International Journal of Information Management 37 (2017) 1428–1440

Contents lists available at ScienceDirect

International Journal of Information Management

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

Research note

Let the users tell the truth: Self-disclosure intention and self-disclosure honesty in mobile social networking

Le Wang[a,b,*], Jie Yan[c], Jun Lin[a], Wentian Cui[a]

[a] School of Management, Xi'an Jiaotong University, Xi'an 710049, China
[b] Sociology, University of Chicago, Chicago 60637, USA
[c] Grenoble Ecole de Management, Grenoble 38003, France

ARTICLE INFO

Article history:
Received 19 June 2016
Received in revised form
27 September 2016
Accepted 24 October 2016

Keywords:
Self-disclosure intention
Self-disclosure honesty
Mobile social networking
Social rewards
Privacy concern
Flow experience
Self-esteem
Application reputation
Compatibility

ABSTRACT

Large amounts of customer data present rich business opportunities. Drawing on the privacy calculus model, this study investigates the antecedents of self-disclosure intention and self-disclosure honesty. We extend the privacy calculus model by exploring how the characteristics of service providers and the interpersonal difference of users influence privacy trade-off. An online empirical survey that involves 913 respondents was conducted. We find that both monetary rewards and social rewards positively predict self-disclosure intention, whereas only social rewards positively predict self-disclosure honesty. Moreover, application reputation and flow experience of users weaken the perceptions of privacy concern, and application compatibility and flow experience strengthen the perceptions of social rewards. Our results suggest that users place more weight on social rewards than on monetary rewards. Therefore, service providers are advised to create salient and distinct social rewards. They can also adopt distinct marketing strategies based on their profiles and the interpersonal difference of their users.

1. Introduction

The popularity of mobile devices has made mobile social networking an indispensable part of people's daily lives (Fan & Gordon, 2014). Statistics show that the mobile daily active users of Facebook reached 989 million in March 2016 (Facebook, 2016). Approximately half of the mobile Twitter users log on to their account the moment they wake up (Twitter, 2015). Activities on social media leave trails of data that expose users' interests, beliefs, and intentions. By utilizing social media analytics techniques, such as opinion mining, sentiment analysis, and social networks, large amounts of customer data have become gold mines for exploiting potential business opportunities (Erevelles, Fukawa, & Swayne, 2016; Gandomi & Haider, 2015).

However, the misuse of personal information is alarming (Awad & Krishnan, 2006). Individuals under the risks of privacy invasion tend to avoid self-disclosure, disclose incomplete information, or manipulate their profiles (Acquisti, Brandimarte, & Loewenstein, 2015). Failure to encourage self-disclosure or obtain inaccurate customer information may cause social and economic impacts (Mason & Harris, 2005; Robertshaw & Marr, 2006). Therefore, it is highly important to understand the factors that predict users' self-disclosure intention and self-disclosure honesty.

The privacy calculus model, which argues that self-disclosure intentions are determined by the rational calculus of the benefits and costs of privacy behaviours, is widely adopted in information system (IS) literatures (Dinev & Hart, 2006; Jiang, Heng, & Choi, 2013; Wang, Duong, & Chen, 2016). Külcü and Henkoğlu (2014) revealed that the concern for the loss of privacy is a significant barrier for self-disclosure in the information age. Monetary rewards, such as cash bonus, discounts and coupons can compensate the privacy concerns of disclosing personal information in online transactions (Posey, Lowry, Roberts, & Ellis, 2010). Social rewards, such as pleasure, satisfaction, and relationship development may also offset the risks of privacy invasions (Jiang et al., 2013; Liu, Min, Zhai, & Smyth, 2016). Individuals perform a costs-benefits calculus before self-disclosure and they may disclose their personal information if the benefits outweigh the costs. Recent studies have enriched the concepts of costs and benefits in the privacy calculus

* Corresponding author at: School of Management, Xi'an Jiaotong University, Xi'an 710049, China.
E-mail address: lewang@uchicago.edu (L. Wang).

http://dx.doi.org/10.1016/j.ijinfomgt.2016.10.006
0268-4012/

model. For instance, the concept of costs has been extended to multiple aspects such as trust in service providers (Chang, Cheung, & Tang, 2013) and sensitivity toward personal information (Bansal & Gefen, 2010). The concept of benefits has been extended to perceived usefulness (Hess, McNab, & Basoglu, 2014), relationship building and maintenance (Ellison, Vitak, Gray, & Lampe, 2014), and emotional support (Oh, Ozkaya, & LaRose, 2014). Several gaps have emerged from the existing literatures.

First, the antecedents of self-disclosure intention have been recognized (Posey et al., 2010; Wang et al., 2016; Zhao, Lu, & Gupta, 2012), whereas those of self-disclosure honesty have been given less attention. Misrepresentations and deceptions commonly occur in virtual social interactions (Krasnova, Spiekermann, Koroleva, & Hildebrand, 2010). Moreover, inaccurate information causes substantial social and economic impacts. For example, inaccurate customer data may mislead manager's strategic decisions (Mason & Harris, 2005) and create bias in the research of marketing scholars (Robertshaw & Marr, 2006). Thus, the first objective of this study is to investigate the factors that predict sincere and accurate self-disclosure.

