The Role of Security Notices and Online Consumer Behaviour: An Empirical Study of Social Networking Users

Abstract

This paper uses a survey of social networking users to empirically explore their perceptions of security notices - independently verified artefacts informing internet site users that security measures are taken by the site owner. We investigate such factors as purchase experience, purchase intention, risk propensity, usage of various social network categories and user victimisation. The results suggest a strong positive link between purchase intention and paying attention to security notices/features on social networks. We find that higher use of narrow-purpose social networking services has a negative association with paying attention to security notices. We also show that users with higher risk propensity pay less attention to security notices/features. Finally, we find no association between purchase experience, user victimisation and perception of security notices/features. Our results provide new, and possibly more refined, evidence of the factors that influence the attention paid to security notices/features by social media users. The results have important implications for theory development, policy and practice.

Keywords: *Social media, security notices, security seals, personal information privacy, information security, cybercrime victimisation, social learning.*

1. Introduction

The proliferation of social technologies has been seen as a positive shift in the way people communicate, collaborate, share knowledge (Susarla et al., 2013; Hsu et al., 2007), transact online and consume (Aral et al., 2013). Originating largely as a set of leisure applications for connecting with friends and family and as content sharing tools, social networks have naturally evolved into instruments for business, professional and commercial uses (Aral et al., 2013)[1]. The delineation between commercial and personal applications of social media is becoming more prominent as the social business models and revenue streams mature.[2] Social media has played a particularly key role in business transformation and has opened new avenues for revenue generation (Agarwal et al., 2008; Bharadwaj et al., 2013; Malthouse et al., 2013). However, Social media security breaches are continually reported in the press, raising concerns about the ability of social networking sites to sustain safe user information management and the provision of appropriate security measures[3]. The growing concern about information security on social networking platforms is hindering business organisations from gaining the full economic benefit of social technologies (Ellison, 2007; Lievrouw and Livingstone, 2002).

Since the early days of ecommerce, information security measures for online consumers have attracted significant research attention (Dhillon and Backhouse, 2001; Liu et al., 2005; Milne et al., 2004Von Solms, 2001). The area of internet information security is

[1] Wirtz et al. (2010) argue that the interaction on social networks is the driving force behind its increasing popularity as a business platform. Social networks evolved from being virtual spaces for socialising to instruments for businesses and customers to co-create and reinforce consumption via virtual word-of-mouth (Kozinets, 1999; Wirtz et al., 2010).

[2] In a study conducted in the US, it was found that Fortune 500 companies use popular social media platforms such as Facebook, Twitter etc. to interact with customers, where they could create virtual customer environments (VCEs) (Culnan et al., 2010). According to Mangold and Faulds (2009: 357), social media is the "new hybrid element of the promotion mix". Co-creation (Zwass, 2010), and word-of-mouth (Park et al., 2007; Cheung et al., 2009) are other applications of social media in commercial settings.

[3] Incidents such as the theft of 2 million passwords affecting Facebook, Google, Twitter, Yahoo, and LinkedIn accounts in December 2014 (Andrew, 2014), the Sony PlayStation information security breach (Minihane, 2011), and criticisms against Facebook apps tracking/selling personal information (Hickins, 2012) are just a the few of the social media security breaches reported in the media in recent years.

well developed and evolves continuously in response to new threats. A proven, successful online security measure was the development of third party security notices or artefacts, informing internet site users that measures are taken by the site owner and are independently verified. The effectiveness of online security notices has been studied for general web users and e-business users (Al-Dwairi, 2013; Belanger et al., 2002; Benassi, 1999; Kim et al., 2008). There is room for further research on the role of security notices in the context of social networking platforms and their perception by social network users. From extant literature, it emerges that the social technology and information security lags behind in the development of appropriate security notices for social media users (Lievrouw and Livingstone, 2002; Campbell et al., 2003; Cavusoglu et al., 2004; Ellison, 2007). This paper empirically examines the link between social media user experience (including past victimisation), attitude and intention and the likelihood of paying attention to security notices online. The paper provides further insights into the existing theory on security notices and informs policy and practice about the importance of security notices to social media users and the affecting factors.

Specifically, the contribution of this paper is threefold. First, we extend the existing literature, which mainly focuses on the role of security notices in e-commerce settings, by turning the research lens towards security notices/features in social media settings. Secondly, we collect rich and original data to allow empirical investigation of the nature and magnitude of the associations between purchase experience, purchase intention, propensity towards risks, usage of different categories of social networks, user victimisation and the attention paid to security notices. Protecting personal information security in social technologies has been a heated topic for the industry, and in policy debate. This paper sheds more light on the mechanisms and user behaviour traits which can help the social technology industry more effectively protect the personal information of their users and ease concerns over transition into the social commerce era.

The article is organised as follows: in Section 2, we review extant literature on the subject of online information security and security notices, setting forth the research hypotheses. We focus on the security notices, or the security visualisation techniques used on websites, such as security seals (e.g. sign-in seals, VeriSign, TRUSTe), notices (e.g. security policies) and other features (e.g. padlock icon, URL indication, SSL protection) in line with the definition by Dang and Dang (2013). We aim to address the following five important questions. First, does higher usage of social media increase the level of attention paid to security notices? Second, do users with previous purchase experience in a social context pay less attention to security notices/features? Third, does past security victimisation influence user attitudes towards security notices? Fourth, is there a link between security notices and user intention to make a purchase from a social media vendor? Finally, are individuals with high risk propensity less likely to pay attention to security notices? Research design and methodology are discussed in Section 3. Specifically the strategy for data collection from over 500 active social network users[4] is described. Section 4 presents the results and Section 5 discusses their implications for theory and practice. The conclusions of this paper, in Section 6, set an important agenda for social networks supporting business use and commercial transactions, and makes recommendations for the significance of social security notices.

2. Existing work and hypotheses development

2.1. Theoretical background

Study of the social media phenomenon has emerged from two dominant areas: while the new medium for content sharing and communication is mainly attributed to the area of

[4] The social network sites used by respondents included Facebook, Twitter, LinkedIn, YouTube, MySpace, Google+, Blogger, Skype, Flickr, and virtual worlds such as Second Life, and World of Warcraft.

communication science, social theory helps explain the social (networking) structures connected via dyadic ties and the behaviour of social actors - individual nodes, groups and networks (e.g. Wasserman and Faust, 1994). Online social networking characteristics are multi-directional, immediate and contingent, which make them different from traditional online and offline communication media (Alba et al., 1997). Peters et al. (2013, p.282) define Social Networking Services (SNS) as "communication systems that allow their social actors to communicate along dyadic ties", and emphasises the egalitarian nature of social networking; unlike the widely accepted hierarchal structures, nodes in social networks have equal weight in information communication and authority.

Attempts have been made to classify social networking services according to their purpose, structure, knowledge-sharing direction, and other characteristics. For example, Kaplan and Haenlein (2010) identify six categories of SNS: collective projects (e.g. Wikipedia); blogs and micro-blogging (e.g. Blogger, Twitter); content communities (e.g. Flickr, Youtube); social networking sites (e.g. Facebook, LinkedIn); multiplayer online role-playing games (e.g. World of War Craft) and finally, virtual social worlds (Second Life). This categorisation is rather one-dimensional and application-based, however, which changes with the evolution of capabilities offered by social media sites. It has been argued that the purpose-based classification approach fails to keep up with the pace of technology and constantly evolving features of social networking services. For example, the functionality of collective projects and content communities is expanding rapidly, and the purposes of the different service categories is starting to converge.

