doi: 10.1111/isj.12082

The role of mobile-computing self-efficacy in consumer information disclosure

Mark J. Keith,* Jeffry S. Babb,† Paul Benjamin Lowry,‡
Christopher P. Furner§ & Amjad Abdullat†

*Brigham Young University, Provo, UT USA, email: mark.keith@gmail.com, †West Texas A&M University, Canyon, TX USA, ‡City University of Hong Kong, Kowloon Tong, Hong Kong, and §East Carolina University, Greenville, NC USA

Abstract. *Smartphones are increasingly penetrating business and consumer markets, and mobile applications (apps) have engendered a large and innovative market. Whereas apps are useful, they also present new forms of privacy risk associated with users' personal and location data. However, these dangers do not appear to increase the perceived risk or reduce the trust consumers demonstrate when using apps. Many information technology (IT) trust indicators are well documented such as the quality of the IT, trust assurances, brand recognition and social influences. However, these traditional indicators appear to have a lesser impact on the adoption of mobile commerce via apps because of the nature of mobile-app adoption and subsequent information disclosure. As a result, we draw from social cognitive theory and its construct of self-efficacy in particular to explain perceived mobile-app risk and provider trust. Through two controlled experiments, we demonstrate the strong direct effect of mobile-computing self-efficacy on users' initial trust in location-based app vendors as well as their perceived risk of disclosing information – regardless of the actual trustworthiness of the app vendor. The results imply that being skilled in the latest smartphones and apps can cause users to place greater trust in app providers and perceive less risk in the app itself, even when the intentions of the app providers cannot be verified.*

Keywords: mobile-computing self-efficacy, location-based services, trust, perceived risk, privacy calculus, mobile apps

INTRODUCTION

Smartphone adoption is taking place at a remarkable rate, surpassing 70% of Americans in the USA in 2014 (Smith, 2012; Dediu, 2014). Similar results are now in evidence around the world, with the fastest growth happening in China (1126%, quarter-by-quarter growth) (Farago, 2012). The demand for these multifunctional devices comes from both the consumer and business markets (Pitt *et al*., 2011). Initially, smartphones (e.g. RIM's Blackberry) were used by organisations to empower employees with mobile email and internet access. However, broader

global use of smartphones has exploded in consumer markets with the complementary emergence of the $11+ billion market (IDG, 2010) for mobile applications (apps).

Of particular interest in the emerging smartphone context are the location-based services (LBS) provided by apps for smartphones and similar mobile devices. Approximately one-third of apps make use of LBS (Security, 2011). LBS have enabled remarkable technology benefits, but they have also increased consumer privacy risks. Recent reports have demonstrated that vendors are indeed storing and transmitting location data and personal identification data, such as phone numbers and international mobile equipment identity numbers, without user consent (Seriot, 2010; Enck *et al*., 2010b; Angwin & Valentino-Devries, 2011).

Our general line of inquiry with regard to apps is not the traditional organisational systems adoption question of 'Why are employees so hesitant in adopting this technology, given how useful it is?' but 'Why are consumers so cavalier about adopting this technology, given how unknown the risk is?' Prior research into user trust in electronic commerce (e-commerce) vendors has identified a number of potentially good explanations, including usefulness (Wang & Benbasat, 2005), the quality of the e-commerce channel (McKnight *et al*., 2002), the attractiveness and usability of the interface (Vance *et al*., 2008), brand recognition and valuation (Lowry *et al*., 2008), user and consumer reviews (Forman *et al*., 2008), social influences such as referrals and word-of-mouth advertising (Kim, 2008; Awad & Ragowsky, 2008) and institutional privacy and security assurances (Kim *et al*., 2008; Xu *et al*., 2010).

Most of these constructs do not apply as strongly in the app context because of some key differences: for example, most apps are free or have a very low cost – consider that the average Apple iPhone app costs $1.83 (148apps, 2012). The adoption decision time is much quicker than for a desktop app. Furthermore, no assurance seals (e.g. Webtrust, VeriSign and Better Business Bureau (BBB)) are established for apps. App stores have consumer reviews and screenshots of app interfaces, but consumers are less likely to devote substantial time to reviewing small purchases. Brand recognition is also different in this consumer market: although recognisable brands do have apps, the vast majority of apps are produced by start-up companies with little to no brand recognition (Reed, 2011).

Although smartphone adoption is increasing rapidly, the smartphone market is still relatively young. In many countries, it has finished reaching the 'early adopters' and is beginning to reach the 'early majority' stage, according to the theory on the diffusion of innovations (Rogers, 1962). 'Early adopters' are described as those with a high degree of social and opinion leadership. From a social cognitive perspective (Bandura, 1977b), early adopters are those with a higher degree of 'self-efficacy'. Self-efficacy refers to a person's belief in his or her own competency and capability (Bandura, 1977a) and has often been linked with personal productivity (Bandura, 1977a; Marakas *et al*., 2007). However, a potential side effect of high self-efficacy is an illogical sense of trust in others or a decreased perception of risk. For example, in contexts such as financial analysts predicting stock market behaviour (Hilary & Menzly, 2006), and recently in software development (Moores & Chang, 2009), high self-efficacy has led to over-trusting and risk-taking behaviours. Applied in our context, as individuals achieve a certain level of success in particular tasks (e.g. cell phone use), they can mistakenly believe that they will be just as successful in related tasks (e.g. LBS app use).

Therefore, we explore another possible factor – derived from and inspired by e-commerce research – that might be playing a larger role in the app-adoption context: mobile-computing self-efficacy (MCSE). The conceptual roots of MCSE can be extrapolated from computer self-efficacy (CSE), which refers to a person's judgement of his or her ability to use a computer to accomplish a diverse range of computing tasks (Marakas *et al*., 1998; Compeau & Higgins, 1995b). A nascent conception of the MCSE construct itself is not new (Viosca *et al*., 2004; Grazioli & Jarvenpaa, 2003). However, MCSE has not yet been examined as a possibly misguided cause of information disclosure in this new arena of LBS-based mobile devices and apps.

Multiple theories have been used to explain consumer transactions with and subsequent information disclosure to e-commerce tools and apps (Li, 2012). We integrate MCSE into two of the dominant theoretical foundations used to explain e-commerce adoption and disclosure: 'trust theory' (Gefen *et al*., 2003) and 'privacy calculus' (Laufer & Wolfe, 1977). Researchers have often incorporated self-efficacy into these two theories in particular (e.g. Milne *et al*., 2009; Hsu *et al*., 2007). We extend these theories by explaining the effect of self-efficacy not only on the dependent variables (e.g. trusting behaviours and disclosure intentions) but also on the critical independent variables that determine disclosure outcomes. Namely, we predict that high-MCSE users tend to be more trusting of app providers and perceive fewer disclosure risks – despite having no way of accurately assessing the real risks.

To test these theories' perspectives, we executed two experiments involving two theoretical models: (1) a controlled simulation experiment of carefully manipulated LBS-based apps ($n = 509$) and (2) an experiment involving a real app with actual information disclosure ($n = 380$). Our results support the proposition that MCSE has a positive and direct effect on consumers' trusting beliefs regarding app vendors as well as a negative direct effect on the perceived privacy risk of information disclosure. Interestingly, although self-efficacy is known to affect behavioural intentions in information security contexts (e.g. Herath *et al*., 2014), our results indicate that MCSE's effect is entirely mediated when examining actual disclosure. We proceed next by conceptualising MCSE.

SOCIAL COGNITIVE THEORY AND SELF-EFFICACY

Social cognitive theory (SCT) is the theory from which self-efficacy as a theoretical construct is derived. As developed by Bandura (1977c, 1986, 1991, 2002), SCT is a learning and human-development theory that is based on the notion that three factors, (1) environment, (2) cognition and (3) behaviour, all play a role in the human development of personality and learning.

SCT posits that the concepts of vicarious learning, identification, self-regulation, self-reflection and self-efficacy increase learning and the human development of personality. SCT also posits that vicarious learning is particularly powerful when both identification and self-efficacy are high. 'Vicarious learning' is learning through observation of others. 'Identification' relates to how much one identifies with the model of behaviour on which the vicarious learning is based. 'Self-reflection' is the capability people have to introspectively understand their experiences and emotions, evaluate their cognitions and beliefs, and self-evaluate and alter their cognition

and behaviour as a result of this introspection (Nisbett & Wilson, 1977). Only through self-reflection is self-efficacy possible. According to Bandura (1986), 'self-efficacy beliefs' are 'people's judgments of their capabilities to organize and execute courses of action required to attain designated types of performances' (p. 391). Thus, individuals who exhibit 'self-efficacy' judge themselves as having the capability of performing in a certain manner to achieve a goal or influence events that affect their lives (Bandura, 1977c). Self-efficacy, in turn, affects behavioural change, which has been primarily operationalised in terms of individual human performance (Bandura, 1982).

