Information disclosure of social media users: does control over personal information, user awareness and security notices matter?

Abstract

Purpose — Our study bridges the gap in the existing literature by exploring the antecedents of information disclosure of social media users. In particular, the paper investigates the link between information disclosure, control over personal information, user awareness and security notices in the social context, all of which are shown to be different from existing studies in e-commerce environments.

Design/methodology/approach — We collected and analysed data from 514 social network users. The model is estimated using OLS and robust standard errors are estimated using the Huber–White sandwich estimators.

Findings — Our results show that in social networking contexts, control over personal information is negatively and statistically associated with information disclosure. However, both user awareness and security notices have a positive statistical effect on information disclosure.

Originality/value — Whilst research on issues of individual information privacy in e-commerce is plentiful, the area of social networking and privacy protection remains under-explored. This paper provides a useful model for analysing information disclosure behaviour on social networks. We discuss the practical implications of our findings for actors in social media interactions.

Key Words: information disclosure, social networks, personal information privacy model, control over personal information, user awareness, security notices

Introduction

With the advent of social networking, individuals are seen voluntarily disclosing personal information in various forms. This raises important questions for individual privacy and civil liberties. These concerns are further exacerbated by the technological development of smart devices. In particular, the emergence of ubiquitous technologies including location services, (Ball, 2001; Clarke, 2001) adds to the need for further research into the issue of *information privacy*. Current information systems research flags up the mixed interpretations of information privacy as shown in various reviews of IS literature (e.g. Bélanger and Crossler, 2011; Conger *et al.*, 2013; Li, 2011; Smith *et al.*, 2011; Xu *et al.*, 2011a), especially where information security is concerned.

In a review of information privacy research, Bélanger and Crossler (2011) found that information security is strongly linked with information privacy. Dinev and Hart (2006) maintain that privacy and security are related concepts but differ in online business environments where security is required to build a sense of privacy in e-commerce transactions. It has been shown that personalisation and privacy are interlinked in e-commerce and mobile marketing, particularly in location-based services (Xu *et al*., 2011b). In information system research privacy has been linked to control over personal information (e.g. Culnan and Bies, 2003; Stewart and Segars, 2002). The notion of self-disclosure of personal information (e.g. Posey *et al*., 2010; Altschuller and Benbunan-Fich, 2013; Jaing *et al*., 2013) has been central to IS research into the treatment of privacy online. Both of these concepts have been studied extensively in online environments, especially in e-commerce. However, privacy and information disclosure have been shown to be dependent on the online context (Nguyen *et al*., 2012) and on individual (Xu *et al*, 2011a) and other factors, in the social media settings — all of which are yet to be fully understood in IS research. Pavlou (2011, p. 977) recommends that information privacy should be studied as a multilevel concept as there are 'promising research directions for advancing information systems research on information privacy'.

In recent years, some academics have argued that in a networked world, information privacy is no longer under the control of individuals but rests with the organisations that hold the information (Conger *et al*., 2013). Therefore, in their view, information privacy 'relates to information an individual wishes to keep private but not to how that information is managed' (Conger *et al*., 2013, p. 401). However, other researchers have argued that information privacy protection should be extended to include secondary use, access, control, notice and so

on (Smith *et al*., 2011; Xu *et al*., 2008; Bélanger *et al*., 2002). This places emphasis on privacy as a multi-dimensional concept involving many parties (the individual who provides information and the parties that collect the information, such as vendors, data-sharing partners or illegal entities — see Dhillon and Backhouse, 2001; Conger *et al*., 2013), and also highlights the importance of different degrees of management and control over personal data. Particularly for emerging technologies, such as social media, it is necessary to refocus the research lens beyond the scope of individual information management (Wright *et al*., 2008). In addition to extending privacy research beyond the individual level of analysis, the contextual nature of privacy needs refining. As argued by Smith *et al*. (2011), the meaning of privacy may vary according to the context in which it is studied or observed. For example, privacy problems associated with information stored on GPS-enabled devices may disclose vast amounts of personal information when coupled with information collected via social media technologies. This demonstrates that emerging technologies such as GPS, RFID and so on are not merely artefacts (Naisbitt *et al*., 2001) but tools that may have negative outcomes in the event of a breach of personal information privacy (Ball, 2001; Clarke, 2001; Smith *et al*., 2011).

Social media are popular not only as spaces for social interaction, but also as platforms for business transactions, thus giving rise to a new form of business model. This provides new meaning to the characteristics of information available in networked environments, their diversity and purpose of use. Aggregated, such information can be used in ways that may result in previously unforeseen consequences for information privacy. For example, in the emerging social technology environments, data aggregation can lead to customer profiling and targeted communication that may affect individual privacy (Young and Quan-Haase, 2013). The challenges to information privacy that result from surfing the personal information handled through social media are significant. This article aims to address the emerging challenges around information privacy in social media. It is organised as follows. Through a review of literature, we first discuss the various actors involved in information sharing transactions on social media. Second, we discuss information privacy in the context of social media and identify privacy indicators and consequences of information disclosure behaviour. Based on the literature review, we then propose a research model of the antecedents of information disclosure which addresses several existing gaps in the literature. The research model is then tested using empirical data from active social media users. The

article concludes with a discussion of the research findings and their implications for practice and future research directions.