Researchers agree that social media is inherently different from other types of media (Hoffman and Novak, 2012; Rapp et al., 2013). Online social networks are self-developing, dynamic, interconnected and interactive; they are beyond the control of an organisation, with a specific set of metrics for analysis and idiosyncratic management principles. The distinct nature of social media presents a challenge for applying known metrics and values from the traditional online context. Consequently, a new set of principles is required to explain the behaviour of actors in social media, and new tools need to be developed by the parties involved in social transactions to communicate their message of privacy and safety to users.

Extensive studies of behavioural descriptive norms (Cialdini et al., 1990) help explain the behaviour of social actor, the acquisition of privacy safety norms and their dynamics in social networking communities as behaviour predictors. Kashimaa et al. (2013) emphasise the role of descriptive norms - what social media users do in particular settings in terms of their behaviour and decision-making online. Internet users can learn how to behave securely and identify artefacts, such as security notices, which reinforce their perceptions of personal information security measures. These conclusions are very important in the context of online purchase behaviour and social users' perceptions of personal information security. Specifically, social users acquire descriptive norms from others with whom they are connected via social networking ties. These norm acquisition behaviours are either experiential, (i.e. users observe what others do and learn or follow their behaviour, or consequently make decisions according to the norms existing in the social networking community), or conceptual. In the latter case, users learn from what their associates say people do (Kashimaa et al., 2013). This resonates with social learning theory on the role of environmental and cognitive factors in influencing human behaviour (Bandura, 1971, 1986). In a social networking context, stimulus response theories, and learning through direct experience take on a new meaning. Those users who experienced cyber victimisation will behave differently in social transactions to those who have not been subject to cybercrime. User behaviour, decision making and trust formation online has been given an original interpretation by Liu and Goodhue (2012). They suggest that trust in e-commerce transactions and consumer behaviour as cognitive misers are interrelated. Trust online, and types of trust online, have been extensively examined (e.g. Corritore et al., 2003) in e-commerce settings, with the conclusion that perception of credibility, ease of use and risk play a major role in trust formation online.

The literature dealing with security is largely based on studies that have been conducted in corporate environments, and highlights potential economic losses to organisations because of lack of security (Campbell et al., 2003; Cavusoglu et al., 2004; Rauch, 2001). Research at the individual level has more significance for practice, however, particularly at a time when social media enables data collection on a previously unimaginable scale, yielding both benefits and undesirable consequences for their users. Amongst such inadvertent outcomes of social networking use are online breaches of personal information security, which have been repeatedly reported in the press[4]. Personal and security sensitive information losses resulting from cybercrime, including online identity theft, financial fraud, and even blackmail, are on the rise (Gradon, 2013; Guitton, 2013). Chellappa and Pavlou (2002) maintain that such breaches of security influence the perceived security and trust of online customers, however, security protection mechanisms such as encryption, authentication and visual notices have been found to positively contribute to customer perceptions of security (Chellappa and Pavlou, 2002).

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). Notices, such as privacy policies on a website, inform customers in advance about how information will be gathered, handled, stored etc. (Liu et al., 2005). There is also an argument that notices such as privacy seals and the use of security features act as trust indices (Belanger et al., 2002). In other words, privacy policies "serve as a basis for decision making for consumers" (Jensen and Potts, 2004: 471). Tang et al. (2008) argue that giving 'notice' to customers empowers them and is considered one of the core fair information principles. The importance of privacy notices is understood by some SNS, and a few sites (e.g. Facebook) give users the option to customise their own privacy policies (Fang and LeFevre, 2010), but studies have shown that Facebook users have misunderstood its privacy policies (Livingstone and Brake, 2010). Felt and Evans (2008) point out that current social media "platforms cannot enforce their privacy policy with third party applications ….thereby increasing the risk of malicious data harvesting" (p.8).

2.2 Hypothesis development

The literature indicates that the presence of security notices serves as a success factor in website development. For instance, past research reveals that security notices enhance trust towards the online vendor (Berthon et al., 2008; Chen and Barnes, 2007; Chang and Chen, 2009; Greunen et al., 2010; Kim et al., 2010) and increase online purchase intention (Delafrooz et al., 2011; Peikari, 2010). It is unclear whether users pay attention to security notices that might not be obvious at a cursory glance (e.g. a security statement as oppose to a security seal). Even if security features with low visibility attract the attention of users, whether they read and understand such statements is doubtful (Volkamer and Renaud, 2013). It appears that some security conscious web users do pay attention to and read less obvious security notices. Kim et al. (2010) and Orito et al. (2013) found proof that security statements increase the perceived security of web users.

Miyazaki and Fernandez (2001) contend that new technologies have increased individual internet use and, as a result, online businesses have benefited from gaining access to customer information. Failing to protect customer information may lead to unfavourable repercussions, however, including the loss of customer trust, or legislative mandate (Petty, 2000). Self-efficacy and past experience were found to be indicators of internet usage (Eastin and LaRose, 2000; Rifon et al., 2005). It is not clear whether higher internet use or experience increases the probability of paying more attention to security notices, however, some argue that seals and notices help customers “to heuristically evaluate a site” (Rifon et al., 2005: 360) and “provide a certain level of institutional assurances” (Sia et al., 2009: 497). Others have found that even experienced users are unfamiliar with, or not aware of, security notices such as web security seals (Belangeret al., 2002). Based on these findings, we argue that social technology experience and higher use give individuals more opportunity to evaluate a site and determine whether there are institutional assurances in the form of security seals. Additionally, we test whether experience of previous purchases in a social context reduces the likelihood of paying attention to security notices. To this end, we propose to test the following two hypotheses:

H1: *The higher the SNS usage the higher the probability of paying attention to security notices/features.*

H2: *Users who have previous purchase experience in SNS pay less attention to security notices/features.*

Debatin et al. (2009) use the following theories to provide context for their research into the privacy awareness of Facebook users. The researchers followed the uses and gratifications theory to explain how individuals use social media to fulfil their needs, including maintaining their social identity online, socialising and finding entertainment (LaRose et al., 2001). It is argued that on social media, the antecedents to behaviour and the consequences are dependent on the extent to which the SNS fulfils the gratification sought by users. Negative consequences, such as loss of privacy and security (victimisation), may seem less significant to users when the SNS experience seem more gratifying (Raacke and Bonds-

Raacke, 2008). The third-person effect theory is related to self-perception, where individuals perceive that privacy threats affect others more than themselves (Brosius and Engel, 1996; Salwen and Dupagne, 2000). Finally, the theory of ritualised media use is used to explain users' lack of attention to privacy settings on social media sites as a result of routine, everyday use of social media, similar to how one would use other media such as television or radio (Couldry, 2002; Liebes and Curran, 1998).