Self-efficacy also plays a role in how individuals approach uncertainties, tasks and goals. Consequently, self-efficacy determines whether people will attempt a particular action, as well as how they will cope with the challenges that might arise as they undertake the action. SCT posits that self-efficacy is core to vicarious learning and to general growth and accomplishment. People will not persevere in tasks that are arduous, new, unknown and so forth, without self-efficacy. People tend to fear and avoid situations that they believe are beyond their self-efficacy to control and thus tend to perform activities that they judge themselves capable of handling (Bandura, 1977a). Self-efficacy thus also dictates the coping mechanisms individuals will utilise after they have begun a course of action. If they judge themselves capable of performing a task or achieving a goal, they will expend more effort in coping with the difficulties that arise after having begun the action (Bandura, 1977a, pg. 194).

As self-efficacy is only a 'belief' in individuals' abilities, it determines whether they will attempt an action, but not necessarily their success. Success also depends on an individual's actual competence, on the incentive to complete the action and on the actions of others (Bandura, 1977a). Consequently, individuals may develop over-confidence from misjudging the transfer of their success from prior actions to new situations where success is less certain and the actions of others are unknown (Hilary & Menzly, 2006; Moores & Chang, 2009).

Application of self-efficacy to mobile adoption and information disclosure

Based on the preceding section, SCT applies well to the question of why people disclose their location data and personal information to mobile-app vendors. When a potential consumer needs an app, the consumer has a goal and a set of actions required to obtain that goal. The goal is to obtain an app that will be both safe and useful in providing them with their desired information or entertainment. The action(s) required to reach that goal include searching through a limited option set in a given app platform and correctly evaluating the capabilities, risks and trustworthiness of the options until a ranking of the overall desirability of each app can be achieved. Extending SCT to our context requires that three outcomes should pertain to individuals with high self-efficacy: (1) they will spend more time and effort in the search and evaluation process for the app, (2) they will have a greater belief in the benefits of the app and (3) they will perceive lower risk and have greater trust in their app-selection decision.

The aforementioned assumptions also point to a potential problem with consumer self-efficacy: although individuals high in self-efficacy might be more confident in their decisions, their trust and risk perceptions are still based on asymmetrical information presented by the app vendor. The consumer has no way of actually verifying the integrity, benevolence

and competence of an unknown app provider beforehand. Recall that self-efficacy determines not only whether individuals will undertake an action but also the construal of their ability to cope with the uncertainties that might arise because of that course of action. As a result, high self-efficacy individuals will place greater trust in an app provider because they have increased confidence that they can circumnavigate the app's risks. However, this increased trust will backfire if the app provider is untrustworthy.

Mobile-computing self-efficacy

Given this theoretical background, we now further specify MCSE as a more targeted form of CSE because the mobile-computing market has evolved greatly in recent years. Consumer e-commerce and information systems research has drawn on SCT research focused on self-efficacy for a couple of decades in predicting a variety of system attitudes, usage and performance outcomes (Compeau & Higgins, 1995a; Compeau & Higgins, 1995b; Marakas *et al*., 1998; Compeau *et al*. 1999; Agarwal *et al*., 2000; Thompson *et al*., 2006; Marakas *et al*., 2007; Venkatesh & Bala, 2008). Research in this area primarily started with self-efficacy as adapted to computer use, a context known as CSE. Compeau and Higgins (1995b, p. 191) define CSE as 'an individual's perceptions of his or her ability to use computers in the accomplishment of a task … rather than reflecting simple component skills'. High-CSE users are more innovative in their use of information technology (IT) (Agarwal *et al*., 2000; Thompson *et al*., 2006) and have decreased technology anxiety (Compeau *et al*., 1999; Venkatesh & Davis, 2000; Venkatesh & Bala, 2008). This connection between self-efficacy and the willingness to adopt new technologies early and to find innovative uses for new technologies holds in other computing contexts, such as the internet and mobile computing (Wang *et al*., 2006; Wang *et al*., 2008).

Hardin *et al*. (2008), following Marakas *et al*. (1998), stress the importance of developing unique self-efficacy constructs for different computing contexts. For example, with the internet revolution came the new construct of 'internet self-efficacy' (Hsu & Chiu, 2004, p. 369). This is an important distinction, because navigating Web-based interfaces requires a skill set beyond simple computer use. For these reasons, MCSE also needs a clear distinction from CSE (Wang *et al*., 2006; Wang *et al*., 2008). Several technologies – cell phones, global positioning system, wireless internet and personal digital assistants (PDAs) – have converged in mobile devices such that new use patterns and threats have emerged. Using mobile-device features requires a different skill set than that needed for Web-based apps. As a result, having high internet self-efficacy, or CSE, does not necessarily translate to high MCSE.

Mobile and desktop apps differ in terms of dexterity, facilitation of focus and location-based functionality. Dexterity is the ability to accomplish tasks using one's hands (Bernstein, 1996). In an app environment, the completion of tasks is far more cumbersome because of the limited nature of the input devices (input controls tend to be closer, making input stressful and error prone). Because mobile devices accept input from touchscreens, accelerometers and gravity sensors, the skills needed to navigate differ from those in Web-based environments that tend to use a mouse and keyboard. Focus refers to the 'centering of attention on a limited stimulus field' (Csikszentmihalyi, 1977, pg. 40). Because websites tend to use larger display areas, they

can facilitate far more contextual information than apps can. Also, because website interfaces tend to be stationary, it allows websites to facilitate far better focus than apps, requiring less cognitive effort to complete tasks (Chae & Kim, 2004). Finally, apps can make use of LBS, providing functionality beyond that which websites can facilitate (turn-by-turn directions in real time, for example). Using these functions requires additional skills beyond those needed for using Web-based apps. The MCSE construct emerges as a better way of understanding computing self-efficacy in relation to the attitudes and usage patterns of today's mobile-device users.

MCSE and control

Regarding its effect on perceived privacy risk, MCSE is somewhat similar to the concept of 'control' as it is used in the privacy literature (Laufer & Wolfe, 1977; Culnan, 1993; Smith *et al*., 1996). Privacy is often referred to as people's ability to control the information available about themselves (Belanger & Crossler, 2011). Research has demonstrated paradoxical behaviours when consumers believe they have control over their personal information (Brandimarte *et al*., 2009). In particular, when consumers self-disclose (as opposed to having third parties disclose their information), their privacy concerns are lowered, even when the exposure of that information increases or is outside of their control (Brandimarte *et al*., 2009; Brandimarte *et al*., 2013;) – thus exhibiting an 'illusion' of control rather than actual control.

In some sense, control may be conceptualised as a targeted form of self-efficacy specifically concerning consumers' ability to control the information available about themselves. However, control and MCSE are not entirely the same. Although control is a belief in one's ability to determine the amount of and extent to which information will be available about oneself (Dinev *et al*., 2013), MCSE is one's belief in one's ability to effectively use mobile devices. Control is heavily influenced by actual privacy control settings available to the consumer through the mobile-device or e-commerce channel (Dinev *et al*., 2013). Alternatively, MCSE exists independently of the availability of privacy controls. In the following section, we predict a positive influence of MCSE on trusting beliefs and a negative influence of MCSE on perceived privacy risks. These predictions are parallel to similar predictions and findings from control theory in which consumers form unwarranted beliefs in their ability to control the information they self-disclose (Brandimarte *et al*., 2009).

THEORETICAL MODELS

Li (2012) provides a thorough review of the theories used to explain online privacy decisions. Of these theories, 'privacy calculus' (Laufer & Wolfe, 1977; Dinev *et al*., 2006) has evolved as the dominant perspective when examining not only general privacy concerns but also a consumer's perceived privacy risk with a specific technology or transaction and their subsequent information-disclosure intentions (e.g. Dinev & Hart, 2006; Dinev *et al*., 2006; Junglas *et al*., 2008; Krasnova *et al*., 2010; Xu *et al*., 2010; Fife & Orjuela, 2012; Keith *et al*., 2013). Moreover, there is evidence that self-efficacy may affect context-specific privacy risk perceptions (Kim & Kim, 2005). Therefore, we adopt privacy calculus as one of our two theoretical lenses.

However, trust theory (McKnight *et al*., 2002; Gefen *et al*., 2003) has also been prominently used to explain transaction decisions under uncertainty. Indeed, trusting beliefs in a transaction partner are one of the important covariates when forming information-disclosure intentions (Dinev & Hart, 2006) and are influenced by self-efficacy (Kim & Kim, 2005). Therefore, we also theorise the effects of self-efficacy on trusting beliefs. However, the purpose of our manuscript is not to create a new combined model of information disclosure but to demonstrate the role of MCSE in terms of both of these theoretical perspectives. Consequently, rather than combining the privacy calculus and trust models, we examine the effect of self-efficacy separately within each theory. Examining multiple theories to explain a phenomenon is a common practice when a phenomenon can inform or be informed by multiple perspectives (e.g. Mathieson, 1991). Indeed, Acquisti and Grossklags (2003) offer a variety of theoretical explanations – in addition to the privacy calculus perspective – of consumer disclosure behaviour. In the present case, we are not comparing which theoretical perspective is 'best' but rather demonstrating the role of MCSE across two of the dominant perspectives in which self-efficacy plays an important role (Kim & Kim, 2005).