Literature review

Actors and planned behaviour in social networks

Legacy views of web-based transactions have traditionally considered consumers and business organisations as transacting parties. Issues of privacy in 'traditional' e-commerce have been explored at length in the information system and marketing literature. Often an important component in such studies is the dimension of trust between the vendor and the buyer (Liu *et al*., 2005; Anderson and Agarwal, 2010). Some research shows that online self-disclosure may be influenced by the trust placed in the vendor or the service provider (Li, 2011), whilst other studies highlight that trust is dependent on the level of personalisation afforded by the e-commerce site (Xu *et al*., 2011b). However, this dichotomous view of the firm-user transactions towards trust is far from being representative of the complexity of online social networking interactions. In sociology and in social network analysis, individuals, groups and organisations are viewed as *actors* that make up the complex structure of a social network (Peters *et al*., 2013). Individual actors may include customers, retailers and suppliers (Rapp *et al*., 2013). Some sources regard computerised systems as actors in online transaction *ecosystems* (Zeng and Lusch, 2013). With the evolution of the online data collection capacity of organisations, other parties have been identified as actors in the social web. According to Conger *et al*. (2013), in the personal information privacy (PIP) model, which shows actors involved in data sharing and collection, consumers or individual users have been categorised as *first parties*. Vendors or providers of products and services are viewed as *second parties* who further transact with the *third party* — legal partners in data sharing. Data disclosure transactions of the vendor/provider with third parties have been identified as little understood by current privacy policy and research (Wright *et al*., 2008). Finally, as data theft and losses spiral on a global scale, the PIP model introduces a *fourth party* of malicious entities. By means of hacking, collusion, theft and other forms of cybercrime or hacktivism (Conger *et al*., 2013), these fourth parties illegally access, repurpose and steal data accumulated by vendors/providers (second parties in the model).

Social networks represent the digital equivalent of a network of actors communicating with each other using digital media (Picard, 2013). However, these differ from other online media and e-commerce transactions. When compared to other online media, as shown by Xu *et al.*

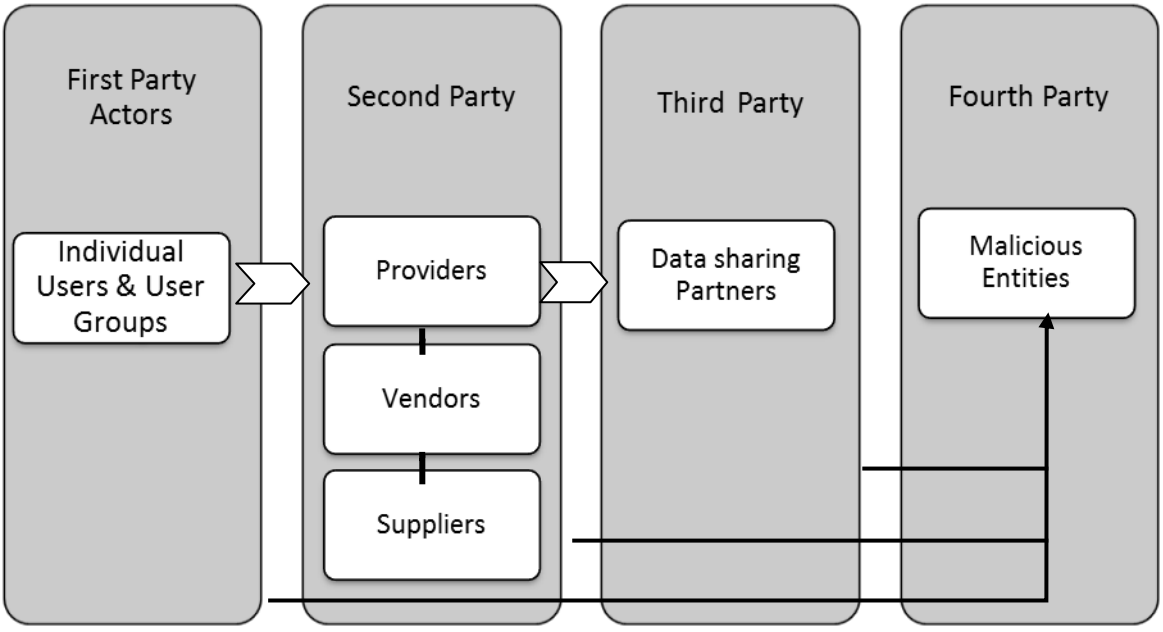
(2008), privacy issues on social networking sites gain an extra level of complexity. Compared to e-commerce, financial and healthcare sites social networking users had an inexplicably higher perception of control of personal information than in any other context (Xu *et al.,* 2008). Picard (2013, p. 836) states that the norms of the digital networks 'are based on amorphous arrangements, revelations and transparency, sharing, empowerment, collaboration, and informality'. The informal norms influenced by peer-to-peer interactions create a false sense of safety or control among social users. The study by Xu *et al*. (2008) also shows that the role of the service provider in the e-commerce context is perceived differently by their users in comparison to social media. For example, security measures in e-commerce sites are expected by their users and leads to a lower perception of privacy risk. The situation reverses in social media settings, which highlights the role of social networking providers in the assurance of safe personal information handling.

Personal information handling can be further explained by the extent of self-disclosure through social networking services (SNS). Posey *et al*. (2010) found that social influence and online trust increased online self-disclosure whilst privacy risk belief decreased self-disclosure. Others have argued that self-disclosure is more prominent in online settings where it is possible to remain anonymous (Altschuller and Benbunan-Fich, 2013), use misrepresentation (Jaing *et al*., 2013) and, thereby, feel less vulnerable (Joinson, 2001). Research studies on social networks have identified that user perceptions of self-anonymity lowers individuals' privacy concerns which, in turn, affects self-disclosure (Jaing *et al.,* 2013). In a comparative analysis of online and off-line self-disclosure literature, it was found that the degree of disclosure varies based on 'the relationship between the communicators, the specific mode of communication, and the context of the interaction' (Nguyen *et al*., 2012, p. 103). The frequency of SNS use is also found to have an impact on self-disclosure. In a longitudinal study by Trepte and Reinecke (2013), it was revealed that higher SNS use led to more self-disclosure.

The greatest controversy in the press and in academic literature has been about vendors/providers collection of the data of individual users'. Particularly ardent issues include using social networks for data harvesting in customer relationship management (Malthouse *et al*., 2013), ubiquitous surveillance (Ball, 2001) and the use of facial-recognition technologies to track the presence of customers at restaurants, cafes and other public places (Andrade *et al*., 2013); all of which are viewed as undesirable information disclosure transactions. Further actual behaviour, honesty and accuracy of disclosed information by individuals have been

studies in depth by (Keith *et al*., 2013). Social networking users were found to show no intention to disclose personal information, yet to gain benefits they tend to do the opposite. Researchers found that their only defence against second party data collectors is to divulge data which may be accurate. Furthermore, when using social networks, privacy concerns for other users (e.g. colleagues, friends and family members) present themselves as an extra personal information privacy dimension which has not previously been seen or studied in e-commerce. Recent studies have explored the factors that influence users to reveal their personal information to other users, that is, self-disclosure (Jiang *et al.*, 2013; Lowry *et al.*, 2011). Whilst overall, self-disclosure is seen as positive and beneficial in interpersonal communication and relationships (Lowry *et al.*, 2011: 163), research shows that interpersonal privacy on social networks could influence self-disclosure and threaten personal information privacy. We, therefore, extend the personal information privacy (PIP) model to include other parties in social media information sharing transactions (as shown in Figure 1). These parties include individuals/consumers and their interpersonal groups or networks, vendors/suppliers and providers, third party organisations with whom second party organisations share post-transactional data and, finally, malicious actors, that range from individual criminals to hostile governments.