There are a number of ways in which an individual can be victimised in an online environment, including cyber-bullying (Wolak et al., 2007), unwanted sexual solicitation (Jones et al., 2012), harassment (Wells and Mitchell, 2013) and fraud (Hutchings, 2013). In this study we are interested in fraud victimisation, such as identity theft and bank fraud. According to Van Wilsem (2013:170) "a necessary condition for victimisation to occur is that targets (unwillingly) expose themselves to offenders". The Routine Activity Theory (RAT) by Cohen and Felson (1979) suggests that for a crime to take place, certain conditions must be fulfilled. These conditions include the convergence of a victim and a motivated offender; a criminal not only capable of, but also willing to commit a crime; and the absence of guardianship to prevent the crime (Cohen and Felson, 1979; Pedneault and Beauregard, 2013). In online crimes, RAT takes on a new meaning when one considers victimisation in terms of creating an 'opportunity' for offenders to find their online victims, and the enablement of 'guardianship'. In terms of guardianship, there is a debate as to who should safeguard, and what they should protect. While some argue that online guardianship should be measured in terms of the availability of firewalls and security software (Choi, 2008; Holt and Bossler, 2009), others suggest that guardianship should be exercised by individuals in terms of control over their online information (Reyns et al., 2011). We argue that the presence of security notices signifies 'guardianship' and that users who have experienced victimisation in the past are likely to look for signs of such guardianship when interacting with social media sites. Hence:

H3: *Previous fraud victimisation increases the probability of paying attention to security notices/features.*

Research into behavioural intentions on e-business sites revealed that there was a positive relationship between web assurance seals and purchase behaviour (Odom et al., 2002). Hu et al. (2002) found that presence of security notices such as Verisign and TRUSTe promoted trust on e-business sites and consequently influenced purchase decision, however, Kimery and McCord (2002) tested a positive relationship between viewing assurance seals and consumer trust towards a specific e-retailer, and found that the hypothesis was not supported. This raises two questions: whether the presence of security notices truly is a successful trust-building strategy and, if so, do customers look first for the security notices on a website before purchasing from an e-vendor? We thus propose the following hypothesis to find an answer to the question of successful trust-building in e-vendor for the social media settings:

H4: *Users who pay attention to security notices/features have higher purchase intentions.*

It has been shown that a sense of credibility affects perception of risk online (Corritore et al., 2003). Prior research indicates that security notices/features have more impact in situations where high risks are involved. For instance, purchasing products such as travel packages online is considered a high-risk situation and the presence of assurance seals seems to imply a sense of low risk (Hunton et al., 2001). Mauldin and Arunachalam (2002) found that when the perceived risk was low, customers did not demonstrate much interest in assurance seals. According to the above studies, there appears to be an association between assurance seals and risk perception (Byramjee and Korgaonkar, 2013; Henthorne et al., 2013), however, we are interested in risk propensity, or the tendency to take or avoid risks based on risk perception. Sitkin and Weingart (1995) and Wong (2005) found that risk propensity was inversely related to risk perception, indicating that in situations where perceived risk was high, the tendency to take risks was low. Founded on the argument that perceived risk is related to assurance seals and perceived risk is related to risk propensity, we contend that risk propensity could be related to security notices/features. Hence:

H5: *Users with higher risk propensity pay less attention to security notices/features.*

3. Empirical methodology

3.1 Sampling and design

The sampling design of the current research closely follows the approach employed by Bhutta (2012) in similar web-based research. The study population consists of social media users on the World Wide Web. The sampling unit is individuals (social media users). There are a large number of social networks online, but access to the member list of such SNSs is difficult and restricted (Smith, 2013). Since probabilistic sampling methods cannot be applied in this context, this research uses a non-probability sampling framework. Non- probability sampling consists of convenience sampling and purposive sampling (divided into judgement and quota sampling). Specifically, convenience sampling is used by researchers to “collect information from members of the population who are conveniently available” and “is often used during the exploratory phase of a research project” (Sekaran and Bougie, 2010: 276). We have used convenience sampling during the pilot testing of the questionnaire. Purposive sampling, particularly judgement sampling was used to collect data in the final stage of the data collection process (i.e. subjects were selected based on their ability to provide the information required for the research (for further discussion see Sekaran and Bougie (2010)). In this case, the respondents are active users of social media sites with access to the internet, which is a 'parameter of interest' for this research. The final questionnaire has been administered to members of popular social media sites including, for example, Facebook, LinkedIn and Twitter.

Krejcie and Morgan (1970), and Isaac and Michael (1981) recommended a sample of approximately 400 respondents for a population of 100,000 plus. Since the respondents are 'volunteer panels of internet users' (Couper, 2000) and because the survey was circulated on multiple SNSs as well as through personal contacts (resulting in snowball sampling or chain-referrals), we were able to increase the representativeness of our sample (Bhutta, 2012). There is evidence suggesting that non-probability sampling using social media as a sampling frame is just as valid as studies conducted using probability sampling (for discussion see Bainbridge (1999) and Bainbridge (2002)). In fact, studies show that using SNS as a sampling frame could increase representativeness because of the demographic variation in the population (Lenhart, 2009). Concerns about self-selection and selection bias (see Duffy, 2002) may be less problematic within the current survey design. In fact, self-selection in web surveys is favoured over interception (e.g. randomly selecting visitors to a website by displaying a message) or using college subject pools (Marsden and Wright, 2010). Research findings indicate that participants from self-selected samples provide clearer, more complete responses than participants who are not self-selected volunteers (Gosling and Vazire, 2004). This view has been further supported by other commentators (Pettit, 2002; Walsh et al., 1992).

The final survey was only accessible to members of a particular group (e.g. LinkedIn specialised groups, such as specialist cybercrime forensics groups, or academics with profiles on Method Space) or posted on personal websites that could 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, bypassing restrictions. The criteria 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. what SNS the respondents were currently using, and how often they used them). Over 700 individuals responded to the survey, and the number of usable responses after data purification and eliminating missing values amounted to 502.

3.2 The dependent variable: Security notices

With the aim of assuring consumers that personal information is handled safely by websites, businesses have widely adopted self-regulatory transparency mechanisms (Acquisti et al., 2013). These mechanisms received the name 'notice' or 'notifications', which refer to privacy statements and privacy seals. Websites use notices, such as privacy policies, to keep their customers aware of how their information is collected, handled, stored, etc., (Liu et al., 2005). Third party privacy seals or security are also used to reassure e-commerce users. While they serve as contextual cues, according to John et al. (2011), they may lead to a rise in information disclosure at different levels. The literature on security artefacts shows that privacy seals may increase willingness to purchase goods online (Kovar et al., 2000; Noteberg et al., 2003) and encourage the disclosure of personal information (Hu et al., 2010;Posey et al., 2010). Belanger et al. (2002) used privacy and security seals, and privacy statements to measure the effect of such notices on the perceived security of customers and found it to be high. Shin (2010) argues that in order to establish trust on SNS, service providers need to include trust indices such as privacy seals. Chen and Shi (2009) point out that when acquiring information on SNS, self-regulation using a third-party notary system can be used as a mechanism for market regulation, especially in the wake of social networking commerce.

Some researchers argue that incorporating privacy and security into online systems (e.g. privacy/security policies, seals) originated from a need to shield organisations from the threat of privacy litigation, rather than from a need to increase the trustworthiness of a business or to protect the personal information of customers (Pollach, 2007; Orito et al., 2013). Some of these privacy notices (e.g. privacy policies) are "too legalistic and complicated for end-users to read and understand" (Coopamootoo and Ashenden, 2011: 316). Research also suggests that privacy/security notices do not influence privacy-related decision making, perhaps because notices such as privacy policies are "often hard to find, difficult to understand" (Acquisti et al., 2013:72). There is also the threat of fake security seals on websites that are used by fraudsters to gain user confidence (Furnell, 2005). In a study by Evil et al. (2003) it was found that even when the web assurance seal was fake, users still trusted the seal. In another study by Moores (2005) a staggeringly low 15% of the respondents recognised fake assurance seals.

The survey asked respondents whether they considered security notices, third party privacy seals, the content of privacy statement and third party security seals important in their decision to buy things online, using a seven-point scale (1 = strongly disagree; 7 = strongly agree). The online security notices (osn_i) variable was constructed from these four items where a seven point index was constructed (mean = 5.347; Cronbach's alpha = 0.852).