Trusting beliefs

Issues related to consumer trust have increased in prominence with the advent of e-commerce, and with the use of IT as a mediator between buyers and sellers who had previously, and traditionally, interacted face-to-face (McKnight *et al*., 2002; Gefen *et al*., 2003). In many ways, e-commerce has effectively eliminated the social cues and interpersonal interactions that had traditionally enabled consumers to overcome perceived risk and uncertainty in transacting with particular sellers. Consequently, if the new Web vendors did not already have social or brand capital (Lowry *et al*., 2008), they had to find alternative ways to convince potential consumers of their trustworthiness. Such persuasion attempts have been, for example, through the use of privacy and security seals (Bélanger *et al*., 2002; Kim *et al*., 2008; Xu *et al*., 2010; Lowry *et al*., 2012) and high-quality and intuitive websites with attractive interfaces (McKnight *et al*., 2002; Gefen *et al*., 2003; Lowry *et al*., 2008) including logos (Lowry *et al*., 2014), mobile websites (Vance *et al*., 2008) and convincing consumer reviews (Forman *et al*., 2008).

As research into online consumer trust developed, several distinct trust constructs emerged that are relevant to our study: (1) initial trusting beliefs, (2) trusting intentions and behaviours, (3) disposition to trust and (4) institution-based trust (McKnight *et al*., 2002; Gefen *et al*., 2003; Lowry *et al*., 2014). 'Initial trusting beliefs' refer to the trust a potential trustee has in a particular vendor before any transaction occurs (McKnight *et al*., 2002). This is relevant to apps, because although many apps are associated with recognisable brands, the majority are not (Reed, 2011), and initial adoption of smartphones is widespread and growing. These trusting beliefs lead to 'trusting intentions' and 'trusting behaviours', which, in the app context, refer to the consumer's intention to purchase, download and subsequently use the app provided by a particular vendor (McKnight *et al*., 2002; Gefen *et al*., 2003). In the LBS context, intent also means the consumer intends to disclose his or her location data and personal information to the vendor (Xu *et al*., 2010). 'Institution-based trust' refers to a user's trust in the larger environment – for example, the internet, in the case of e-commerce; an app platform (Apple

app store, Android, Windows mobile, etc.); or a qualified third party who will provide security and privacy assurances. Institution-based trust is determined, in part, by 'structural assurances', which are mechanisms designed to convince the consumer of the trustworthiness of the transaction environment (Pavlou, 2002; Pavlou & Gefen, 2004). Lastly, 'disposition to trust' refers to a consumer's predisposition toward trusting others in general, and this predisposition can also influence their willingness to trust the structural assurances upon which institution-based trust is based (McKnight *et al*., 2002).

Figure 1 outlines our first theoretical model: as the positive effect moving from trusting beliefs to trusting intentions to trusting behaviours is well established (McKnight *et al*., 2002; Ba & Pavlou, 2002; Gefen *et al*., 2003; Komiak & Benbasat, 2006; Lowry *et al*., 2008; Li *et al*., 2008; Lowry *et al*., 2014; Moody *et al*., 2014), we use trusting beliefs as our primary dependent variable, as used in other studies (Wang & Benbasat, 2007; Wang & Benbasat, 2005), and we also incorporate elements of institution-based trust and control for the consumer's disposition to trust. To clarify, this theoretical model is built on the foundational trust theory from the e-commerce literature, where trusting beliefs result from structural assurances and disposition to trust (McKnight *et al*., 2002; Gefen *et al*., 2003). Consequently, we do not formally hypothesise those relationships in our model. Our contribution to the underlying model is to extend it to include SCT and specifically the construct of self-efficacy. We explain why high levels of self-efficacy can cause LBS users to be more trusting – regardless of the actual ethics and intentions of the LBS provider – and thus to take more privacy risks in using LBS-based apps than they would do otherwise.

Privacy calculus

A more recently favoured theory used to explain information disclosure over mobile devices is 'privacy calculus' in the e-commerce (Laufer & Wolfe, 1977; Dinev & Hart, 2006) and mobile-phone commerce (m-commerce) (Xu *et al*., 2010) contexts. Privacy calculus is based on the rational

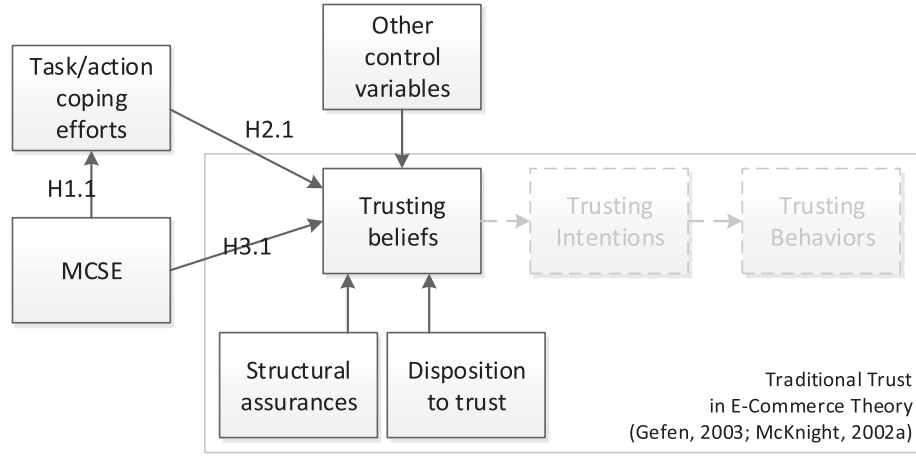


Figure 1. Trust model.

calculated trade-off between the consumer's perceived risks and benefits of disclosing information over an e-commerce channel or, in this case, a mobile app.

Although it has been found to be insignificant in some mobile-app studies (Xu *et al*., 2010; Keith *et al*., 2010; Keith *et al*., 2013), 'privacy concern' is a theoretical control variable that influences both the perceived risks and disclosure intentions of consumers. Privacy concern refers to the consumers' beliefs about the safety of mobile apps and information disclosure in general. These feelings are not related to a specific mobile app.

Traditionally, privacy calculus (Figure 2) has only been used to explain disclosure 'intentions'. This is because privacy calculus is based, in part, on the theory of reasoned action, stating that behavioural intentions lead to actual behaviours (Ajzen, 1991). However, research on the 'privacy paradox' suggests that when it comes to information disclosure, intentions are a poor indicator of actual behaviour (Acquisti & Grossklags, 2004). Therefore, in our adapted model of privacy calculus, we forgo the 'disclosure intentions' construct and relate each of our independent variables directly to actual disclosure behaviours.

Hypotheses

As the primary relationships of trust theory and privacy calculus have already been established in the e-commerce literature (Dinev & Hart, 2006), we only formulate specific hypotheses concerning the role of MCSE in each of these models. Only limited research into trust theory and privacy exists in the mobile context, and findings generally indicate that trust still represents a driver of use intention and behaviour in the mobile context.

Although research into MCSE is limited, there is relevant literature on self-efficacy, which can support SCT-based hypotheses in the MCSE context. When adopting a new technology, consumers are faced with uncertainty about the potential risk to both their information assets and their ability to continue their information-processing activities. Based on SCT, high-MCSE consumers are more likely to engage in coping behaviours if any uncertainty exists about which of the potential apps is the most useful and trustworthy. In contrast, consumers with low self-efficacy allow uncertainty to cloud their behaviour and decision-making processes. The

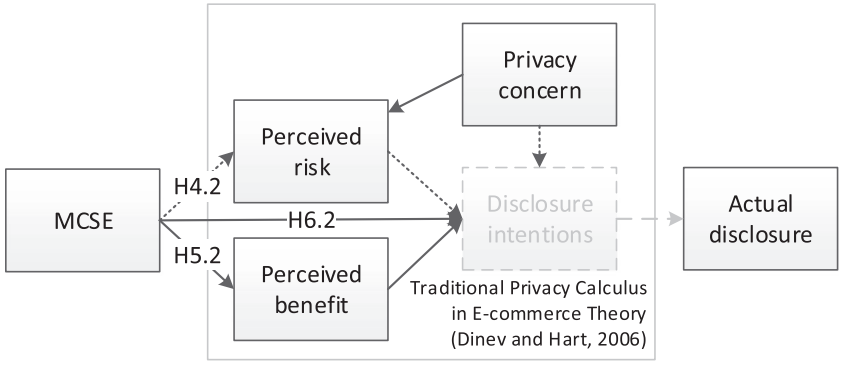


Figure 2. Privacy calculus model.

term 'coping behaviours' characterise the actions and efforts taken by individuals to overcome obstacles, solve problems or mitigate threats (Bandura, 1977b). Coping behaviours are a natural result of self-efficacy because they demonstrate consumers' confidence that they can address uncertainty. In addition, coping mechanisms could include seeking risk information through privacy seals. Similarly, in other studies, self-efficacy has been demonstrated to positively influence risk information seeking in a variety of contexts, from industrial waste risks (Ter Huurne & Gutteling, 2008) to human health risks. As a result, we hypothesise the following:

H1: (Trust model) MCSE has a positive direct effect on the coping efforts made by consumers in the app-adoption process.

