Full length article

Security and privacy in online social networking: Risk perceptions and precautionary behaviour

Paul van Schaik a, *, Jurjen Jansen b, Joseph Onibokun c, Jean Camp d, Petko Kusev e

a Teesside University, School of Social Sciences, Business and Law, Middlesbrough, United Kingdom
b NHL University of Applied Sciences, Cybersafety Research Group, Leeuwarden, The Netherlands
c The Union Advertising Agency, Union Digital, Edinburgh, United Kingdom
d Indiana University, School of Computing, Bloomington, IN, USA
e University of Huddersfield, Huddersfield Business School, Department of Management, Huddersfield, United Kingdom

A R T I C L E   I N F O

Article history:
Received 23 June 2017
Received in revised form 6 October 2017
Accepted 7 October 2017
Available online 9 October 2017

Keywords:
Online privacy
Information security
Social media
Risk perception
Facebook
Precautionary behaviour

A B S T R A C T

A quantitative behavioural online study examined a set of hazards that correspond with security- and privacy settings of the major global online social network (Facebook). These settings concern access to a user’s account and access to the user’s shared information (both security) as well as regulation of the user’s information-sharing and user’s regulation of others’ information-sharing in relation to the user (both privacy). We measured 201 non-student UK users’ perceptions of risk and risk dimensions, and precautionary behaviour. First, perceptions of risk and dread were highest and precautionary behaviour was most common for hazards related to users’ regulation of information-sharing. Other hazards were perceived as less risky and less precaution was taken against these, even though they can lead to breaches of users’ security or privacy. Second, consistent with existing theory, significant predictors of perceived risk were attitude towards sharing information on Facebook, dread, voluntariness, catastrophic potential and Internet experience; and significant predictors of precautionary behaviour were perceived risk, control, voluntariness and Internet experience. Methodological implications emphasise the need for non-aggregated analysis and practical implications emphasise interventions to promote safe online social-network use.

© 2017 Elsevier Ltd. All rights reserved.

1. Introduction

People are increasingly using online social networks (or social media)1, such as Facebook, Twitter and LinkedIn. However, information-sharing by social-network users can result in violations of privacy (Garg & Camp, 2015) and security (Benson, Saridakis, & Tennakoon, 2015). For example, a user whose contact details have been revealed may become the subject of harassment in a deliberate, repeated, and hostile manner (cyber-bullying) or become a potential victim of identity theft. It is therefore essential to study people’s use of online social networks, especially where users are non-specialists in security and privacy, to reduce such violations (Garg & Camp, 2015). In particular, by developing models of human behaviour in relation to computer security and -privacy, research has aimed to develop a better understanding of this risk-related behaviour (Anderson & Agarwal, 2010; Liang & Xue, 2010). Risk perceptions continue to play a fundamental role in these models, both in security (Huang, Patrick Rau, Salvendy, Gao, & Zhou, 2011) and privacy (Dinev, McConnell, & Smith, 2015). In the context of computer systems, three dimensions of information security (the protection of information by means of access control) are confidentiality (protection from unauthorised reading information), integrity (protection from unauthorised writing information) and availability (protection against actions that prevent reasonable access by legitimate users to their systems) (Schneier, 2015). Security is considered a necessary, but not sufficient requirement for privacy (Morton & Sasse, 2012). In this research, we study security- and privacy settings in Facebook.

Various conceptualisations of privacy have been published (e.g., Westin, 1967; Zureik & Stalker, 2010). In relation to online privacy, Dienlin and Trepte (2015) distinguish three types: informational privacy (control over the processing and transferring of personal information on line), social privacy (regulating proximity and...
distance toward others on line) and personal privacy (perceived control over emotional and cognitive outputs). The current study examines on the second type. We focus on privacy settings in social media because they play an important role in this regard by providing a mechanism for social privacy.

The aim of this research is to study security- and privacy-related risk perceptions and precautionary behaviour in social-network use. Our goals are to (1) determine how different potential security- and privacy-related hazards in an online social network are perceived, (2) establish to the extent to which people take precautions against different potential security- and privacy-related hazards, and (3) ascertain the antecedents of risk perception and precautions taken against risk of security- and privacy violations.

2. Theoretical approaches to studying risk perception

Various approaches to studying risk perception have been published. For the present study, the most significant ones are the following. **Availability** ("the ease with which instances come to mind") influences people's risk perception (Kahneman, 2011, p. 129). **Saliency** (the extent to which an event attracts attention), dramatic nature of an event (e.g., a plane crash) and the source of experience (e.g., personal experiences) can enhance **availability**. According to the **tract heuristic**, the more technologies or activities are associated with positive feelings (e.g., sunbathing), the less they are judged to be risky and the more they are judged to be beneficial (Finucane, Alhakami, Slovic, & Johnson, 2000).