3.3 The independent variables

The social media usage variable was measured by frequency analysis, whereby respondents indicated their use (or non-use) of SNSs (Twitter, LinkedIn, MySpace, Google+, YouTube,Blogger, Skype, Flickr, Second Life, World of Warcraft and Facebook), and how often each SNS was used (Scale: 'Never'; 'Registered but do not use'; 'Open all the time'; 'Several times a day'; 'Once or twice per day'; 'Every 2–3 days'; 'Once a week'; and 'Less than once a week'). We recoded the variables to range from one to eight, where one meant 'No use' and eight meant 'Open all time'. Principal component analysis revealed that patterns of use varied between different types of SNSs. Consequently, in line with the classifications developed and used by Hoffman and Fodor (2010), Kaplan and Haenlein (2010) and Xiang and Gretzel (2010), we adopted the following typology:

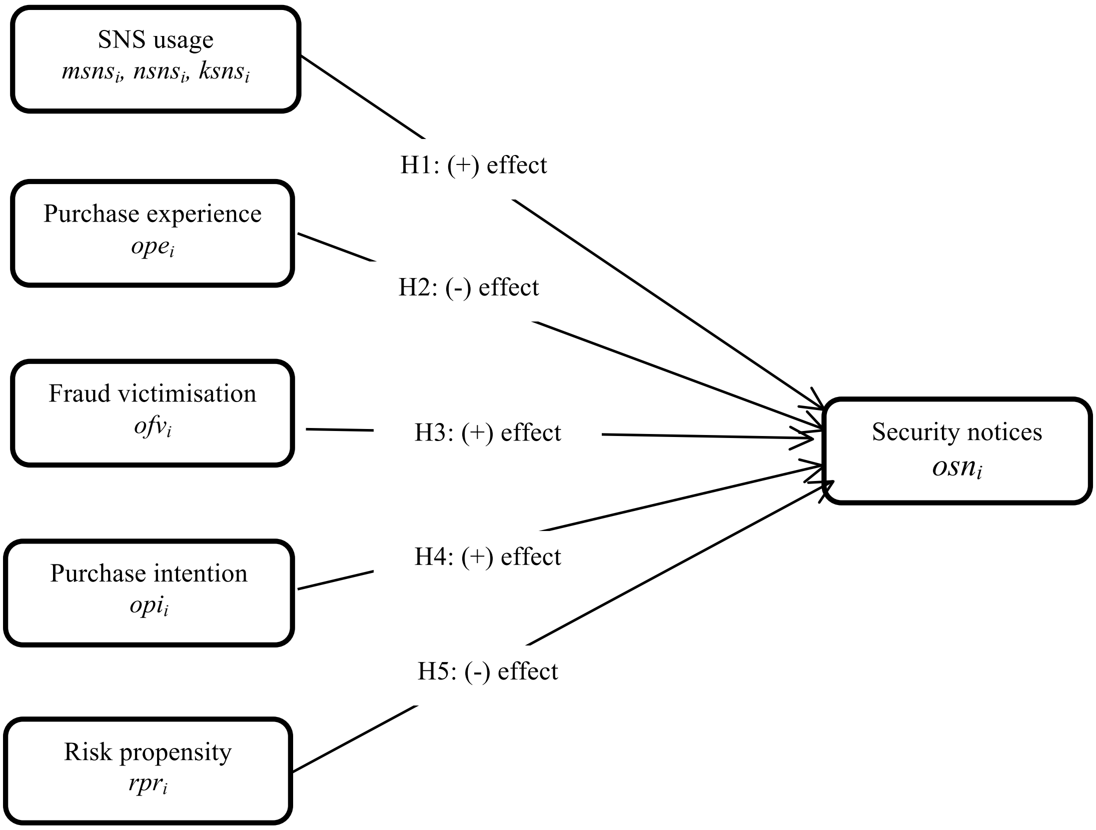
- *Multi-purpose dominant social networking services usage* ($msns_i$) includes Facebook, Skype, Google+ and YouTube, which demonstrated a common feature - all were used for content sharing and viewing in addition to socialisation at the personal and professional levels. These are the dominant platforms in the social media landscape.
- *Narrow-purpose social networking services usage* ($nsns_i$) included social media primarily used for specific purposes, such as gamification or virtual worlds, for instance, World of War Craft, Second Life and MySpace.
- *Knowledge-exchange purpose social networking services usage* ($ksns_i$) included Twitter, LinkedIn, Blogger and Instagram. According to Kietzmann et al. (2011), SNSs used for sharing were seen as a means of interaction and whether users wished to interact or not may depend on the functional objectives of the social media platform. For instance, the objects of social exchange are photographs, in the case of Instagram or Flickr.

The survey asked respondents whether they had been victims of cybercrime, providing them with a number of options to describe the nature of victimisation. The options included 'Fraud (e.g. bank fraud, identity theft)'; 'Offensive content'; 'Harassment (e.g. cyber-stalking, cyber-bullying)'; and any other type of victimisation, as well as 'I have never been a victim of cyber-crime'. We constructed a binary indicator to capture online fraud victimisation (ofv_i), which took the value of one for the individuals who had been victims of fraud (16.93%), and the value of zero if the individual has not experienced cyber victimisation (83.07%).[5] The online purchase experience (ope_i) variable was also measured as a binary indicator, taking the value of one if an individual purchased from SNS frequently or occasionally (18.01%) and the value of zero otherwise (81.91%). The online purchase intention (opi_i) was measured using a five item scale, where respondents were asked whether they preferred shopping on SNS, whether they intended or were willing to purchase from SNS in the future or were worried about security when purchasing from an SNS (mean = 2.863; Cronbach's alpha = 0.890) through a seven-point scale (1 = strongly disagree, 7 = strongly agree). Finally the risk propensity variable (rpr_i) was measured using a seven-point scale (1 = strongly disagree; 7 = strongly agree), and was measured with five items asking respondents about their willingness to take and accept risks (mean = 2.827; Cronbach's alpha = 0.793).

[5] We also examine whether fraud differs from other types of online victimisation(ocv_i).

FIGURE 1.

Social media behaviour towards security notices.



3.4 Empirical specification

Figure 1 represents the proposed research model, along with the hypothesised statistical associations between the constructs. As discussed earlier, the dependent variable, security notices (*osn_i*), is ordinal, which is measured on a 7-point scale assigning the numerals {1, . . . 7} to the categories {‘‘Strongly disagree . . . ‘‘Strongly agree’’}. The metric used to code the variable, however, is substantively meaningful and thus, the difference between 1 and 2 may be different from the difference between 2 and 3, 3 and 4 etc. (see Wooldridge, 2002). Additionally, when using discrete dependent variables, ordinary least squares (OLS) is not an appropriate estimator for our model (e.g. predicted probabilities are not bounded by the values of 0 and 1, heteroskedasticity is present) (for further discussion see Maddala, 1983). In this paper we therefore conducted an ordered probit analysis to explore the determinants of the security notices/feature index:

$$osn_i^* = b'X_i + u_i \quad (1)$$

where osn_i^* represented the latent variable, denoting the unobserved propensity of individual *i* in paying attention to security notices/features, X_i is a row vector of explanatory variables ($msns_i$, $nsns_i$, $ksns_i$,ope_i, ofv_i , opi_i , rpr_i) and u_i is assumed to be normally distributed. In this model, an underline score is estimated as a linear function of the explanatory variables and a set of cut points. Although osn_i^* was unobserved, we observed osn_i such that: $osn_i = 1$ if $osn_i^* \leq \mu_1$; $osn_i = 2$ if $\mu_1 < osn_i^* \leq \mu_2$; $osn_i = 3$ if $\mu_2 < osn_i^* \leq \mu_3$; $osn_i = 4$ if $\mu_3 < osn_i^* \leq \mu_4$; $osn_i = 5$ if $\mu_4 < osn_i^* \leq \mu_5$; $osn_i = 6$ if $\mu_5 < osn_i^* \leq \mu_6$ and $osn_i = 7$ if $\mu_6 < osn_i^*$, where b and μ (threshold parameters) are the parameters to be estimated (Wooldridge, 2002).[6]

4. Empirical findings

Recent studies (Kashimaa et al., 2013) show that social network users acquire risk-averse behaviours during social media usage. Their decision making process changes based on personal predisposition, peer-to-peer knowledge sharing, and external influences, such as the role of security notices (Acquisti et al., 2013). Users learn to act securely online and protect their personal information (Belanger et al., 2002). Our findings enrich the existing knowledge in the field and help gain an understanding of online user behaviour in the social media context.