By reducing risk perceptions, coping actions will reinforce an individual's trust in the technology that he or she is considering adopting (Serino *et al*., 2005). In other words, not only will high self-efficacy individuals engage in more coping efforts, but they are more likely to believe that their coping behaviours will lead to a desired outcome because the actions were implemented to succeed in the first place (Bandura, 1977a). For example, in 1999, when individuals were faced with the 'Y2K bug' scare, those who implemented coping efforts expected significantly lower damage as a result (Aspinwall *et al*., 2005). Other research has demonstrated that a strong positive correlation exists between coping behaviours (in various forms), interpersonal trust (Grace & Schill, 1986) and reduced stress (Krohne, 1989). In summary, we hypothesise the following:

H2: (Trust model) Consumers' coping efforts during the app-adoption process have a positive direct effect on their trusting beliefs in an app provider.

In addition to affecting perceived trust through coping behaviours, perceived self-efficacy also has a direct effect on trusting beliefs. Prior research has identified a relationship between the self-efficacy of entrepreneurs and what they termed 'over-trust'. Over-trust does not refer to blind trust, but instead to an 'unwillingness to … take into account the potential risk involved in a relationship or an inability to assess the intentions of the other party' (Goel & Karri, 2006, pg. 480). They proposed that because entrepreneurs with greater self-efficacy have higher levels of aspiration, goal commitment, task persistence and work attitudes, they will have a higher perceived ability to control the behaviour of people they trust, and therefore, they are more likely to over-trust. Accordingly, in electronic health records research, one study found that nurses with lower self-efficacy were less likely to trust the confidentiality of electronic records (Lending & Dillon, 2007). Similarly, individuals with high self-efficacy placed much greater trust in the government's and industry's ability to help protect them from harm and natural disaster (ter Huurne & Gutteling, 2009). Other studies have shown similar findings in relationships between various forms of self-efficacy and identification-based trust (Hsu *et al*., 2007), trust in decision-support systems (Madhavan & Phillips, 2010) and risky decision-making (Heath & Tversky, 1991). High self-efficacy individuals view risks as opportunities, whereas low self-efficacy individuals view them as threats (Krueger & Dickson, 1994), because high self-efficacy individuals believe they can overcome threats through their skills (Bandura, 1977a).

Some consumer research on e-commerce has also supported the relationship between self-efficacy and trusting behaviours and beliefs. For example, consumers with high CSE are less likely to avoid risky online shopping (Milne *et al*., 2009). In what is possibly the most relevant study to our model, Luo *et al*. (2010) found a strong positive correlation between self-efficacy and trusting beliefs in m-commerce, although this relationship was not formally hypothesised. Therefore, assuming that our theory and these reviewed findings should also hold in a mobile-computing context, we hypothesise a positive relationship between MCSE and trusting beliefs in app vendors:

H3: (Trust model) MCSE has a positive direct effect on consumers' trusting beliefs in their chosen app provider.

H4: (Privacy calculus model) MCSE has a negative direct effect on consumers' perceived risk of mobile-app adoption.

As discussed, if individuals judge themselves capable of performing a task or achieving a goal, they will expend more effort in coping with the difficulties that arise after having begun the action in order to ensure they have achieved the goal (Bandura, 1977a, pg. 194). As a result, if high-MCSE consumers need an app to help them find the best local restaurant, they will expend greater effort to understand the advantages and capabilities of each app, leading them to a greater belief in the competency of the app. This effect has been identified previously in that high-CSE users have a greater belief in the ease of use and usefulness of the computer systems they use to perform common work tasks. Thus,

H5: (Privacy calculus model) MCSE has a positive direct effect on consumers' perceived benefits of mobile-app adoption.

In recent years, the disclosure intentions construct has been criticised and demonstrated to be an unreliable indicator of actual disclosure behaviour (Acquisti & Grossklags, 2004; Acquisti & Grossklags, 2005; Keith *et al*., 2013). Consequently, rather than investigate the effects of MCSE on information-disclosure intentions, we forgo intentions and hypothesise the effect directly on actual information disclosure.

Information disclosure has been tied to self-efficacy in a number of other contexts. Kalichman and Nachimson (1999) linked self-efficacy to disclosure of personal health information, whereas Wei *et al*. (2005) linked social self-efficacy to emotional self-disclosure among college freshmen. In both cases, the authors demonstrated that individuals who suffer from low self-efficacy experience increased anxiety during interactions with others and this anxiety leads them to avoid disclosure of their human immunodeficiency virus status (Kalichman & Nachimson, 1999) and to have feelings of depression (Wei *et al*., 2005). In psychology contexts, the anxiety tends to be about the uncertainty of the risk of others forming a negative opinion about the subject and the subsequent uncertainty related to future social interaction.

Hauser *et al*. (2012) used both CSE and anxiety as predictors of success in the performance of computer-related tasks by students in a junior-level management information system course, in both an online and face-to-face environment. In a commerce context, the uncertainty that causes anxiety is not associated with personal relationships, but rather the possibility that the information might be used opportunistically by the other party in such a way that is damaging to the subject (Serino *et al*., 2005). Self-efficacy is a well-documented control variable in studies of technology adoption.

Self-efficacy has also been shown to influence a variety of computing outcomes in multiple contexts. For example, it has a direct effect on consumer intentions to use mobile technology, gathering information and making e-commerce purchases (Pavlou & Fygenson, 2006) and is one of the core concepts of the technology acceptance model (Venkatesh *et al*., 2003).

We predict that the relationships between self-efficacy and information disclosure will hold in the mobile context as well, because those who rate themselves highly in MCSE will experience less anxiety about the potential opportunistic use of their location information – Compeau and Higgins (1995b) identify a negative relationship between CSE and computer anxiety – and will be more likely to permit the disclosure of that information.

H6: (Privacy calculus model) MCSE has a positive direct effect on consumers' actual information disclosure.

METHODOLOGIES

To test our hypotheses, two experiments were performed that separately tested our two theoretical models. Study 1 tested the hypotheses related to the trust model, while Study 2 tested the hypotheses in the privacy calculus model.

Study 1 methodology

Study 1 involved a simulation experiment as used in similar studies of trust involving mobile devices (e.g. Vance *et al*., 2008). To improve the generalisability of the results, we simulated four different LBS-based apps. Because MCSE is an individual factor that cannot be manipulated, we chose rather to manipulate three types of structural assurance (i.e. privacy seals and promises) across the apps, which are common in e-commerce settings. Structural assurance is a key component of institution-based trust (McKnight *et al*., 2002) and a traditional antecedent examined in prior research. This manipulation allowed us to compare the effects of structural assurances to MCSE.

College students were used as participants because the largest demographic block of mobile internet users is those of ages 18–29 years (Rainie, 2010) and because college students have been shown to be excellent candidates for mobile-technology studies (e.g. Pedersen, 2005; Xu *et al*., 2010). Participants were recruited from the business colleges at three large public universities, located in Virginia, Texas and Arizona. At those universities, 509 undergraduate and graduate students successfully completed the experiment, which took place outside of regular class time. They were offered extra credit, as well as a chance to win one of several $50 gift

cards. The 509 participants represent a 55% response rate of those who were solicited to complete the experiment. Table 1 summarises the demographics.

Study 1 tool, task and procedures

We selected Apple iPhone apps as the LBS of interest. Based on a pilot test of 26 participants, we selected four different iPhone app scenarios from the iPhone app store that reflected a variety of the salient uses of LBS apps: (1) an app that gave real-time updates on traffic congestion along commonly used roads and highways; (2) an app that allowed users to map their fitness routes for running, biking and so forth and to record their times; (3) an app that located friends and family members on a map; and (4) an app that mapped and located registered sex offenders in a user's area. These apps do not represent variations in the independent variables but rather offer a range of contexts to reduce the variance attributed to any un-captured context-dependent variables. Such a scenario approach has been effectively used previously in the LBS privacy literature (e.g. Xu, 2010; e.g. Xu *et al*., 2010) and in other mobile contexts (Vance *et al*., 2008).

Each participant worked individually and took as much time as was needed. Most participants spent between 15 and 25 min on the task. The experiment involved five steps, which are summarised in Supporting Information Appendix 3, together with the detailed scenarios. Consistent with prior mobile simulations (Vance *et al*., 2008), each participant answered a set of pre-test questions (including their MCSE), then followed a simulation of app screenshots involving the search, discovery and selection of an app to meet their needs and then answered a set of post-test questions.