Figure 1. Expanded model of transaction actors on social networks.



The extended model shows that privacy in social media may be viewed in terms of institutional privacy (Gürses and Diaz, 2013). Institutional privacy is 'related to users losing control and oversight over the collection and processing of their information' (Gürses and Diaz, 2013, p. 30). For individual users and groups, this entails handing control of their personal data, self-generated content, and multimedia to the social networking provider. On social networks in the event of a cyber-attack second and third party organisations lose control of data to the malicious fourth party, as shown in the extended transaction actor model (see Figure 1). Xu *et al*. (2011b) argue that there is an association between institutional privacy, individual privacy and the institutional privacy assurances. For example institutional privacy assurances, such as policies, can reduce individual privacy concerns.

TPB and TRA: the answer to understanding privacy?

Consumer behaviour, particularly antecedents of privacy and trust, has been considered though the lens of the theory of planned behaviour (TPB). TPB is an extension of the theory of reasoned action (TRA), as developed by Fishbein and Ajzen (1975), which argues that there is often a second stage appraisal of behavioural intentions. The use of TPB to examine online purchase behaviours (and sometimes information-seeking behaviours) is important. As argued by Pavlou and Fygenson (2006), other theoretical lenses such as TRA or the technology acceptance model, do not account for the 'impersonal nature of the online environment, the extensive use of IT, and the uncertainty of the open internet infrastructure' (p. 423). These characteristics of online environments play an important role in the decision-making process of online consumers (Hansen *et al*., 2004). Literature which relies on TPB demonstrates a chain association of privacy, trust and behaviour (George, 2004; Liu *et al*., 2005; Pavlou and Fygenson, 2006).

Current conceptualisations of social media transactions have two important premises. Firstly, privacy in social media is not necessarily an individual issue but extends to organisational and institutional actors involved in data sharing. Secondly, the volume and ease of accumulation of information through social networks is responsible for triggering adverse consequences to benign actors interacting on social platforms. In this article, our focus is on *individual actors* and the *consequences of information disclosure* behaviour and information privacy loss as a result of engaging with the emerging technologies, such as *online social networking.* Existing literature provides five variables of privacy including 'perceived ability to control submitted information', 'use of information', 'notice', 'perceived privacy' and

'privacy protection behaviour'. Information disclosure serves as a consequence of users' behavioural intention in the online transaction ecosystems. In the following section, we further discuss this variable and its antecedents.

Hypotheses development

Personal information, its disclosure and use, has attracted attention from a wide range of researchers and has raised the issue of privacy as a multi-faceted concept (e.g. Malhotra *et al.*, 2004; Smith *et al*., 2011; Stewart and Segars, 2002). The privacy concerns identified in these studies have been empirically validated and used to measure the perception of privacy. In line with these findings, behavioural models now include the construct of privacy concerns (Chellappa and Sin, 2005; Dinev and Hart, 2006). As shown by Xu *et al.* (2008) there are a variety of conceptualisations of privacy, but in information systems research privacy is associated with control over personal information (Culnan and Bies, 2003; Xu *et al.*, 2008; Stewart and Segars, 2002).

Perceived ability to control submitted information

Control over personal information has been viewed as a 'necessary tool for consumer privacy management' and is also referred to in the literature as 'choice' or 'consent' (Acquisti *et al*., 2013, p. 72). Malhotra *et al.* (2004) explored the multidimensional concept of Internet Users Information Privacy Concerns (IUIPC) and emphasised the role of control over personal information, awareness of privacy practices of companies gathering information and personal attitudes towards individual privacy. Brandimarte *et al*. (2013) maintain that privacy control presents a paradox, that is, 'the dichotomy between individuals' intentions to disclose private information and their actual behaviors' (p. 6). According to previous studies, information disclosure increases when people perceive they have more control over information (Keith *et al*., 2013; Knijnenburg *et al*., 2013; Hong and Thong, 2013). Moor (1997) and Tavani (2000) point out that privacy is best understood by assessing the amount of control users have over personal information. Most commercial websites offer users some control over information by giving them the option to opt-out (Chakraborty *et al*., 2013; Jai *et al*., 2013; Chadwick, 2001) of certain actions (e.g. sharing customer contact information with third parties). The social media activity of individuals results in unprecedented levels of information disclosure. Individuals, however, have little say in the control over personal information aggregation. Moreover, the richness of media on social networks is often perceived as social value or reward by their users. This may lead to individuals behaving in discord with their privacy

concerns (Jaing *et al*., 2013). Social data aggregation is used in customer profiling and targeted communication which, in turn, threatens individual privacy (Young and Quan-Haase, 2013) and leads to loss of control over personal information. Having a 'choice' of whether or not to disclose personal information, influences individual behaviour in e-commerce settings (Acquisti *et al*., 2013). In social networks, self-disclosure is seen as a privacy trade-off when users attach (or perceive) a value or reward for disclosing personal information and act contrarily to privacy protection behaviour (Jaing *et al.*, 2013). We propose to look at the connection between control and disclosure of personal information on social networks using the following hypothesis:

H1: Higher control over personal information by users reduces personal information disclosure on social media.