The ordered probit estimates of the security notice model are given in Table 1. Three models are shown. Model 1 includes the three categories of social media usage as

[6] $0 < \mu_1 < \mu_2 < \mu_3 < \mu_4 < \mu_5 < \mu_6$.

explanatory variables, the online fraud victimisation variable, the online purchase experience and intention variables, and finally, the risk propensity variable. Model 2 is a restricted form of the previous model and Model 3 makes a distinction between online fraud and other forms of online victimisation. **Hypothesis 1** suggests there is a positive and statistical association between SNS usage and paying attention to security notices/features. The coefficient of both multi-purpose dominant social networking services usage ($msns_i$) and knowledge-exchange purpose social networking services usage ($ksns_i$) are found to be positive and statistically insignificant. Thus, Hypothesis 1 is partially rejected. The coefficient for narrow purpose social networking services usage ($nsns_i$) is, however, found to be negative and statistically significant. The main purpose of these social networking services is to enable virtual interactions between users with narrow interests (for example, music interest or gaming). Only a small (narrow) subset of functionalities are used, which may explain this result.

Hypothesis 2 suggests a negative and statically significant link between purchase experience in SNS and paying attention to security notices/features, however, we found no empirical support for Hypothesis 2. Perhaps this implies that individuals with more purchase experience are just as likely to pay attention to security notices/features rather than endanger the safety and success of their purchase. The third-person effect theory (Debatin et al., 2009) offers an explanation of this finding as e-shoppers perceive that privacy threats affect others more than themselves.

Hypothesis 3 suggests that previous fraud victimisation increases the probability of paying attention to security notices/features, however, our results fail to establish any statistical association, even when we distinguish between fraud and other forms of online victimisation. This may be explained by considering that online fraud may involve very different circumstances and situations from those in which it has previously experienced. In other words, it can be argued that individuals perceive that the gratification obtained from using a SNS outweigh the negative consequences of victimisation, and therefore, users would not let incidents of past victimisation prevent them from using SNS to fulfil their needs for socialising, finding entertainment, etc.

Hypothesis 4 implies that there is a strong positive link between purchase intention and paying attention to security notices/features. All three models provide empirical support for this hypothesis. This finding has practical significance for SNS providers and for businesses using SNS for commercial purposes. In similar research in the e-commerce context, it has been found that customers recognise privacy/security notices on websites (Harris, 2001) and that privacy/security statements have a positive impact on purchase intention (Miyazaki and Fernandez, 2001). Social media web merchants can use privacy/security notices for economic benefit by displaying notices such as TRUSTe, BBBOnLine and Verisign on SNS (Belanger et al., 2002).

Finally, **Hypothesis 5** suggests that the higher the propensity towards risk the lower the probability of paying attention to security notices/features. Our results support this association. Risk awareness has been shown to be an antecedent of the intention to engage in security behaviour in leisure and professional activity (Dutta and McCrohan, 2002; Von Solms and van Niekerk, 2013). Social learning theory and the acquisition of descriptive norms (what others do in such situations), provides an explanation as to why the propensity towards risk of certain individuals can be influenced through conceptual norm acquisition (Kashimmaa et al., 2013). While learning by direct observation in online social networks is rarely available as an option, conceptual norm acquisition, either through what other members of the network say or through awareness initiatives, provides a proven tool to influence risky behaviour. Businesses, education institutions and government organisations now provide some form of education programme aimed at raising awareness of the risks of social media use. This research provides evidence that social networking requires more efforts to ensure safe use from the SNS providers, third parties and end users. Effective risk awareness education has the potential to improve safety on social networks and, consequently, heighten risk perception amongst users, making them aware of the ways to avoid victimisation.

TABLE 1

Ordered probit estimates of the probability of paying attention

to security notices/features (*osn_i*)

	Model 1		Model 2		Model 3	
Variable	Coef.	Std. Err.	Coef.	Std. Err.	Coef.	Std. Err.
$msns_{i,}$	0.029	0.051				
$nsns_{i,}$	-0.075*	0.033	-0.076*	0.033	-0.074*	0.034
$ksns_i$	0.012	0.047				
ofv_i	-0.134	0.094	-0.135	0.094	-0.175	0.108
ocv_i					-0.113	0.141
ope_i	-0.073	0.133	-0.069	0.133	-0.066	0.133
opi_i	0.099**	0.037	0.106**	0.035	0.103**	0.036
rpr_i	-0.125**	0.034	-0.124**	0.034	-0.124**	0.034
Loglikelihood	-833.87663		-834.07861		-833.7585	
Wald chi2	29.29		28.43		29.28	
Observations	502		502		502	

**Significant at the 1% level. *Significant at the 5% level.

5. Implications for practice

The phenomenon of SNS as portals for web transactions is still relatively new but it is becoming increasingly important for SNS to diversify their revenue streams and move away from pure advertising models. This paper used a survey of over 500 active social networking users to explore how they perceive information security seals from third parties in their online buying behaviour. In particular, we empirically examined the relationships between the use of various types of social networks, user victimisation, purchase experience, purchase intention, propensity towards risks and the attention paid to security notices by social media users.

The findings of this study showed that the overall intensity of social media use alone did not increase the probability of paying attention to security notices. In line with the third-person effect theory, social networking users may think that privacy threats affect others more than themselves (Brosius and Engel, 1996; Salwen and Dupagne, 2000). This self-denial of the threat to privacy may explain the empirical finding for Hypothesis 1 of the current research (i.e. that association between social media usage and attention to privacy/security notices are statistically insignificant). The situation is different for the narrow-purpose social networking sites (World of War Craft, Second Life and MySpace) where the probability of users paying attention to security notices actually decreases with use. As we know from theory, the possibility of victimisation seems less worrying to users seeking a gratification experience on SNS (Raacke and Bonds-Raacke, 2008). An explanation for this may be dependent on the type of use on the sites. For most SNS, making purchases is still a rare occurrence for users and such transactions are infrequent for the majority of users. They will, therefore, pay the same amount of attention to security notices. For narrow purpose sites however, the revenue model was based on more frequent user transactions (e.g. purchase of virtual goods on Second Life). The nature of the transaction was often confined to a single merchant relationship, which users may trust more as they use the site more. This would also explain why purchase experience did not appear to influence the amount of attention paid to security notices for the majority of SNS. The conclusion that higher use and previous volume of transactions does not lead to higher complacency in social networking users is an important one.

We also found no effects between learning from past purchase experience, a history of online victimisation and paying attention to security notices. Communication theories (users and gratifications theory, third-person effect theory, and theory of ritualized media use) discussed in this paper may provide some explanation for these findings. For example, the ritualistic or repetitive use of SNS may reduce SNS users' anxiety about victimisation and prevent them from paying more attention to security/privacy notices. However, we found strong statistical effects in online purchase intention and risk propensity on security notices. Risk-averse users tend to pay more attention to security notices, which is an important finding for fostering safe behaviour online.