Study 1 measures

Mobile-computing self-efficacy

Marakas *et al*. (2007) posited CSE as a formative measure because the indicators can vary independently from each other. However, it has since been argued that CSE is actually better modelled as reflective, because the underlying self-efficacy construct represents a complex psychological process that guides human action (Hardin *et al*., 2008). In other words, although the CSE indicators might vary independently from each other, they are still a reflection of an underlying psychological construct that is best measured as reflective and validated using techniques appropriate for reflective items. Hardin *et al*. (2008) also contend that the decision to model CSE as formative, vs. reflective, represents a trade-off between explanatory power and generalisability. As our purpose was to establish a generalisable link between self-efficacy

Table 1. Demographic statistics

Mobile purchases (last year)	7.10 $\bar{x}$ (22.907σ)
Age	21.81 $\bar{x}$ (5.18σ)
Smartphone user	52.1%
Apple iPhone user	18.5%
Gender (male/female)	55.0%/45.0%

and trusting beliefs, and not necessarily to find the greatest possible explanatory power, we modelled MCSE as a reflective construct. Doing so also allowed us to better represent how the measurement items were developed for this study (Hardin *et al*., 2008).

Many CSE researchers agree that CSE-based constructs should be developed uniquely to each context they are measured in, which greatly improves validity and explanatory power, as compared with more general attempts at measuring self-efficacy. Therefore, because of the rapid emergence of smartphone technologies, we developed a new measure for MCSE, even though one had been previously proposed (Wang *et al*., 2008). To develop the MCSE items, we moderated an open-panel discussion with 32 undergraduate and graduate college students who were offered extra credit. Just over half of these students were existing smartphone users. We based the discussion topic on the posed question, 'What kinds of skills do competent smartphone users have which less competent users do not have?' A large list was developed, containing over 20 responses. We then revised the list to combine sets of similar skills into single topics.[1] We then asked the participants to rank order the top four skills[2] that represented 'competent smartphone users'. The resulting top four skills, based on the sum total of all responses, were pilot tested, along with all other measurement items, with 26 participants, other than the 32 used to derive the items. All four items were retained and represented the skills of making purchases using a mobile device, correcting common problems, adding and removing features and apps and effectively using the apps, and were not specific to LBS. All measurement items are contained in Supporting Information Appendix 1.

Structural assurance

As stated, structural assurance was manipulated in the experimental design. In particular, the app description was manipulated to include (1) no privacy or security assurance ('no assurance' condition), (2) a BBB seal only ('low assurance' condition) or (3) a BBB seal, a VeriSign seal and a written privacy promise ('high assurance' condition). Consequently, the measure for structural assurance is a dummy code, representing which of the three structural assurance conditions the participant was randomly assigned to during the simulation. Figure 3 illustrates these manipulations.

Coping efforts

Carver *et al*. (1989) identified several theoretically based coping efforts. We measure two of them that are particularly relevant to our context and experimental design: (1) active coping and (2) seeking social support. 'Active coping' refers to the active steps taken to 'remove or circumvent the stressor or … its effects' (p. 268). Active coping takes place during the task execution (e.g. searching for the most trustworthy app) and includes increasing one's efforts in a stepwise fashion. In our context, participants who are more actively involved in the search

[1]For example, two of the skills included 'being able to buy songs and movies' and 'being able to buy apps'. These were combined into 'being able to make purchases'.
[2]Because the purpose of this study was not to generate an exhaustive MCSE scale (e.g. Wang *et al*., 2008), and because our data collection includes many other constructs in addition to MCSE, only the top four skills were included in order to minimise the cognitive load on participants.

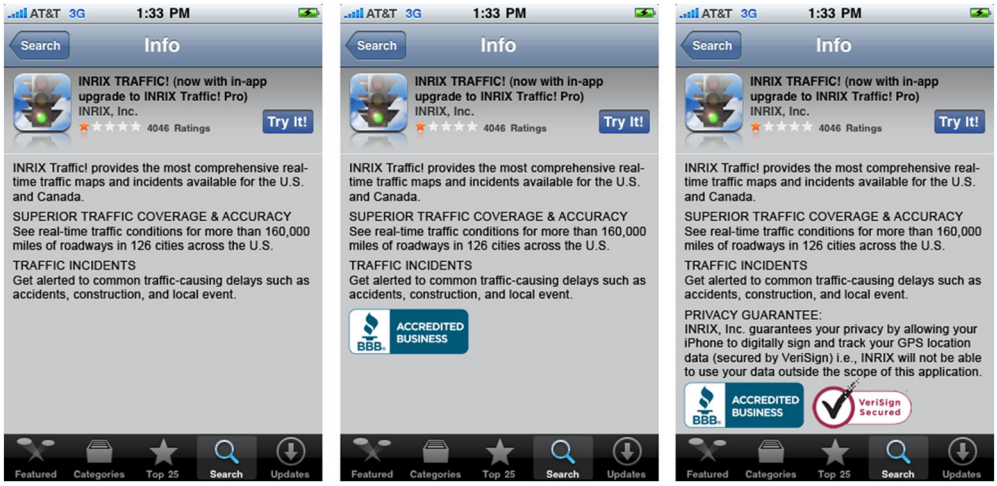


Figure 3. Structural assurance manipulations.

process will pay greater attention to the trust-assuring cues (i.e. privacy seals) and apply more effort to reading the actual written privacy promise. Therefore, we measured active coping efforts based on their ability to recall each of the three structural assurances correctly: (1) BBB seal, (2) VeriSign seal and (3) privacy promise. The resulting formative measure is labelled 'recalled assurances correctly' in Figure 3. Clearly, this measure would be influenced by each participant's capability in terms of working memory. Therefore, to minimise this error, we allowed participants to return to their manipulated app description if they so desired. However, answering these questions correctly was not a requirement of the experiment. As a result, those who were actively coping (i.e. high-MCSE participants), yet poor in memory capabilities, would be more likely to return to the app description, thus minimising the potential error variance due to individual differences in memory capability.

'Seeking support' refers to the process of 'seeking advice, assistance, or information' (Carver *et al*., 1989, pg. 269) in order to reduce, remove or circumvent a stressor. We operationalised active coping efforts as seeking privacy assurance cues, which is conceptually quite similar to 'seeking support'. However, support seeking is distinguishable because it involves seeking information from a potentially objective third party. To replicate this, the experimental interface offered a 'What's this?' link placed on the simulation Web page next to the BBB seal and not within the app itself (Supporting Information Appendix 3). If the user clicked the link, a pop-up window opened that gave the BBB's actual self-description of what its seal means, with minor adaptations for the app context. The resulting variable had a binary value of 0 or 1, depending on whether or not they clicked the BBB link. While prior knowledge concerning BBB seals may lead some high-MCSE participants not to click the link, it would be expected that participants with lower MCSE would be less inclined to click.

The resulting measure of coping efforts is a formative construct consisting of the degree to which participants 'recalled assurances correctly' as well as whether or not the BBB seal was clicked (labelled 'BBB clicked').

Trusting beliefs and disposition to trust app vendors

Both trusting beliefs and disposition to trust were modelled as second-order formative constructs, composed of first-order reflective constructs, consistent with similar studies. Based on the work of McKnight *et al*. (2002), 'trusting beliefs' include three reflective sub-constructs, (1) competence, (2) benevolence and (3) integrity; while 'disposition to trust' includes the three reflective sub-constructs, (1) benevolence, (2) integrity and (3) trusting stance.

Following prior studies on trusting beliefs (Wang & Benbasat, 2005; Vance *et al*., 2008), we first analysed the measurement properties of the reflective sub-construct and then replaced the first-order reflective constructs with their latent factor scores, allowing us to test the second-order formative construct validity and analyse the structural paths.

Controls

Several controls were also included, many of which were found to be relevant in similar studies (Xu *et al*., 2010; Hui *et al*., 2007). Typical demographic variables, including age and gender, were measured. A control for the context of the app was included as a predictor of each variable. Participants were also asked if they currently used a smartphone or other mobile device (e.g. iPod touch or PDA) capable of downloading and installing apps. They were also asked to indicate the number of transactions they had made in the last year over a mobile device (indicating their m-commerce experience) and how many times their information had been misused as a result of any e-commerce transaction (an indicator of the trust experience).

Study 2 methodology

Study 2 was an experiment designed to have participants evaluate and test a real forthcoming mobile app in 'beta' stage and then decide (1) whether to register to use the app in the future and (2) how much of their personal profile information to complete. Participants ($n = 380$) were again drawn from college students, but the group also included a snowball sample of friends and relatives over the age of 30 years (representing about 40% of the sample). Snowball sampling was used to find people who had an innate interest in and motivation for using apps, as opposed to artificial motivations typical in experimental studies. The students were offered extra credit for their participation and their recruitment of participants over 30 years old, which allowed us to obtain a more generalisable sample. Additionally, because of the social networking nature of the experiment app, we asked participants to specifically refer friends or family members who would be interested in the type of app they were evaluating. As a control, we required that their referral live no closer than five miles from campus (to prevent roommates from participating as though they were family members over 30 years old). As the mobile app used in the experiment gathered location data, we verified that the participants referred by students retained in our sample completed the experiment no closer than five miles from campus.