Second, previous studies fail to differentiate the roles played by social rewards and monetary rewards in predicting privacy protective behaviours. Existing studies on the privacy calculus model focus on either monetary (Premazzi et al., 2010) or social rewards (Jiang et al., 2013) in offsetting privacy risks. Other studies that propose social and monetary rewards jointly predict privacy protective behaviours have integrated them into an aggregate construct (Youn, 2009). Social and monetary rewards differ in predicting behaviours (Deci, Koestner, & Ryan, 1999). For example, individuals in search for emotional supports are willing to disclose their inner feelings. Conversely, individuals may share a superficial self-disclosure for monetary rewards. Therefore, the second objective of this study is to provide a comprehensive understanding of the privacy calculus model by differentiating the roles of social and monetary rewards.

Third, the privacy calculus model views the privacy protective behaviours as a result of a rational calculus of the costs and benefits. However, not all individuals are rational, and an individual cannot be rational at all times. The perceptions of privacy concerns and rewards, especially social rewards, are influenced by interpersonal difference and contextual settings (Acquisti et al., 2015). For example, adults have a higher reward threshold for self-disclosure than teenagers (Youn, 2009). Individuals who are addicted to a certain type of activity may ignore or downplay the negative effects of that activity (Partington, Partington, & Olivier, 2009). Contextual settings influence the way people manage their privacy. For instance, we may reveal personal information to a stranger on a plane, which rarely happens in other situations. Legal regulations are positively related to the intention of disclosing personal information (Andrade, Kaltcheva, & Weitz, 2002). In general, the privacy protective behaviours vary with interpersonal differences and specific contexts given certain amounts of rewards and risks. Thus, the third objective of this study is to explore the influence of interpersonal difference and contextual settings on privacy trade-off.

The results of the present study inform theory and practice in several aspects. Investigating the antecedents of self-disclosure honesty provides a comprehensive understanding of privacy protective behaviours. We differentiated the roles of social rewards and monetary rewards in predicting privacy protective behaviours. Moreover, we provided evidence that privacy trade-off depends on interpersonal difference and contextual settings. This study offers practical insights as well. For self-disclosure intention, we found that users of mobile social media place more weight on social rewards than on monetary rewards. Monetary rewards were not found to predict self-disclosure honesty. These findings suggest that service providers should exert additional effort to create salient and distinct social rewards. Operators of social media are suggested to broaden their brand awareness, as we found that application reputation helps attenuate the perceptions of privacy concern. The flow experience of users has been shown to mitigate the perceptions of privacy concern and strengthen the perceptions of social rewards. Service providers are encouraged to maximize the flow experience of their users. Given that high self-esteem increases the perceptions of privacy concern, administering a self-esteem test before registering is advised such that service providers can recommend optional privacy policies. Overall, the results indicated that service providers may adopt distinct marketing strategies based on their profiles and the interpersonal differences of their users.

2. Theoretical background and hypotheses development

2.1. Self-disclosure and privacy calculus

Self-disclosure refers to the act of revealing personal information, such as locations, hobbies, and photos when registering or using mobile social networks (Posey et al., 2010). The user-generated data can possibly benefit academic scholars and business managers. The popularity of mobile social networking enables operators to collect large amounts of customer data. The "big data" of customers provide an ideal source for academic scholars in investigating consumer behaviours (Robertshaw & Marr, 2006). By utilizing social media analytics techniques, customer data are rich in opportunities for improving customer satisfaction and service quality (Fan & Gordon, 2014; Wang et al., 2016). However, individuals increasingly suffer from information misuse (Awad & Krishnan, 2006). Avoiding self-disclosure and deceptions are commonly adopted strategies for protecting privacy (Acquisti et al., 2015). For instance, users may manipulate their profiles for the purpose of conveying positive images to others (Krasnova et al., 2010). Users facing privacy risks may create and convey false information to others through synchronous online interactions (Jiang et al., 2013). Thus, the factors that drive sincere self-disclosures deserve further investigation.

Any social behaviour may result in costs and benefits. The privacy calculus model argues that individuals perform a costs-benefits analysis before self-disclosure (Dinev & Hart, 2006). In the context of mobile social interactions, one of the major threats of self-disclosure is the concerns for privacy invasion (Külcü & Henkoğlu, 2014). Users who disclose personal information may obtain social rewards, such as developing and maintaining intimate relationships with peers or monetary rewards, such as coupons, cash bonuses, and discounts. Essentially, individuals conduct a privacy calculus in which privacy concerns are weighed against perceived benefits when deciding whether to disclose personal information.

Privacy protective behaviours vary with interpersonal differences and specific contexts. Individuals who are highly sensitive toward personal information have greater concerns for privacy invasion and are thus less likely to self-disclose (Korzaan & Boswell, 2008). Similarly, persons with high self-esteem are highly self-protective (Crocker, Thompson, McGraw, & Ingerman, 1987). Individuals can exhibit any sentiment ranging from extreme concern to apathy about privacy depending on the situation. For example, the Chinese are open about financial matters, such as income, housing cost, and possession, which are private matters for most Western populations (Acquisti et al., 2015). The privacy calculus model provides a general foundation for predicting self-disclosure and taking interpersonal difference and contextual settings into account provides a comprehensive framework.