6. Conclusions

The literature highlights that social networks lag behind in the development of suitable security notices to address the online protection of social media users. In a survey of over 500 active social media users, this study empirically explored the association between purchase experience, purchase intention, propensity towards risk, use of different categories of social networks, user victimisation and the attention paid to security notices/features. This article closes the gap in literature about consumer purchase behaviour in the social networking context and helps inform practices on how social media user behaviour affects their purchase intentions.

The findings of this study have implications for social networking service providers. Security notices are deemed important in the SNS context, as they are in traditional e-commerce - users who pay attention to them also tend to be in the group of those willing to transact, and who are more risk-averse. Such notices, therefore, continue to play an important role in reassuring customers. As the transactional potential in SNS becomes better known and used, security notices remain an underexplored field needing further attention from both industry experts and researchers. This study sheds more light on the customer perceptions of security notices, but larger scale and longitudinal studies should be carried out to address potential weaknesses of smaller samples, and capture possible changes of experience, attitude and intention over time, respectively. Comparisons among countries and sub-populations (e.g. different genders and age groups) may also deserve future attention. We welcome further empirical testing of the proposed model and engagement with industry in order to develop effective security notices suitable for social networking context.

References

Acquisti, A., Adjerid, I., Brandimarte, L., 2013, Gone in 15 seconds: The limits of privacy transparency and control. IEEE Security and Privacy. 11(4): 72-74.

Agarwal, R., Gupta, A.K., Kraut, R., 2008, Editorial overview: The interplay between digital and social networks. Information Systems Research.19(3): 243-252.

Alba, J., Lynch, J., Weitz, B., Janiszewski, C., Lutz, R., Sawyer, A., Wood, S., 1997. Interactive home shopping: consumer, retailer, and manufacture incentives to participate in electronic marketplaces. Journal of Marketing, 61(3):38–53.

Al-Dwairi, R.M., 2013, E-commerce web sites trust factors: An empirical approach. Contemporary Engineering Sciences. 6 (1): 1-7.

Andrew, S., 2014, Recent security breaches for social networks. Retrieved December 14, 2014, from http://www.ieplexus.com/web-20/social-networking/6227-recent-security-breaches-for-social-networks/.

Aral, S., Dellarocas, C., Godes, D., 2013, Introduction to the special issue—Social media and business transformation: A framework for research. Information Systems Research. 24(1): 3-13.

Bainbridge, W. S., 1999, Cyberspace: Sociology's natural. Contemporary Sociology. 28(6): 664-667.

Bainbridge, W. S., 2002, Validity of web-based surveys: Explorations with data from 2,382 teenagers. In Burton, O. V (eds.) Computing in the Social Sciences and Humanities. Chicago: University of Illinois Press. 51-66.

Bandura, A., 1971, Social learning theory. New York, NY: General Learning Press.

Bandura, A., 1986, Social foundations of thought and action: A social cognitive theory. Englewood Cliffs. NJ: Prentice-Hall.

Belanger, F., Hiller, J.S., Smith, W.J., 2002, Trustworthiness in electronic commerce: The role of privacy, security, and site attributes. The Journal of Strategic Information Systems. 11(3): 245-270.

Benassi, P.,1999, TRUSTe: An online privacy seal program. Communications of the ACM, 42(2): 56-59.

Berthon, P., Pitt, L., Cyr, D., Campbell, C., 2008, E-readiness and trust: Macro and micro dualities for e-commerce in a global environment. International Marketing Review. 25(6): 700-714.

Bharadwaj, A., El Sawy, O.A., Pavlou, P.A., Venkatraman, N., 2013, Digital business strategy: Toward a next generation of insights. MIS Quarterly. 37(2): 471-482.

Bhutta, C.B., 2012, Not by the book: Facebook as a sampling frame. Sociological Methods and Research. 41:57-88.

Brosius, H.B., Engel, D., 1996, The causes of third-person effects: Unrealistic optimism, impersonal impact, or generalized negative attitudes towards media influence? International Journal of Public Opinion Research, 8(2): 142-162.

Byramjee, F., Korgaonkar, P., 2013, A review of the role of consumers' transaction costs in the traditional and online shopping environments. Review of Business Research. 13(3): 41-46.

Campbell, K., Gordon, L.A., Loeb, M.P., Zhou, L., 2003, The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. Journal of Computer Security. 11:431-448.

Cavusoglu, H., Mishra, B., Raghunathan, S., 2004, The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. International Journal of Electronic Commerce. 9: 69-104.

Chang, H.H., Chen, SW., 2009, Consumer perception of interface quality, security, and loyalty in electronic commerce. Information and Management. 46:411-417.

Chellappa, R.K., Pavlou, P.A., 2002, Perceived information security, financial liability and consumer trust in electronic commerce transactions. Logistics Information Management. 15(5/6):358-368.

Chen, Y., Barnes, S., 2007, Initial trust and online buyer behaviour. Industrial Management and Data Systems. 107(1): 21-36.

Chen, X., Shi, S., 2009, A literature review of privacy research on social network sites. International Conference on Multimedia Information Networking and Security. 1: 93-97.

Cheung, M.Y.,Luo, C., Sia, C.L., and Chen, H. (2009) Credibility of electronic word-of-mouth: Informational and normative determinants of on-line consumer recommendations. International Journal of Electronic Commerce, 13 (4): 9-38.

Choi, K., 2008, Computer crime victimisation an integrated theory: An empirical assessment. International Journal of Cyber criminology. 2:308-333.

Cialdini, R.B., Reno, R.R., Kallgren, C.A., 1990, A focus theory of normative conduct: Recycling the concept of norms to reduce littering in public places. Journal of Personality and Social Psychology. 58(6): 1015-1026.

Cohen, L.E., Felson, M., 1979, Social change and crime rate trends: A routine activity approach. American Sociological Review. 44:588-608.

Coopamootoo, P. L., Ashenden, D., 2011, Designing usable online privacy mechanisms: What can we learn from real world behaviour? In Turner, A. J. (ed.) Privacy and Identity Management for Life. Heidelberg: Springer: 311-324.

Corritore, C.L., Kracher, B., Wiedenbeck, S., 2003. On-line trust: concepts, evolving themes, a model. International Journal of Human-Computer Studies 58 (6), 737-758.

Couldry, N., 2002, Media rituals: A critical approach. London: Routledge.

Couper, M. P., 2000, Web surveys: A review of issues and approaches. The Public Opinion Quarterly. 64 (4): 464-494.

Culnan, M. J., McHugh, P. J., and Zubillaga, J. I., 2010, How large US companies can use Twitter and other social media to gain business value. MIS Quarterly Executive, 9(4): 243-259.

Dang, T.K., Dang, T.T., 2013, A survey on security visualization techniques for web information systems'. International Journal of Web Information Systems. 9(1): 6-31.

Debatin, B., Lovejoy, J.P., Horn, A.K., Hughes, B.N., 2009, Facebook and online privacy: Attitudes, behaviours, and unintended consequences. Journal of Computer-Mediated Communication. 15(1): 83-108.

Delafrooz, N., Paim, L.H., Khatibi, A., 2011, Understanding consumer's internet purchase intention in Malaysia. African Journal of Business Management. 5(3):2837-2846.

Dhillon, G., Backhouse, J.,2001, Current directions in IS security research: towards socio-organizational perspectives. Information Systems Journal, 11(2): 127-153.

Duffy, M.E., 2002, Methodological issues in web-based research. Journal of Nursing Scholarship. 34: 83-88.

Dutta, A., McCrohan, K., 2002, Management's role in information security in a cyber-economy. California Management Review, 45(1): 67-87.

