control-based definition of privacy offered by Westin [66], in which privacy is constructed 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". This kind of control refers to the limiting of vulnerability during information transactions [37]. A second definition is based on commodities [14], arguing that privacy can be traded and marketed and is subject to the economic principles of cost–benefit analysis and trade-offs [58]. The commodity-based definition now is the underlying assumption in many studies and theories in IS.

Recently, privacy disclosure has become an important phenomenon, particularly on online social network sites [25]. However, most literature about privacy in IS focuses on privacy concern. Dimensions, predictors, outcomes, and measurement of privacy concern have been discussed and developed [22,58]. Such developments could be one of the reasons why recent articles have noted the importance of information privacy in the IS literature and the need for additional empirical studies [48,53,58].

Privacy disclosure is generally referred to as the self-disclosure of personal information. Self-disclosure is a concept borrowed from sociology which refers to the process of individuals communicating information about themselves with other persons [67]. Intimacy and sensitivity appear to be particularly critical to information self-disclosure in previous studies in social psychology. Self-disclosure is considered to be an important building block for intimacy; therefore, degree of intimacy is used to define categories of disclosed information [4]. Information sensitivity must also be considered in discussions of personal disclosure. Previous privacy studies have found that consumers' willingness to disclose personal information depends on the sensitivity of this information [36]. While intimacy is related more to an intrinsic risk, sensitivity is related to an extrinsic risk such as monetary loss [43]. Altman and Taylor [4] concluded that there are two dimensions to self-disclosure: breadth and depth. Both are crucial in developing a fully intimate relationship. It is easier for breadth to be expanded first in a relationship due to its more accessible features; it consists of outer layers of personality and elements of everyday life, such as occupations and preferences. Depth is more difficult to reach, given its inner location; it includes more sensitive memories and traits that we might try to hide from others not well known to us. This is why we reveal ourselves most thoroughly and discuss the widest range of topics with our spouses and loved ones [64]. At present, the most popular explanation of users' privacy disclosure is illustrated by the privacy calculus model, which draws on the exchange theory [29,59]. Individuals are willing to disclose personal information in exchange for some social benefits [13,16]. Therefore, an individual's decision to disclose private information on social media becomes a rational choice. As personalized services become more popular on social media platforms [27], a personalization–privacy paradox arises from privacy calculus in different contexts ranging from online web [5] to mobile [61,68].

While it is beneficial for people to disclose different kinds of information on social network sites, some degree of risk necessarily accompanies the benefits of disclosure; prompting concern among scholars, privacy advocators, and the media [7,22]. In the existing literature, the proposed privacy paradox implies that individuals who perceive high benefit and low risk will have a greater intention to disclose privacy. However, research has also found that people do not always act rationally in their privacy disclosure [3]. At times the perception of high privacy risk and low intention to disclose information still result in relatively higher levels of actual information disclosure [44]. This phenomenon causes us to disregard the "trade-off" approach based on perceived benefits and risks.

On a social network site, privacy disclosure is related not only to the amount of personal information that an Internet user decides to release to others [25] but also to the ease with which a user can be identified as a real person [20]. SNS has been likened to a stage upon which people can manipulate information, choosing what to disclose and what to hide [62]. In this study, we therefore treated privacy disclosure as an individual privacy boundary management

Download English Version:

https://daneshyari.com/en/article/553780

Download Persian Version:

https://daneshyari.com/article/553780

Daneshyari.com