Study 2 tool, task and procedures

To ensure our model was tested rigorously and to increase the likelihood of generalisable results, participants were recruited under the misleading pretence that they were needed to help analyse

and test a new mobile app being readied for market. With institutional review board approval, participants were led to believe an app called 'Sharing Tree' (which was created by the researchers for this experiment) was a production app and that the researchers had been hired to help perform market research and testing prior to its release. Participants were told that in return for their participation, they would be given the opportunity to continue using the app for free after it reached the market but they must become registered users immediately. However, their only mandatory requirement was to evaluate it in trial mode, which did not require registration. As a result, we were able to analyse 'initial' information disclosure for those who registered willingly.

Rather than create an iPhone-specific app (as in Study 1), this prototype HTML5-based mobile app was formatted to fit and adjust to the majority of mobile-device screen sizes. This app was designed to incorporate some of the major benefits and privacy risks commonly found in most LBS apps, including location-sensitivity, social networking, financial and personal data. The stated purpose of the app was to allow users to share local shopping deals, gas prices, activities or other interests with friends and family in the user's area. For example, if users were to find a great deal on clothing from the local Gap retail store, they could share that information only with their intended friends and family members before the limited stock ran out. In addition, this app would not include advertisements or sponsored locations, so that all shared data would be relevant and based on the word-of-mouth recommendations of those they care about. Figure 4 summarises the screenshots of this app.

Sharing Tree's LBS allowed users to view a map of their current location with markers of useful sites generated by friends and family members. The list of friends and family members in the user's social network could be imported automatically from Facebook. In addition to storing the user's social network, Sharing Tree also allows the user to store credit card information to pay for shopping deals available online. Furthermore, the user could store detailed profile information, which would allow the app to suggest personally relevant points of interest in the user's local area. The app included a settings screen that allowed the user to specify four 'on' or 'off' privacy settings: (1) use of the app's LBS, (2) location data sharing, (3) storage of credit card data and (4) sharing the user's profile with 'anyone', 'friends only' or 'nobody'. To facilitate the participant's review of the app, we created an online survey and specific instructions to capture the user's overall perceptions of the app. The specific participant steps are detailed in Supporting Information Appendix 3, while an explanation of manipulation checks is in Supporting Information Appendix 2.

Study 2 measures

MCSE was measured using the same items developed for Study 1. Privacy concern, perceived benefits (Xu *et al*., 2010) and perceived risks (Keith *et al*., 2010) were adapted from prior research with minor modifications. Perceived privacy risks were expanded for this study to include both privacy risks to location data (three items) and risks to personal information (three items). Similarly, items measuring perceived benefits were modelled to include both personalisation-based and locatability-based benefits (Xu *et al*., 2010). As a result, perceived privacy risks and perceived benefits were each modelled as second-order formative constructs with first-order reflective sub-constructs, similar to research on trust with mobile commerce (Vance *et al*., 2008).

Two variables were measured and combined into a single dependent variable labelled 'disclosure'. First, we captured a true/false value representing the participant's decision to

Figure 4. Screenshots of Sharing Tree app.

disclose each type of registration information (email address, password, first name, last name, home address, phone number, level of education, employment experience, age, gender, ethnicity, marital status and income). However, it is easy to falsify these data. Therefore, when the data collection was finished, participants were awarded extra credit before informing them that the app was fake and that they had participated in a research study. The second variable measured involved asking the participants to indicate the percent of information they had entered that was accurate. This percentage was multiplied by the percent of profile data disclosed to form our dependent variable. Lastly, the app privacy settings selected by the participants were captured as a control variable.

ANALYSES AND RESULTS OF STUDIES 1 AND 2

Study 1 results

Measurement model

Extensive analyses were performed to determine if the constructs were formative or reflective, to examine the convergent and discriminant validity of the reflective measures, to ensure that multicollinearity was not a problem, to establish strong reliabilities and to check for common-method bias, using the latest techniques appropriate to both formative and reflective constructs. All of these detailed analyses are available in Supporting Information Appendix 2. The results of our factor validity procedures, checks for multicollinearity, reliability checks and tests for common-method bias show that our models meet or exceed the validation standards expected in similar research (Straub *et al*., 2004) and particularly for partial least squares (PLS) analysis (Gefen & Straub 2005; Lowry & Gaskin, 2014). In addition, our experimental design included checks that confirmed that our experimental manipulations were valid (also in Supporting Information Appendix 2).

Hypothesis testing

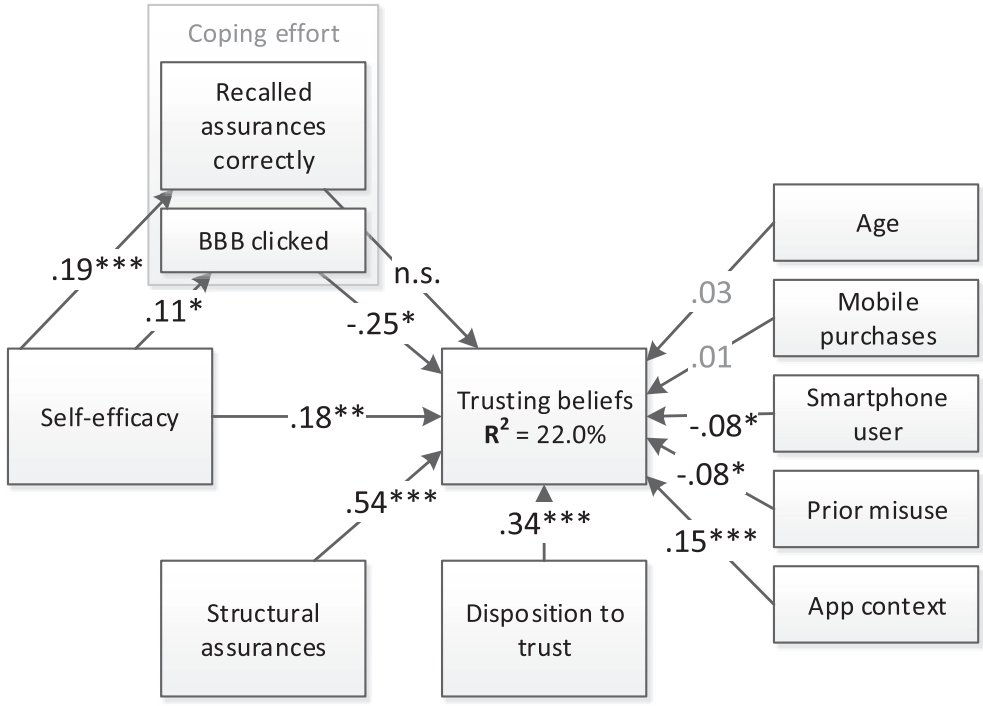
After confirming the validity of the data and that our manipulations indeed followed our underlying theory, we analysed the path model with a PLS structural equation modelling (SEM) technique using SmartPLS 2.0.M3 (Ringle *et al*., 2005). PLS is appropriate because it is an effective technique for early theory development; it does not depend on normal distributions and interval scales (Fornell & Bookstein, 1982; Lowry & Gaskin, 2014; Chin *et al*., 2003), making it better for incorporating our control variables and structural assurance construct; and because we used formative trust constructs (Gefen *et al*., 2000). It is also useful for analysing complex mixed models with formative and reflective measures (Lowry *et al*., 2009; Chin *et al*., 2003). All items were standardised, and the product-indicator approach was used for measuring the exploratory interaction effects (Chin *et al*., 2003).

Figure 5 summarises the testing of the theoretical paths in the model for each study. The betas (βs) are indicated on the paths between two constructs, along with their direction and significance. The significance of the path estimates was calculated using a bootstrap technique with 500 resamples. The explanatory power of the model was assessed through the R^2 scores (i.e. the amount of variance accounted for) and the latent variable paths. Table 2 summarises the measurement model statistics. Table 3 summarises the hypotheses, the path coefficients and the *t*-values for each path. We also explored the use of five covariates against trusting beliefs (participants' age, smartphone usage, mobile purchases, prior information misuse and the app context they were randomly assigned to), which are also accounted for in these results.

Study 2 results

Study 2 measurement model

As with Study 1, the detailed analyses of the measurement validity are available in Supporting Information Appendix 2. No significant violations of convergent validity, discriminant validity or common methods bias were found in Study 2.



Note: *** p < 0.001, ** p < 0.01, * p < 0.05

Figure 5. Summary of hypothesis testing for Study 1.

Table 2. Measurement model statistics

Construct	Mean	SD	(1)	(2)	(3)	(4)	(5)
Mobile self-efficacy (1)	5.10	1.51	–	–	–	–	–
Trusting beliefs (2)	4.33	1.40	0.11	–	–	–	–
Disposition to trust (3)	4.36	1.40	0.21	0.35	–	–	–
BBB clicked (4)	12.4%	0.33	0.11	−0.03	0.03	–	–
Structural assurances (5)	(n/a)	(n/a)	−0.01	0.21	−0.00	−0.12	–
Recalled assurances correctly (6)	80.1%	0.43	0.19	0.07	0.01	0.03	0.09

SD, standard deviation; BBB, Better Business Bureau; n/a, not applicable.