Eastin, M.S., LaRose, R., 2000, Internet self-efficacy and the psychology of the digital divide. Journal of Computer Mediated Communication. 6 (1).

Ellison, N.B., 2007, Social network sites: Definition, history, and scholarship. Journal of Computer-Mediated Communication. 13(1):210-230.

Evil, A. Y., Shaver, E. F., Wogalter, M. S., 2003, On trust in the internet: Belief cues from domain suffixes and seals of approval. In Proceedings of the Human Factors and Ergonomics Society Annual Meeting. 47 (11): 1346-1350.

Fang, L., and LeFevre, K. (2010). Privacy wizards for social networking sites. In Proceedings of the 19th International Conference on the World Wide Web, pp. 351-360, ACM.

Felt, A., and Evans, D., 2008, Privacy protection for social networking apis 2008 Web 2.0 Security and Privacy (W2SP'08).

Furnell, S. M., 2005, Considering the security challenges in consumer-oriented eCommerce. In Proceedings of the Fifth IEEE International Symposium on Signal Processing and Information Technology. 534-539.

Gosling, S.D., Vazire, S., 2004, Should we trust web-based studies? A comprehensive analysis of six preconceptions about Internet questionnaires. American Psychologist. 59:93-104.

Gradon, K., 2013, Crime science and the internet battlefield: Securing the analogue world from digital crime. Security and Privacy. 11:93-95.

Greunen, D.V., Herselman, M.E., Niekerk, J.V., 2010, Implementation of regulation-based e-procurement in the Eastern Cape provincial administration. African Journal of Business Management. 4(17):3655-3665.

Guitton, C., 2013, Cyber insecurity as a national threat: Overreaction from Germany, France and the UK? European Security. 22:21-35.

Harris, I., 2001, Why some companies are trusted and others are not: Personal experience and knowledge of company more important than glitz. Available at http://www.harrisinteractive.com/harris_poll/index.asp?PID ¼ 237 [Accessed: 20/01/2014].

Henthorne, T.L., George, B.P., Smith, W.C., 2013, Risk perception and buying behaviour: An examination of some relationships in the context of cruise tourism in Jamaica. International Journal of Hospitality and Tourism Administration. 14(1):66-86.

Hickins, M., 2012, The morning download: How Facebook could kill your business. Retrieved April 21, 2014, from http://blogs.wsj.com/cio/2012/04/09/the-morning-download-how-facebook-could-kill-your-business/.

Hoffman, D. L., Fodor, M., 2010, Can You Measure the ROI of Social Media Marketing? MIT Sloan Management Review, 52 (1):41–49

Hoffman, D.L, Novak, T. P., 2012, Toward a Deeper Understanding of Social Media, Journal of Interactive Marketing, 26 (2):69–70

Holt, T.J., Bossler, A.M., 2009, Examining the applicability of lifestyle-routine activity theory for cybercrime victimisation. Deviant Behaviour. 30:1-25.

Hu, X., Lin, Z., Zhang, H., 2002, Trust promoting seals in electronic markets: An exploratory study of their effectiveness for online sales promotion. Journal of Promotion Management. 9(1-2):163-180.

Hsu, M.-H., Ju, T.L., Yen, C.-H., Chang, C.-M., 2007, Knowledge sharing behavior in virtual communities: The relationship between trust, self-efficacy, and outcome expectations. International Journal of Human Computer Studies. 65, 153-169.

Hunton, J.E., Benford, T., Arnold, V., Sutton, S.G., 2000, The impact of electronic commerce assurance on financial analysts' earnings forecasts and stock price estimates. Auditing: A Journal of Practice and Theory. 19(1):5-22.

Hutchings, A., 2013, Hacking and fraud qualitative analysis of online offending and victimization'. In Global Criminology (eds.) Jaishankar K. and Ronel N., Crime and Victimization in a Globalized Era. pp. 93-112, Taylor and Frances Ltd.

Isaac, S., Michael, W.B., 1981, Handbook in research and evaluation. San Diego, CA: EdITSPublishers.

Jensen, C., Potts, C., 2004, Privacy policies as decision-making tools: An evaluation of online privacy notices. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, ACM: 471-478.

Jones, L.M., Mitchell, K.J., Finkelhor, D., 2013, Online harassment in context: Trends from three youth internet safety surveys (2000, 2005, 2010). Psychology of Violence Special Issue on Technology and Violence: Risk, Prevention, Intervention, and Methodology. 3:53-69.

Kaplan, A. M., Haenlein, M., 2010, Users of the world, unite! The challenges and opportunities of Social Media, Business Horizons, 53(1): 59-68.

Kashimaa, Y., Wilson, S., Lusher, D., Pearson, L., Pearson, C., 2013, The acquisition of perceived descriptive norms as social category learning in social networks. Social Networks. 35:711-719.

Kelley, P.G., Bresee, J., Cranor, L.F., Reeder, R.W., 2009, A nutrition label for privacy. In Proceedings of the 5th Symposium on Usable Privacy and Security (SOUPS), Mountain View, CA, 1-12.

Kim, C., Tao, W., Shin, K. K., 2010, An empirical study of customers' perceptions of security and trust in e-payment systems. Electronic Commerce Research and Applications. 9:84-95.

Kim, D.J., Steinfield, C., Lai, Y.J., 2008, Revisiting the role of web assurance seals in business-to-consumer electronic commerce. Decision Support Systems. 44(4):1000-1015.

Kimery, K.M., McCord, M., 2002, Third-party assurances: Mapping the road to trust in e-retailing. Journal of Information Technology Theory and Application. 4(2):63-82.

Kovar, S. D., Burke, K.G., Kovar, B. R., 2000, Consumer responses to the CPA WEBTRUST Assurance. Journal of Information Systems, 14:17-35.

Kozinets, R. V. (1999) E-Tribalized marketing? The strategic implications of virtual communities of consumption, European Management Journal, 17(3), 252-264.

Krejcie, R. V., Morgan, D.W., 1970, Determining sample size for research activities. Educational and Psychological Measurement. 30:607-610.

LaRose, R., Mastro, D., Eastin, M.S., 2001, Understanding internet usage: A social-cognitive approach to uses and gratifications. Social Science Computer Review. 19(4):395-413.

Lala, V., Arnold, V., Sutton, S.G., Guan, L., 2002, The impact of relative information quality of e-commerce assurance seals on internet purchasing behaviour. International Journal of Accounting Information Systems. 3(4):237-253.

Lenhart, A., 2009, Adults and Social Network Websites. Pew Internet and American Life Project. Available at:

http://www.pewinternet.org/~/media//Files/Reports/2009/PIP_Adult_social_networking_data_memo_FINAL.pdf.

Liebes, T., Curran, J., 1998, Media, ritual and identity. London: Routledge.

Lievrouw, L.A., Livingstone, S., 2002, Handbook of new media: Social shaping and consequences of ICTs. Sage.

Liu, C., Marchewka, J. T., Lu, J., Yu, C. S., 2005, Beyond concern-a privacy-trust-behavioral intention model of electronic commerce, Information and Management, 42 (2): 289-304.

Liu, B.Q., Goodhue D.L., 2012, Two worlds of trust for potential e-commerce users: Humans as cognitive misers. Information Systems Research. 23(4):1246-1262.

Livingstone, S., and Brake, D. R., 2010, On the rapid rise of social networking sites: New findings and policy implications. Children and society, 24(1), 75-83.

Maddala, G. S. 1983, Limited-dependent and qualitative variables in economics, New York: Cambridge University Press.