Use of information

Once customers disclose personal information and lose control over it, it is natural for them to feel concerned about what the vendor will do with their information. Referring to the social media transaction parties categories (see Figure 1), the concern of individual users (first party) is well substantiated. Second parties in social transactions gather and disseminate information to third parties. At this point in the personal information privacy model (Conger *et al*., 2013), individuals lose, or exercise much less control over their information; whereas, malicious fourth party entities threaten the information integrity of all parties involved in the social transaction ecosystem. When information gathered for transaction purposes is used without customers' consent for anything other than the original purpose, it is considered a breach of privacy (Brandimarte *et al*., 2013; Wang *et al*., 2013; Liu *et al*., 2005; Sheehan and Hoy, 2000; Malhotra *et al*., 2004). Policies regarding the use of information collected on social networking sites vary considerably across sites (Gross and Acquisti, 2005). Hoffman *et al*. (1999, p. 82) argue that even a website with the best opt-out policies can still freely use customer information 'in any (presumably legal) way it sees fit' without the informed consent of customers. Sheehan and Hoy (2000) and Milne (2000) found that customers who have concerns about the way in which websites use their information (e.g. whether it will be shared with third parties) are less likely to disclose information. However, less is known about disclosure and the role of user awareness of information use on social networks, particularly when there is strong criticism regarding the use of individual data by social

media sites for surveillance, targeted advertising, profiling and so on (Barnes, 2006; Zheleva and Getoor, 2009). Hence, the following hypothesis is proposed:

H2: When social media users have better knowledge about the use of personal information, they are more likely to disclose personal information.

Notices

In an attempt to reassure users that their personal information is safe online, businesses have begun to rely on self-regulatory transparency mechanisms (Acquisti *et al*., 2013). These techniques are generally referred to as giving *notice* or *notifications* and include privacy statements and privacy seals. Notices, such as privacy policies on a website, inform customers in advance about how their information will be gathered, handled, stored, and so on (Liu *et al*., 2005). Privacy seals (e.g. TRUSTe™, VeriSign™ Trusted sign), on the other hand, act as 'contextual cues' that can give 'rise to different levels of disclosure' (John *et al*., 2011, p. 858). Previous research has found that privacy seals can increase willingness to disclose personal information (Hui *et al*., 2007; Hu *et al*., 2010). A detailed review of privacy seals in e-commerce has been conducted by Moores and Dhillon, 2003. They drew a parallel between traditional and e-commerce business transactions and identified a significant gap in trust amongst customers when they were required to disclose personal information online. The authors state that, 'This trust gap centers primarily on the privacy of personally identifiable information, such as name, address, and so forth, that is an essential element of B2C transactions' (Moores and Dhillon, 2003, p. 1). Social media users also disclose personally identifiable information through networks (Light and MacGrath, 2010). Privacy notices on social networking sites may have a similar impact on information disclosure as they have in e-commerce. H3 is proposed to test this claim:

H3: The presence of privacy notices on a social networking site increases the likelihood of information disclosure.

Data collection and measures

The research population for this study consisted of active online social media users. Purposeful (non-probability) sampling or volunteer panels of online users were recruited. A web-based questionnaire was developed using Qualtrics software, and, to increase the

representativeness of our sample these were administered to the target sample through social media postings (e.g. on popular SNS such as Facebook™, LinkedIn™, Twitter™, and so on) and through personal contacts (see Bhutta, 2012). The survey was either only accessible to members of a particular group (e.g. LinkedIn specialised groups, such as specialist cybercrime forensics groups, academics with profiles on Method Space) or posted on personal websites that can only be accessed by contacts of the site owner (e.g. the researcher's Facebook, LinkedIn and Twitter pages; The Web Experiment List). In the survey invitation, a criterion was imposed to eliminate any non-social media users who might come across the survey, thus, by-passing restrictions. The criterion specified that only those using social media sites were eligible to take part in the survey. Further filtering was conducted by analysing responses to questions in the first section of the questionnaire (e.g. which SNS are the respondents currently using, and how often do they use them). Our sample consists of 514 individuals, which is in line with the sample size recommended by Krejcie and Morgan (1970) and Isaac and Michael (1981).

To capture *information disclosure (idi$_i$)* the survey asked respondents to rate whether they were concerned/bothered — on a scale that ranged from (1) strongly disagree to (7) strongly agree — when online companies asked for personal or financial information and about the frequency and quantity of the information requested (mean = 5.635; Cronbach's alpha = 0.892). The variable, *perceived control over personal information (cpi$_i$)*, was measured using four items: capturing ability to control access, and information released, used and provided. The responses varied from strongly disagree (1) to strongly agree (7) (mean = 3.318; Cronbach's alpha = 0.893).[1] The variable *use of information* (*uin$_i$*) was measured through a seven-point scale (1 = strongly disagree, 7 = strongly agree) using four items which asked respondents if online companies should never use personal information for any purpose, or for any purpose other than the one specified, or never exchange or share information with other companies (mean = 6.344; Cronbach's alpha = 0.901).[2] Using a seven-point scale (1 = strongly disagree; 7 = strongly agree), the survey asked respondents whether they considered security features, third party privacy seals, the content of privacy statements and third party security seals important in their decision to buy items online. The online security notices

[1] Since our study is cross-sectional, changes in perceptions over time cannot be observed. For example, perceptions may change if an individual experiences victimisation. However, this issue goes beyond the scope of this paper.

[2] A variable was also created by combining responses into a dichotomous variable taking the value of one for those who scored 6 or 7 on this question (82.49%) and zero (reference category) otherwise (17.51%). The results from this exercise show that the coefficient of the dummy variable is positive and statistically significant and robust across different specifications (results are available upon request).