Study 2 hypothesis testing

For similar reasons as Study 1, we analysed the path model with a PLS SEM technique using SmartPLS 2.0.M3 (Ringle *et al*., 2005). In particular, our measure of actual disclosure violates the Shapiro–Wilk test of normality, making PLS more appropriate than covariance-based SEM (Fornell & Bookstein 1982). In addition, the measures of perceived risk and benefit are both second-order formative constructs, which are better analysed by PLS SEM, as noted. All items were standardised, and the product-indicator approach was used for measuring the exploratory interaction effects.

Table 3. Summary of tested paths

Tested paths	Path coefficient (β)	*t*-value	Supports model?
Hypotheses			
H3. MCSE ➔ trusting beliefs	0.175	2.84**	Yes
H1. MCSE ➔ BBB clicked	0.105	1.69*	Yes
H1. MCSE ➔ recalled assurances correctly	0.190	3.51***	Yes
H2. BBB clicked (coping efforts) ➔ trusting beliefs	−0.247	2.11*	No
H2. Recalled assurances correctly ➔ trusting beliefs	0.101	1.43	No
Other relationships of interest			
MCSE * structural assurances ➔ trusting beliefs	−0.463	2.63**	(n/a)
Structural assurances ➔ trusting beliefs	0.536	3.45***	(n/a)
Disposition to trust ➔ trusting beliefs	0.343	8.00***	(n/a)
Age ➔ trusting beliefs	0.032	0.90	(n/a)
Smartphone user ➔trusting beliefs	−0.084	2.38**	(n/a)
Prior misuse ➔ trusting beliefs	−0.076	2.75**	(n/a)
Mobile purchases ➔trusting beliefs	0.011	0.14	(n/a)
App context ➔ trusting beliefs	0.149	4.16***	(n/a)

MCSE, mobile-computing self-efficacy; BBB, Better Business Bureau; n/a, not applicable.
***$p < 0.001$, **$p < 0.01$, *$p < 0.05$, $^{\dagger}p < 0.10$.

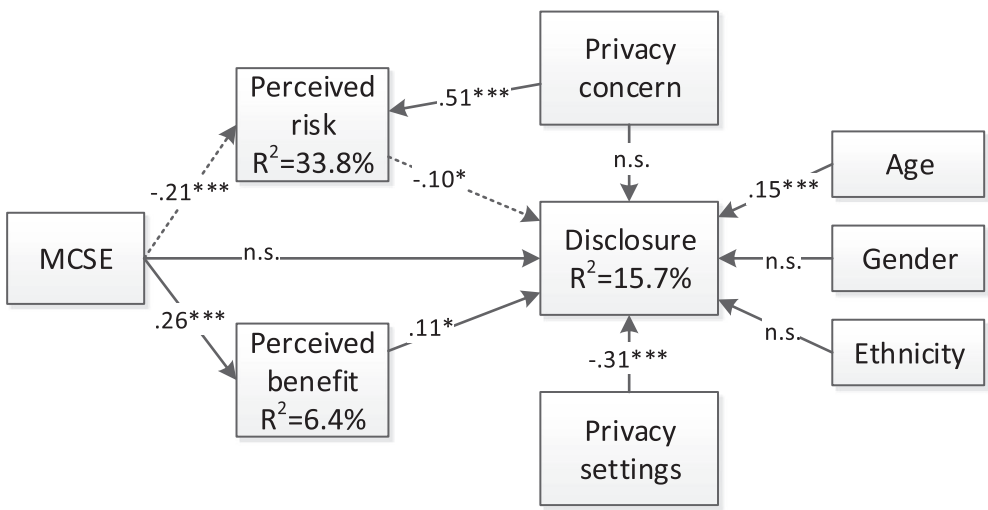


Figure 6. Summary of hypothesis testing for Study 2.

Figure 6 summarises the testing of the theoretical paths in the model for each experiment. The significance of the path estimates was calculated using a bootstrap technique with 600 resamples. Table 4 summarises the demographics of the Study 2 participants, while Table 5 summarises the measurement model statistics. Table 6 summarises the hypotheses, the path coefficients and the *t*-values for each path.

Table 4. Demographic statistics

Apps currently used (non-system apps)	30.4 $\bar{x}$ (20.87σ)
Age	32.6 $\bar{x}$ (15.35σ)
Smartphone user	89.3%
Apple iPhone user	52.1%
Gender (male/female)	55.1%/44.9%

This study occurred 18 months later than the first (resulting in much higher smartphone user rates).
apps, applications.

Table 5. Measurement model statistics

Construct	Mean	SD	(1)	(2)	(3)	(4)	(5)
MCSE (1)	5.53	1.23	–	–	–	–	–
Perceived risk (2)	3.89	1.39	−0.26	–	–	–	–
Perceived benefit (3)	4.81	1.17	0.26	−0.13	–	–	–
Disclosure (4)	1.18	1.97	0.09	−0.14	0.14	–	–
Privacy concern (5)	5.26	1.32	−0.08	0.53	0.08	−0.07	–
Privacy settings (6)	0.97	0.42	−0.07	0.07	−0.07	−0.33	−0.06

Privacy settings is a formative combination of the average of several settings (0 = *share nothing* to 1.25 = *share everything*). MCSE, perceived risk and perceived benefit are Likert scales (1 = *strongly disagree* to 7 = *strongly agree*). Disclosure ranges from 0 to 6 and is calculated by multiplying the accuracy measure (0 = *nothing accurate*, 6 = *everything accurate*) by the percent (0 to 1) of profile data disclosed.
SD, standard deviation; MCSE, mobile-computing self-efficacy.

Table 6. Summary of tested paths

Tested paths	Path coefficient (β)	*t*-value	Supports model?
Hypotheses	–	–	–
H4. MCSE ➔ perceived risk	−0.212	3.92***	Yes
H5. MCSE ➔ perceived benefit	0.264	4.37***	Yes
H6. MCSE ➔ disclosure	0.036	0.71	No
Other relationships of interest	–	–	–
Perceived risk ➔disclosure	−0.101	2.12*	(n/a)
Perceived benefit ➔disclosure	0.112	2.52**	(n/a)
Privacy settings ➔ disclosure	−0.320	6.58***	(n/a)
Privacy concern ➔ disclosure	−0.076	1.35	(n/a)
Privacy concern ➔perceived risk	0.506	13.45***	(n/a)
Gender ➔ disclosure	−0.017	0.36	(n/a)
Ethnicity ➔disclosure	0.056	0.86	(n/a)
Age ➔ disclosure	0.152	3.52***	(n/a)

MCSE, mobile-computing self-efficacy; n/a, not applicable.
***$p < 0.001$, **$p < 0.01$, *$p < 0.05$, $^{\dagger}p < 0.10$.

DISCUSSION OF STUDIES 1 AND 2 RESULTS

As shown in Tables 3 and 6, H1.1, H3.1, H4.2 and H5.2 were supported, while H2.1 and H6.2 were not. In summary, MCSE has a clear positive effect on trusting beliefs in app providers

(H3.1), a positive effect on the perceived benefits of a mobile app (H5.2) (albeit a very small effect size; $R^2 = 6.4\%$) and a negative effect on perceived risks (H4.2). In addition, participants who were high in MCSE put greater effort into finding the best app to meet their needs, indicated by them being likely to click the BBB link and by their higher accuracy in recalling their structural assurances correctly (H1.1). However, those who clicked on the BBB link were significantly 'less' trusting of the app rather than more trusting (H2.1). As expected, structural assurances played a significant role in developing the participants' trusting beliefs.

In addition, because it is possible that fear-induced coping behaviours can be primed (e.g. by structural assurances) (Passyn & Sujan, 2006), we performed a *post hoc* analysis of the interaction effect between self-efficacy and structural assurances on trusting beliefs. The results revealed that higher levels of MCSE reduced the impact of structural assurances on the consumer's trust. Interestingly, we found that MCSE did not have a direct effect on actual information disclosure (H6.2). Rather, its effect is mediated by perceived risk and benefits. Perhaps the simplest explanation for this fully mediated effect of MCSE is that privacy calculus theory is, in fact, the best explanation for actual information disclosure and that the role of MCSE is only in forming perceptions of perceived risk and benefits. The studies cited that showed direct effects of self-efficacy on information disclosure did not use a privacy calculus theoretical base and may, therefore, have also found a fully mediated model if they had done so.