McDonald, A.M., Cranor, L.F., 2008, Cost of reading privacy policies, the I/S. A Journal of Law and Policy for the Information Society. 4(3):543-568.

Mangold, W. G., and Faulds, D. J., 2009, Social media: The new hybrid element of the promotion mix. *Business Horizons*, *52*(4): 357-365.

Malthouse, E.C., Haenlein, M., Skiera, B., Wege, E., Zhang, M., 2013, Managing customer relationships in the social media era: Introducing the social CRM house. Journal of Interactive Marketing. 27(4):270-280.

Marsden, P.V., Wright, J.D., 2010, Handbook of survey research, 2nd ed. Emerald Group Publishing.

Mauldin, E., Arunachalam, V., 2002, An experimental examination of alternative forms of web assurance for business-to consumer e-commerce. Journal of Information Systems. 16:33-54.

Milne, G.R., Culnan, M.J., 2004, Strategies for reducing online privacy risks: Why consumers read (or don’t read) online privacy notices. Journal of Interactive Marketing. 18(3):15-29.

Minihane, J. (2011) New PlayStation security breach: 93,000 accounts hit. Retrieved November 27, 2010, from http://www.t3.com/news/new-playstation-security-breach-93000-accounts-hit

Miyazaki, A.D., Fernandez, A., 2001, Consumer perceptions of privacy and security risks for online shopping. The Journal of Consumer Affairs. 35(1):27-44.

Moores, T., 2005, Do consumers understand the role of privacy seals in e-commerce? Communications of the ACM. 48(3): 86-91.

Noteberg, A., Christiaanse, E., Wallage, P., 2003, Consumer trust in electronic channels. E-Service Journal, 2(2): 46-67.

Odom, M.D., Kumar, A., Saunders, L., 2002, Web assurance seals: How and why they influence consumers' decisions. Journal of Information Systems. 16(2): 231-250.

Orito, Y., Murata, K., Fukuta, Y., 2013, Do online privacy policies and seals affect corporate trustworthiness and reputation? International Review of Information Ethics. 19:52-65.

Park, D., Lee, J., and Han, I., 2007, The effect of on-line consumer reviews on consumer purchasing intention: The moderating role of involvement. International Journal of Electronic Commerce, 11 (4): 125-148.

Pedneault, A., Beauregard, E., 2013, Routine activities and time use: A latent profile approach to sexual offenders' lifestyles. Journal of Research and Treatment. 26:1-24.

Peikari, H.R., 2010, Does nationality matter in the B2C environment? Results from a two nation study. Communications in Computer and Information Science. 92:149-159.

Peters, K., Chen, Y., Kaplan, A. M., Ognibeni, B., Pauwels, K., 2013, Social Media Metrics—A Framework and Guidelines for Managing Social Media. Journal of Interactive Marketing, 27(4): 281-298.

Pettit, F.A., 2002, A comparison of World Wide Web and pencil personality questionnaires. Behaviour Research Methods, Instruments, and Computers. 34:50-54.

Petty, R.D., 2000, Marketing without consent: Consumer choice and costs, privacy, and public policy. Journal of Public Policy and Marketing. 19:42-53.

Pollach, I., 2007, What's wrong with online privacy policies? *Communications of the ACM*. 50 (9): 103-108.

Posey, C., Lowry, P. B., Roberts, T. L., 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, 19(2):181-195.

Raacke, J., Bonds-Raacke, J., 2008, MySpace and Facebook: Applying the uses and gratifications theory to exploring friend-networking sites. Cyberpsychology and Behavior. 11(2):169-174.

Rapp, A., Beitelspacher, L. S., Grewal, D., Hughes, D. E., 2013, Understanding social media effects across seller, retailer, and consumer interactions, Journal of the Academy of Marketing Science, 41(5):1-20.

Rauch, J.E., 2001, Business and social networks in international trade. Journal of Economic Literature. 39:1177-1203.

Reyns, B.W., 2013, Online routines and identity theft victimisation: Further expanding routine activity theory beyond direct-contact offenses. Journal of Research in Crime and Delinquency. 50:216-238.

Rifon, N.J., LaRose, R., Choi, S., 2005, Your privacy is sealed: Effects of web privacy seals on trust and personal disclosures. Journal of Consumer Affairs. 39(2):339-362.

Rojas, H., Shah, D.V., Faber, R.J., 1996, For the good of others: Censorship and the third-person effect. International Journal of Public Opinion Research. 8(2):163-186.

Rubin, A.M., 1984, Ritualized and instrumental television viewing. Journal of Communication. 34 (3):67-77.

Salwen, P.B., Dupagn, M., 2000, The third-person effect: A meta-analysis of the perceptual hypothesis. Mass Communication and Society. 3(1):57-85.

Sekaran, U. and Bougie, R., 2010, Research methods for business: A skill building approach. 5th edn. New York : John Wiley and Sons.

Shin, D. H., 2010, The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption. Interacting with Computers. 22(5): 428-438.

Sia, C.L., Lim, K.H., Leung, K., Lee, M., Huang, W.W., Benbasat, I., 2009, Web strategies to promote internet shopping: Is cultural-customization needed? MIS Quarterly. 33(3):491-512.

Sitkin, S.B., Weingart, L.R., 1995, Determinants of risky decision-making behaviour: A test of the mediating role of risk perceptions and propensity. Academy of Management. 38(6):1573-1592.

Smith, T. W., 2013, Survey-research paradigms old and new. International Journal of Public Opinion Research. 25(2): 218-229.

Susarla, A., Oh, J.H., Tan, Y., 2013, Social networks and the diffusion of user-generated content: Evidence from YouTube. Information Systems Research. 23(1):23-41.

Tang, Z., Hu, Y. J., and Smith, M. D., 2008, Gaining trust through online privacy protection: Self-regulation, mandatory standards, or caveat emptor. Journal of Management Information Systems, 24(4): 153-173.

Van Wilsem, J., 2013, Bought it, but never got it: Assessing risk factors for online consumer fraud victimization. European Sociological Review. 29(2):168-178.

Volkamer, M., Renaud, K., 2013, Mental models–General introduction and review of their application to human-centred security. 255-280, Heidelberg: Springer Berlin.

Von Solms, B, 2001, Information Security — A Multidimensional Discipline, Computers & Security, 20(6): 504–508.

Von Solms, R., van Niekerk, J., 2013, From information security to cyber security. Computers and Security. 38: 97-102.

Walsh, J.P., Kiesler, S., Sproull, L.S., Hesse, B.W., 1992, Self-selected and randomly selected respondents in computer network survey. Public Opinion Quarterly. 56:241-244.

Wasserman, S., Faust, K.,1994, Social Network Analysis: Methods and Applications. Cambridge, ENG and New York: Cambridge University Press.

Wells, M., Mitchell, K.J., 2013, Patterns of internet use and risk of online victimization for youth with and without disabilities. The Journal of Special Education. 47(5):1-10

Wirtz, B. W., Schilke, O., and Ullrich, S. , 2010, Strategic development of business models: implications of the Web 2.0 for creating value on the internet. Long Range Planning, 43(2): 272-290.

Wolak, J., Mitchell, K.J., Finkelhor, D., 2007, Online harassment by known peers and online-only contacts. Journal of Adolescent Health. 41:S51-S58.

Wong, K.F.E., 2005, The role of risk in making decisions under escalation situations. Applied Psychology. 54(4):584-607.

Xiang, Z., Gretzel, U., 2010, Role of social media in online travel information search. Tourism Management, 31 (2): 179-188.

Zwass, V., 2010, Co-creation: Toward a taxonomy and an integrated research perspective. International Journal of Electronic Commerce, 15 (1): 11-48.