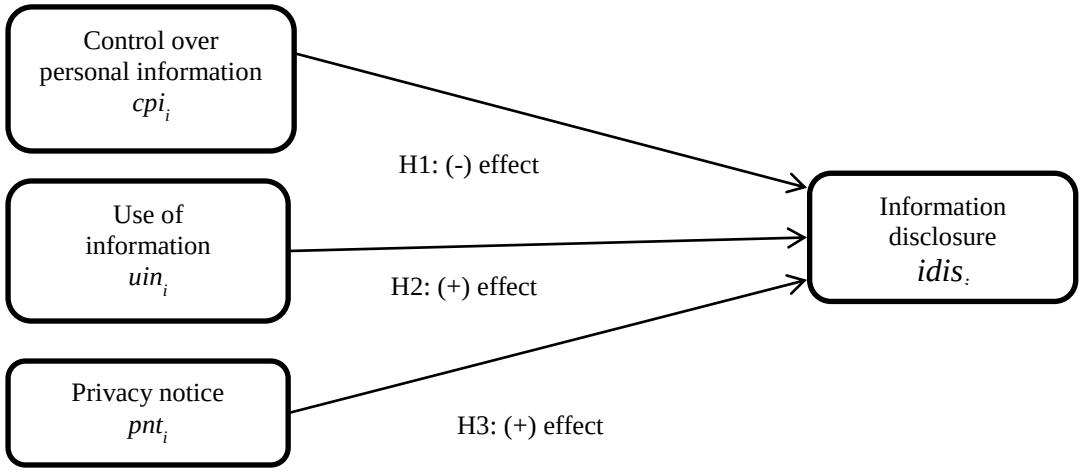
(pnt_i) variable was constructed from these four items where a seven-point index was constructed (mean = 5.347; Cronbach's alpha = 0.852).

The scale items used in this paper are based on existing sources, and Table A1 in the Appendix provides further information about the constructs. Before proceeding to our empirical model, we also tested for collinearity among the variables using the Variance Inflation Factor (VIF) method. The VIFs were found to have low values (mean VIF=1.22) suggesting that multicollinearity is not a problem here.[3] The empirical model is set out in equation (1) below, and Figure 2 presents the empirical model and associations.

$$idis_i = b_0 + b_1 cpi_i + b_2 uin_i + b_3 pnt_i + e_i \quad (1)$$

In order to estimate the size of the coefficients we estimate equation (1) using ordinary least squares (OLS). We estimated standard errors using the Huber–White sandwich estimators to account for potential concerns regarding heterogeneity and non-normality. For a robustness check, we also conceptualized our model as an ordered probit regression with seven ordered categories (see Wooldridge, 2002) and additionally estimated the model using an interval regression model assuming that each observation represents interval data (see Cameron and Trivedi, 2009).

Figure 2. Information disclosure and expected associations with explanatory variables.



[3] The correlations among the three antecedents of self-disclosure are also found not to be strong: $r_{cpi,uin}$=-0.024 , $r_{cpi,\ pnt}$= 0.141and $r_{uin,pnt}$=0.453. A moderate correlation between usage information and privacy notice can be explained, for example, as due to potential knowledge that the SN users gain if they read the security notices provided by the website. However, the correlation test is ineffective for detecting multicollinearity (see Kumar, 1975).

Empirical findings

Data analysis yielded some important results, which are presented in Table 1. The results show that perceptions of exercising control over personal information have a negative and statistical effect on information disclosure. Hence, this finding supports Hypothesis 1. Social media activity results in the generation of vast amounts of information which may be commercially sensitive or considered private. Current studies (Bertot *et al*., 2010; Bertot *et al*., 2012) show a general lack of awareness from social networking users regarding the way in which their information and user-generated content is used by the social networking sites and third parties, including government. In light of these conclusions, the findings of our study are highly significant. When social media users feel assured that they have more control over their personal information, they are more careful about disclosing information about themselves.

We also found a statistical but positive association between user awareness and information disclosure, thus, supporting Hypothesis 2. Consumers have been shown to trust social media; resulting in vast quantities of self-disclosed information (Elmi *et al*., 2012). Trust has been linked to a higher predisposition towards information disclosure and is relevant in the context of social media. As social technology matures, its high quality and ease of use (Young and Quan-Haase, 2013), have manifested themselves in elevated levels of trust. Trust between network members, however, encourages users to disclose personal information and impacts on personal information privacy. The outcomes of this study demonstrate that when social media users have better knowledge about the use of personal information, they are more inclined to disclose their personal information. This outcome has significant implications for user awareness programmes. Online social networking providers (second parties), should be more transparent about how individual user information is collected and passed on to third parties and how its integrity is protected from fourth parties in the social transaction ecosystem.

Table 1. Results for information disclosure model and robustness check.

Model:	OLS		OLS		Ordered probit		Interval regression	
$idis_i$	Coef.	Robust Std. Err.	Coef.	Robust Std. Err.	Coef.	Robust Std. Err.	Coef.	Robust Std. Err.
cpi_i	-0.211*	0.044	-0.172*	0.048	-0.149*	0.038	-0.269*	0.071
uin_i	0.251*	0.068	0.256*	0.067	0.201*	0.051	0.322*	0.089
pnt_i	0.101**	0.047	0.106**	0.047	0.091**	0.038	0.167**	0.069
Intercept	4.202*	0.476	3.587*	0.715			4.696*	0.981
Controls	*No*		*Yes*		*Yes*		*Yes*	
F(3, 510)	18.19*							
F(19, 494)			6.14*					
Wald Chi2(19)					89.14*		94.86*	
Observations	514		514		514		514	
R-squared	0.126		0.1704					
Log likelihood					-744.052		-833.127	

Controls include variables such as age, gender, qualifications and occupational status. We found, however, that these variables have an insignificant individual effect (with the exception of age which was found to be statistically significant at the 5% level) but jointly, they are statistically significant in the models using the F-test and Wald-test, and improve the general performance of the models (full results are available upon request).
*Significant at 1% level. **Significant at 5% level

Finally, our results show a positive and statistical association between security notices and information disclosure. Our results prove that when social media users perceive that a social networking service provides security notices, they are more likely to trust the service and benevolently share their information with the site. This finding has several implications. Firstly, it indicates that social media users deem security notices to be important attributes of an online service and feel more comfortable transacting with a provider that offers a seal of approval or informs users of the implications of their actions through appropriate notices.

Therefore, notices become a more important tool for social user awareness than in traditional e-commerce. Secondly, the trust social media users show towards sites providing security notices can be easily undermined by false or exaggerated claims by social networking services. Hence, whilst users may be notified of the implications of using a social media site through notices, the provider may not take the necessary steps to safeguard personal information privacy. In this case, notices may serve as a false incentive to lead users into information disclosure in circumstances where information safety cannot be guaranteed.