Starr (1969) used population statistics of human behaviour to infer people's **revealed risk-related preferences** regarding particular technologies and human activities. He analysed the relationship between risk (the statistical expectation of death per hour of exposure) and benefit (the average amount of money spent per individual participant or the average contribution made to a participant's annual income) for some common activities. However, the approach of revealed preferences suffers from several shortcomings. First, preferences may not be stable over time and aggregate data do not take into account the variability among hazards (Fischhoff, Slovic, Lichtenstein, & Combs, 1978). Second, the underlying assumption that people both have full information and use that information optimally has been refuted (Simon, 1956). Third, different measures of risk and benefit lead to different conclusions (Fischhoff, Slovic, Lichtenstein, Read, & Combs, 1978).

Psychometric methods have been used to study **expressed risk preferences** regarding particular technologies and human activities (Slovic, 1987). This has the advantage of eliciting perceptions (thoughts and judgments) of risk from people who are (potentially) exposed to particular risks that are studied, and can provide information about the causes of behaviour and potential ways to influence this. Applications of the results of work using these methods include risk communication (e.g., Kim, Choi, Lee, Cho, & Ahn, 2015; Young, Kuo, & Chiang, 2015) and risk policy (e.g., Huang et al., 2013). From a set of risk dimensions (e.g., voluntariness, controllability and newness; see Online Appendix OA1), prediction equations of risk perception have been developed (Fischhoff et al., 1978). A limitation is that data are usually averaged over hazards. Therefore, the effect of or variability in hazards cannot be analysed, with (other) predictors held constant, and the analysis may not predict risk perceptions for individual hazards. Moreover, there is an apparent lack of research showing how risk perceptions 'translate' into behaviour. The current research combines the study of expressed preferences and revealed preferences. This enables us to pursue our goals: to quantify variation among hazards, and to predict risk perception and precautionary behaviour. Risk perceptions and precautionary behaviour have also been the subject of existing research on privacy and security of social media.

3. Privacy and security of social media

3.1. Privacy and security are major issues in social media

First, it has been noted that security and privacy design of social media is weak (Acquisti & Gross, 2006), thereby creating security- and privacy vulnerabilities. Second, the main purpose of social media, information-sharing, inherently has implications for privacy: for example, whom to share information with, what to share and how much to share. Given these issues, users' behaviour and underlying risk perceptions becomes even more important to protect against security- and privacy hazards.

3.2. Online security in social networks

Saridakis, Benson, Ezingaard, and Tennakoon (2016) note an imbalance in behavioural research on online social networks, with many studies on privacy, but a dearth of research on security. They studied how social-network use and security perceptions are related to online victimisation. The results show that those with high perceived control over personal information on social networks, those with high perceived risk propensity on social networks and users of multi-purpose social networks are less likely to be cyber-crime victims, but users of knowledge exchange social networks are more likely to be victims.

3.3. Online privacy in social networks

Dienlin and Trepte (2015) distinguish informational, social and psychological privacy and study each of these privacy types empirically in Facebook. Based on the reasoned-action approach (Fishbein & Ajzen, 2011), privacy attitude, intention and behaviour were studied for each of the privacy types, but privacy concern was studied more generally, without reference to these types. The authors demonstrate that, for each of the three privacy types, privacy concerns were an indirect predictor of privacy behaviour, mediated by privacy attitude and privacy intention. Moreover, privacy attitude was an indirect predictor of privacy behaviour, mediated by privacy intention.

Taddicken (2014) studied willingness to self-disclose in social media rather than how people protect their information that they have already previously disclosed as personal content on an online social network. In disclosure, a distinction was made between sensitivity (facts versus sensitive) and access (open versus restricted). The findings show that privacy concerns are not a predictor of self-disclosure; perceived social relevance of online social networks are a predictor for self-disclosure of open facts and restricted sensitive information; and number of social networks used and general willingness to disclose are predictors of self-disclosure (except for self-disclosure of restricted facts).

Acquisti and Gross (2006) studied information-sharing by student-Facebook users. Various types of personal information were shared to a different extent (most users did not share cell-phone number, home-phone number, personal address, class schedule and partner's name; however, a majority did share birthday, political views and sexual orientation). There was little or no relation between participants' privacy attitudes and their information-sharing: students shared particular information, although they expressed concern about strangers identifying that information. As a potential explanation for this lack of correlation there was a lack of awareness in a significant minority regarding how to change their profile visibility in Facebook. Furthermore, a significant minority of users who had not changed the default...
دریافت فوری
متن کامل مقاله

امکان دانلود نسخه تمام متن مقالات انگلیسی
امکان دانلود نسخه ترجمه شده مقالات
پذیرش سفارش ترجمه تخصصی
امکان جستجو در آرشیو جامعی از صدها موضوع و هزاران مقاله
امکان دانلود رایگان ۲ صفحه اول هر مقاله
امکان پرداخت اینترنتی با کلیه کارت های عضو شتاب
دانلود فوری مقاله پس از پرداخت آنلاین
پشتیبانی کامل خرید با بهره مندی از سیستم هوشمند رهگیری سفارشات