Conclusions

Previous studies have identified that social networking environments differ from e-commerce and other online environments, such as e-healthcare, multimedia or financial sites (e.g. Bélanger *et al*., 2002; Xu, *et al.*, 2008; John *et al*., 2011), in terms of information disclosure and user behaviour. Social networking is an interesting but complex context in which service providers, users, and other third parties engage in information disclosure and can potentially serve as information privacy violators. It has been shown that users perceive measures against information disclosure to either benign or malicious entities differently in social networks. Our study built upon the calls for further research on information disclosure behaviour and privacy in social networks and the research agenda set by Xu, *et al*., 2011a, Smith et *al*., 2011 and Conger *et al.*, 2013. The paper has investigated the link between information disclosure and three important aspects: control over personal information, user awareness, and security notices.

We found a negative association between information disclosure and perceived control over personal information, but a positive association was found with user awareness and security notices. Our study carries a number of highly important implications for practice. As the number of registered users and the proportion of time spent by people using social media continues to increase year on year, the commercial value of personal information and commercial opportunities on social networks continues to rise. The main contribution of this research is in bridging the gap in current literature by exploring the link between user behaviour on social media and personal information disclosure, which makes users vulnerable to the loss of personal information privacy. This further contributes to current theoretical perspectives on information security in IS literature which explore antecedents or consequences of various aspects of user personal information disclosure when applied to social media. The findings of this study will help inform the development of social media user awareness practices and the enhancement of security mechanisms implemented on social networking platforms. Further, the results are important to future researchers and scholars who may wish to test similar relationships in different contexts.

References

Acquisti, A., Adjerid, I. and Brandimarte, L. (2013), "Gone in 15 seconds: the limits of privacy transparency and control", *IEEE Security and Privacy*, Vol. 11 No. 4, pp. 72–74.

Altschuller, S. and Benbunan-Fich, R. (2013), "The pursuit of trust in ad hoc virtual teams: how much electronic portrayal is too much", *European Journal of Information Systems*, Vol. *22* No. 6, pp. 619–636. doi: 10.1057/ejis.2012.39.

Anderson, C.L. and Agarwal, R. (2010), "Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions", *MIS Quarterly*, Vol. 34 No. 3, pp. 613–643.

Andrade, N., Martin, A. and Monteleone, S. (2013), "All the better to see you with, my dear: facial recognition and privacy in online social networks", *IEEE Security and Privacy*, Vol. 11 No. 3, pp. 21–28.

Ball, K. (2001), "Surveillance society: monitoring everyday life", *Information Technology & People*, Vol. 14 No. 4, pp. 406–419.

Barnes, S.B. (2006), "A privacy paradox: social networking in the United States", *First Monday*, Vol. 11 No. 9. Available at: http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/arti- cle/view/1394/1312 [Accessed on 08/01/2015]

Bélanger, F., Hiller, J.S. and Smith, W.J. (2002), "Trustworthiness in electronic commerce: the role of privacy, security, and site attributes", *Journal of Strategic Information Systems*, Vol. 11 No. 3, pp. 245–270.

Bélanger, F. and Crossler, R.E. (2011), "Privacy In the digital age: a review of information privacy research in information systems", *MIS Quarterly*, Vol. 35 No. 4, pp. 1017-141.

Bertot, J.C., Jaeger, P.T. and Grimes, J.M. (2010), "Using ICTs to create a culture of transparency: e-government and social media as openness and anti-corruption tools for societies", *Government Information Quarterly*, Vol. 27 No. 3, pp. 264–271.

Bertot, J.C., Jaeger, P.T. and Hansen, D. (2012), "The impact of polices on government social media use: issues, challenges, and recommendations", *Government Information Quarterly*, Vol. 29 No. 1, pp 30–40.

Bhutta, C.B. (2012), "Not by the book: Facebook as a sampling frame", *Sociological Methods and Research*, Vol. 20 No. 10, pp. 1–32.

Brandimarte, L., Acquisti, A. and Loewenstein, G. (2013), "Misplaced confidences privacy and the control paradox", *Social Psychological and Personality Science*, Vol. 4 No. 3, pp. 340–347.

Cameron, A.C. and Trivedi, P. K. (2009), *Microeconometrics Using Stata*, Stata Press, College Station, TX.

Chadwick, S. A. (2001), "Communicating trust in e-commerce interactions", *MIS Quarterly*, Vol. 14 No. 4, pp. 653–658.

Chakraborty, R., Vishik, C. and Rao, H.R. (2013), "Privacy preserving actions of older adults on social media: exploring the behaviour of opting out of information sharing", *Decision Support Systems*, Vol. 55 No. 4, pp. 948–956.

Chellappa, R.K. and Sin, R. (2005), "Personalization versus privacy: an empirical examination of the online consumer's dilemma", *Information Technology and Management*, Vol. 6 No.2, pp. 181–202.

Clarke, R. (2001), "Person location and person tracking — Technologies, risks and policy implications", *Information Technology & People*, Vol. 14 No. 2, pp. 206–231.

Conger, S., Pratt, J.H. and Loch, K.D. (2013), "Personal information privacy and emerging technologies", *Information Systems Journal*, Vol. 23 No. 5, pp. 401–417.

Culnan, M.J. and Bies, J.R. (2003), "Consumer privacy: balancing economic and justice considerations", *Journal of Social Issues*, Vol. 59 No.2, pp. 323–342.

Dhillon, G. and Backhouse, J. (2001), "Current directions in IS security research: towards socio-organizational perspectives", *Information Systems Journal*, Vol. 11 No 2, pp. 127–153.

Dinev, T. and Hart, P. (2006). "An extended privacy calculus model for e-commerce transactions". *Information Systems Research*, Vol. 17 No.1, pp. 61-80.

Elmi, A. H., Iahad, N. and Abdirahman A. (2012) "Factors Influence Self-Disclosure Amount in Social Networking Sites (SNSs)." Available at: http://seminar.spaceutm.edu.my/jisri/download/F_FinalPublished/Pub6_Factors_Self-Disclosure_inSNSs_amenfd.pdf [Accessed on 08/01/2015]

Fishbein, M. and Ajzen, I. (1975), *Belief, Attitude, Intention, and Behavior: An introduction to theory and research*, Addison-Wesley, Reading, MA.

George, J.F. (2004), "The theory of planned behavior and internet purchasing", *Internet research*, Vol. 14 No. 3, pp. 198–212.

Gross, R. and Acquisti, A. (2005), "Information revelation and privacy in online social networks", in *Proceedings of the 2005 ACM workshop on Privacy in the electronic society*, pp. 71–80.

Gürses, S. and Diaz, C. (2013), "Two tales of privacy in online social networks", IEEE *Security and Privacy*, Vol.11 No. 3, pp. 29–37.

Hansen, T., Jensen, J.M. and Solgaard, H.S. (2004), "Predicting online grocery buying intention: a comparison of the theory of reasoned action and the theory of planned behavior", *International Journal of Information Management*, Vol. 24 No. 6, pp. 539–550.

Hoffman, D.L., Novak, T.P. and Peralta, M. (1999), "Building consumer trust online", *Communications of the ACM*, Vol. 42 No. 4, pp. 80–85.

Hong, W. and Thong, J.Y. (2013), "Internet privacy concerns: an integrated conceptualization and four empirical studies", *MIS Quarterly*, Vol. 37 No.1, pp. 275–298.

Hu, X., Wu, G., Wu, Y. and Zhang, H. (2010), "The effects of Web assurance seals on consumers' initial trust in an online vendor: a functional perspective", *Decision Support Systems*, Vol. 48 No. 2, pp. 407–418.

Hui, K.L., Teo, H.H. and Lee, S.Y.T. (2007), "The value of privacy assurance: an exploratory field experiment", *MIS Quarterly*, Vol. 31 No. 1, pp. 19–33.

Isaac, S. and Michael, W.B. (1981), "*Handbook in Research and Evaluation"*, EdITSPublishers, San Diego, CA.

Jai, T.M.C., Burns, L.D. and King, N.J. (2013), "The effect of behavioural tracking practices on consumers' shopping evaluations and repurchase intention toward trusted online retailers", *Computers in Human Behaviour*, Vol. 29 No. 3, pp. 901–909.

Jaing, Z.J., Heng, C. S. and Choi B.C. (2013), "Research note-privacy concerns and privacy-protective behavior in synchronous online social interactions", *Information Systems Research*, Vol. 24 No. 3, pp. 579–595.

John, L.K., Acquisti, A. and Loewenstein, G. (2011), "Strangers on a plane: context-dependent willingness to divulge sensitive information", *Journal of Consumer Research*, Vol. 37 No. 5, pp. 858–873.

Joinson, A.N. (2001) "Self-disclosure in computer-mediated communication: the role of self-awareness and visual anonymity", *European Journal of Social Psychology*, Vol. 31 No. 2, pp. 177–192.

Keith, M., Thompson, S. Hale, J., Lowry, P.B. and Greer, C. (2013) "Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior". *International Journal of Human-Computer Studies*. Vol.71, No. 12, pp. 1163–1173

Knijnenburg, B.P., Kobsa, A. and Jin, H. (2013), "Dimensionality of information disclosure behaviour", *International Journal of Human-Computer Studies*, Vol. 71 No. 12, pp. 1144–1162.

Krejcie, R.V. and Morgan, D.W. (1970), "Determining sample size for research activities", *Educational and Psychological Measurement*, Vol. 30, pp. 607–610.

Kumar, T. (1975), "Multicollinearity in regression analysis", *Review of Economic and Statistics*, Vol. 57 No. 3, pp. 365–366.

Li, Y. (2011), "Empirical studies on online information privacy concerns: literature review and an integrative framework", *Communications of the Association for Information Systems*, Vol. 28 No. 1, pp. 453-496.

Light, B. and McGrath, K. (2010), "Ethics and social networking sites: a disclosive analysis of Facebook", *Information Technology & People*, Vol. 23 No. 4, pp. 290–311.

Liu, C., Marchewka, J.T., Lu, J. and Yu, C.S. (2005), "Beyond concern — a privacy- trust-behavioral intention model of electronic commerce", *Information and Management*, Vol. 42 No. 2, pp. 289–304.

Lowry, P.B., Cao, J. and Everard, A. (2011), "Privacy concerns versus desire for interpersonal awareness in driving the use of self-disclosure technologies: the case of instant messaging in two cultures", *Journal of Management Information Systems*, Vol. 27 No.4, pp. 163–200. doi: 10.2753/mis0742-1222270406.

Malhotra, N.K., Kim, S.S. and Agarwal, J. (2004), "Internet users' information privacy concerns (IUIPC): the construct, the scale, and a causal model", *Information Systems Research*, Vol. 15 No. 4, pp. 336–355.

Malthouse, E.C., Haenlein, M., Skiera, B., Wege, E. and Zhang, M. (2013), "Managing customer relationships in the social media era: introducing the social CRM house", *Journal of Interactive Marketing*, Vol. 27 No. 4, pp. 270–280.

Milne, G. R. (2000), "Privacy and ethical issues in database/interactive marketing and public policy: a research framework and overview of the special issue", *Journal of Public Policy and Marketing*, Vol. 19 No.1, pp. 1–6.

Moor, J.H. (1997), "Towards a theory of privacy in the information age", *Computers and Society*, Vol. 27 No.3, pp. 27–32.

Moores, T. and Dhillon. G. (2003), "Do privacy seals in e-commerce really work?", *Communications of ACM*, Vol. 46 No. 12, pp. 265–271.

Naisbitt, J., Philips, D. and Naisbitt, N. (2001), *HighTech/High Touch: Technology and Our Search for Meaning*, Nicholas Brealey Publishing, London, UK.

Nguyen, M., Bin, Y.S. and Campbell, A. (2012), "Comparing online and offline self-disclosure: a systematic review", *Cyberpsychology, Behavior, and Social Networking*, Vol.15 No. 2, pp. 103–111.

Pavlou, P.A. (2011), "State of the information privacy literature: where are we now and where should we go?", *MIS Quarterly*, Vol. 35 No. 4, pp. 977–988.

Pavlou, P.A. and Fygenson, M. (2006), "Understanding and predicting electronic commerce adoption: an extension of the theory of planned behavior", *MIS Quarterly*, Vol. 30 No. 1, pp. 115–143.

Peters, K., Chen, Y., Kaplan, A.M., Ognibeni, B. and Pauwels, K. (2013), "Social media metrics — a framework and guidelines for managing social media", *Journal of Interactive Marketing*, Vol. 27 No.4, pp. 281–298.

Picard, R.G. (2013), "What social media are doing and where they are taking us", in Mike, F. and Wolfgang, M-B. (Eds.), *Handbook of Social Media Management*, Springer, Berlin, Heidelberg, pp. 835–841.

Posey, C., Lowry, P.B., Roberts, T.L. and Ellis, T.S. (2010), "Proposing the online community self-disclosure model: the case of working professionals in France and the UK who use online communities", *European Journal of Information Systems*, Vol. 19 No. 2, pp. 181–195.

Rapp, A., Beitelspacher, L.S., Grewal, D. and Hughes, D.E. (2013), "Understanding social media effects across seller, retailer, and consumer interactions", *Journal of the Academy of Marketing Science*, Vol. 41 No. 5, pp. 1–20.

Sheehan, K.B. and Hoy, M.G. (2000), "Dimensions of privacy concern among online consumers", *Journal of Public Policy and Marketing*, Vol. 19 No. 1, pp. 62–73.

Smith, H., Dinev, T. and Xu, H. (2011), "Information privacy research: an interdisciplinary review", *MIS Quarterly*, Vol. 35 No. 4, pp. 989–1016.

Stewart, K.A. and Segars, A.H. (2002), "An empirical examination of the concern for information privacy instrument", *Information Systems Research*, Vol. 13 No.1, pp. 36–49.

Tavani, H.T. (2000), "Privacy and the internet", available at: http://www.bc.edu/bc_org/avp/law/st_org/iptf/commentary/content/2000041901.html [Accessed on 08/01/2015]

Trepte, S. and Reinecke, L. (2013), "The reciprocal effects of social network site use and the disposition for self-disclosure: a longitudinal study", *Computers in Human Behavior*, Vol. 29 No. 3, pp. 1102–1112.

Wang, N., Grossklags, J. and Xu, H. (2013), "An online experiment of privacy authorization dialogues for social applications", in *Proceedings of the 2013 Conference on Computer Supported Cooperative Work*, ACM, pp. 261-272.

Wooldridge, J.M. (2002), *Econometric Analysis of Cross Section and Panel Data*, MIT Press, Cambridge, MA.

Wright, D., Gutwirth, S., Friedewald, M. and Vildjiounaite, E. (2008), "*Safeguards in a World of Ambient Intelligence: The International Library of Ethics, Law, and Technology*", Springer, London, UK.

Xu, H. Dinev, T., Smith, H.J. and Hart, P. (2008), "Examining the formation of individual's privacy concerns: toward an integrative view", in *Proceedings of International Conference on Information Systems (ICIS)*, Paris, Paper 6.

Xu, H., Carroll, J.M. and Rosson, M.B. (2011a), "The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing", *Decision Support Systems*, Vol. 51 No. 1, pp. 42–52. doi: 10.1016/j.dss.2010.11.017

Xu, H., Dinev, T., Smith, J. and Hart, P. (2011b), "Information privacy concerns: linking individual perceptions with institutional privacy assurances", *Journal of the Association for Information Systems*, Vol.12 No. 12, pp. 798–824.

Young, A.L. and Quan-Haase, A. (2013), "Privacy protection strategies on Facebook: the internet privacy paradox revisited", *Information, Communication and Society*, Vol. 16 No. 4, pp. 479–500.

Zeng, D. and Lusch, R. (2013), "Big data analytics: perspective shifting from transactions to ecosystems", *IEEE Intelligent Systems*, Vol. 28 No. 2, pp. 2–5.

Zheleva, E. and Getoor, L. (2009), "To join or not to join: the illusion of privacy in social networks with mixed public and private user profiles", in *Proceedings of the 18th International Conference on World Wide Web*, April 20-24, Madrid, Spain, pp. 531–540.

Table A1: Summary of constructs

Construct	Measurement scale in *original* study	Original items	Modified items	Source
Perceived ability to control submitted information	"Strongly disagree" to "Strongly agree"	1. I believe I have control over who can get access to my personal information collected by these websites. 2. I think I have control over what personal information is released by these websites. 3. I believe I have control over how personal information is used by these websites. 4. I believe I can control my personal information provided to these websites.	1. I believe I have control over who can get access to my personal information collected by SNS. 2. I think I have control over what personal information is released by SNS. 3. I believe I have control over how personal information is used by SNS. 4. I believe I can control my personal information provided to SNS.	Xu *et al.*, 2008
Use of information	"Strongly disagree" to "Strongly agree"	1. Online companies should not use personal information for any purpose unless it has been authorized by the individual who provided the information. 2. When people give personal information to an online company for some reason, the online company should never use the information for any other reason. 3. Online companies should never sell the personal information in their computer databases to other companies. 4. Online companies should never share personal information with other companies unless it has been authorized by the individual who provided the information.	1. SNS should not use personal information for any purpose unless the individual who provided information has authorized it. 2. When people give personal information to a SNS for some reason, the online company should never use the information for any other reason. 3. SNS should never sell the personal information in their computer databases to other companies. 4. SNS should never share personal information with other companies unless the individual who provided the information has authorized it.	Malhotra *et al*., 2004
Notices	"Very important" to "Not Important"	1. How important are security features (e.g. SET, SSL, locks, etc.) in your decision to buy on the world wide web? 2. How important are third party privacy seals in your decision to buy on the world wide web? 3. How important is the content of the privacy policy statement in your decision to purchase on the world wide web? 4. How important are third party security seals in your decision to buy on the world wide web?	1. Security features (e.g. SSL, locks, HTTPS) are important in your decision to buy things online. 2. Third party privacy seals are important in your decision to buy things online. 3. The 'content' of privacy statement is important in your decision to buy things online. 4. Third party security seals are important in your decision to buy things online.	Bélanger et al., 2002