On the contrary, an unexpected negative effect of clicking on a BBB seal on the participant's trust in the app provider deserves further elaboration. One possibility is that this effect is most likely related to the characteristics of the BBB seal link content itself, where the language used to describe what constitutes a BBB-endorsed company triggered risk-averse thoughts and responses from the participants. In other words, it could be that participants were not considering the possible risks of using the app until an experimental threat cue (i.e. BBB seal) (cf., Mogg *et al*., 2008; Grillon *et al*., 2004) brought it to their attention. At that point, they decided to be more cautious in their decision-making. This explanation also reconciles the significant positive interaction effect of H4.2 with SCT. In other words, MCSE still had a reinforcing effect with clicking the BBB seal description link because higher MCSE individuals place greater faith in their coping efforts. In summary, (1) higher MCSE individuals were more likely to click the BBB seal (i.e. undertake coping efforts); then, (2) once they read the explanation and were reminded of the fact that they could not verify the integrity of the app provider without a third party like the BBB, they decided to be more cautious in choosing whom to trust; and (3) their higher MCSE reinforced this realisation and the caution produced by reading the BBB seal explanation.

Finally, the significant interaction effect discovered *post hoc* between self-efficacy and structural assurances on trusting beliefs should be explained: our results demonstrate that high self-efficacy individuals are more likely to search for trust-assuring cues (e.g. privacy seals and promises), yet they also place less importance on the actual assurance cues themselves than on their own judgments. In other words, high-MCSE individuals believe in their own trust-assuring efforts (e.g. the act of searching for structural assurances) while discounting the trust-assuring efforts (e.g. structural assurances) of those who might have a conflict of interest. However, this finding is in agreement with prior research that has demonstrated that high self-efficacy individuals are less concerned with structural assurances of trust (ter Huurne & Gutteling, 2009). To clarify, our high-MCSE participants did indeed seek out the details of the privacy assurances; however, after

reading the assurance statement, they were also wise enough not to place as much confidence in that statement as lower MCSE participants were, knowing that a simple assurance statement is not a legal guarantee of privacy. This phenomenon is also consistent with the coping-effort conceptualisation by Carver *et al*. (1989), where the 'suppression of competing activities' refers to the downplay of competing channels of information conflicting with one's own efforts. That is, individuals faced with a stressor (a potential opportunistic use of their location information in this context) will attempt to cope by suppressing their attention through focusing on other activities and information (e.g. seeking and comprehending details of privacy statements). As participants with high MCSE understand the potential downfalls of disclosure better and understand the limited nature of protection that assurances offer, those assurances are less effective in trust formation.

Implications for research and practice

Our study's findings, juxtaposed against our underlying theoretical model, provide a number of interesting implications for both research and practice. Foremost, this study posits MCSE as an important factor in understanding the behaviour of mobile-computing consumers.

Concerning SCT-based self-efficacy studies, our results demonstrate that MCSE has impacts beyond personal performance and includes the trusting beliefs consumers form in vendors as well as the risk/benefit calculus they perform when making disclosure decisions. In addition, higher levels of MCSE can lead not only to self-misevaluation but also to the misevaluation of others. These findings are of particular interest to research on self-efficacy, because self-efficacy and associated CSE are typically assumed by the literature to be a positive attribute of a user or consumer. Instead, we provide evidence of a counterintuitive effect of high self-efficacy – specifically through high MCSE. This generally positive attribute has a potentially dark side in early adopters of innovative mobile technologies in creating false beliefs about their ability to evaluate the risks that can expose them to notable privacy and security risks. This is particularly problematic because high self-efficacy is highly associated with early adoption and innovation (Agarwal *et al*., 2000; Thompson *et al*., 2006), such as in the early use of smartphones.

This counterintuitive relationship between MCSE and trust and risk/benefit calculations is a potentially dangerous one for consumers of apps, and it has strong implications for practice because this relationship has the potential to undermine the global market for apps. It means that consumers are willing to trust in the benevolence, integrity and competence of app providers, simply when the consumers deem themselves capable of coping with any of the potential risks and dangers of disclosing their personal and location data. However, unless the consumer is a skilled hacker who can 'jailbreak' their smartphone and examine the actual data flows to and from their device (e.g. Enck *et al*., 2010a; e.g. Enck *et al*., 2010b), the reality is that the consumer has little practical way of accurately evaluating the app risks. Of still greater concern, the spyware that has been shown to exist in both the Apple and Android app stores (Seriot, 2010; Gingrich, 2011) is virtually undetectable. Consequently, many confident consumers of LBS-based apps are being unwittingly exploited because lower MCSE consumers are less likely to trust app providers. Therefore, during these early stages of LBS-based mobile-technology adoption, consumers need increased awareness of their privacy risks and should be careful to avoid letting

their perceived skills influence them into making casual adoption decisions. This problem points to the need for greater consumer awareness.

Some might hold a contrary position and posit that this is a consumer problem, not a business problem. Although consumers might be the first wave of victims in our context, we argue that building such consumer protection aligns with businesses as well. We argue that legitimate purveyors of apps that use consumer data ethically are directly and indirectly harmed when app consumers fall victim to unscrupulous app vendors. Considering the effects of the Nigerian money fraud on the brand equity of Nigeria and Africa (Viosca *et al*., 2004) and the effects of internet fraud on early e-commerce (Friedman, 1998; Friedman *et al*., 2000), it would be wise for legitimate app providers, as well as for the creators of mobile handsets, to take an interest in helping consumers to avoid, or cope with, unscrupulous app vendors. It is not difficult to find examples of how stable robust markets, designed around verification, trust and legitimacy thrive far more than markets ridden with unscrupulous behaviour (Sadka, 2006; Schweitzer *et al*., 2006). Leaving consumers alone to make app-adoption decisions, based on their MCSE or on other personal factors, leaves them open to exploitation.

In terms of apps for practice, these consumer vulnerabilities point to opportunities that need to be resolved by industry. As a result, perhaps the most important practical implication of this research is that there is a great need for the market to provide credible risk information for apps and their use of LBS. Our findings indicate that privacy assurances still play a larger role in fostering trust than MCSE, yet standard third-party systems do not exist for mobile apps. While some app providers would certainly prefer to keep consumer information flowing, other more ethical providers who are struggling to compete may prefer a more level playing field offered by third-party auditing services such as BBB and eTrust.

In addition, because it is well documented that location data are being unethically collected and distributed, and because our research shows that some LBS users are willing to make disclosure decisions without accurate and objective information, an opportunity exists for a market to develop around protecting location data ‘post hack’. Such a market is similar to that developed by companies such as LifeLock to protect personal-identity information by resolving ID theft both before and ‘after’ information is misused.

Limitations and future research

Our research has limitations that point to the need for exciting future research to be conducted in the area. At a high level, the purpose of this research was not to identify the exact boundaries of the MCSE construct as it currently exists. Nor was this research meant to provide a comprehensive model explaining trust and information disclosure in the mobile context. Rather, our purpose was to explore the role of self-efficacy as a new and unexpected indicator of the seemingly irrational rates of consumer information disclosure. In order to further refine the form of the MCSE construct, future research could contribute by specifying the exact dimensions of the construct. However, such a project may be difficult given the rapidly changing mobile technologies and contexts for their use.

Next, although our research supports a strong relationship between MCSE and trusting beliefs, the R^2 value of our trusting beliefs construct was only 22%. Therefore, consumers are basing their trusting beliefs and risk perceptions on many other factors as well. Again, as

stated previously, the purpose of this research was not to develop an all-inclusive model but rather to first establish the role of MCSE mobile-app trust and information disclosure. Future research should compare the effects of MCSE with other known predictors, such as brand valuation and recognition and social influences, and examine its interaction with product reviews. In fact, we posit that MCSE should be included with most studies on mobile-computing adoption and diffusion. As already argued, self-efficacy is a complex psychological construct that theoretically interacts with many of the known predictors of IT adoption.

One possible limitation of our experimental design is that in Study 1, participants were not asked to indicate how familiar they were with BBB seals. Therefore, many participants who were truly concerned about the risk, and high in MCSE, may have not clicked on the link simply because they already knew what it meant. In addition, participants had the option of clicking the 'What's this?' link either while reviewing the app or immediately after when asked to verify whether they recalled the BBB seal. Active coping takes place during task execution – in this case, reviewing the app. As a result, those who clicked the link afterward – although doing so immediately after reviewing the app – were not 'actively' coping. Similarly, because participants in Study 1 were asked to recall the privacy assurances of the app they were assigned to 'after' they were done reviewing the app, it is possible that they simply forgot the assurances even though they may have been actively coping. In summary, there is likely to be some degree of error in our coping measurement.

As with all experiments, our study also has limited generalisability. It thus behoves researchers in this area to examine additional app contexts, with an additional array of privacy and security risk possibilities. Older and less innovation-adopting consumers should also be considered, especially as the smartphone market matures to include increased mainstream consumer use. Our theoretical model should also be extended and applied to other forms of mobile technology that are related but still have subtle differences that might make self-efficacy considerations different, such as with the exploding tablet market, innovative uses of consumer-based radio-frequency identification and other forms of geospatially aware devices, such as child-tracking devices and running watches.

CONCLUSION

In summary, we developed, discussed and identified a measure for MCSE and found that MCSE is a key indicator of the trusting beliefs of LBS-based app consumers. Our findings should motivate consumers to become educated and cautious in their decisions to disclose personal and location data, even when they feel that they are very knowledgeable, both about the risks associated with mobile computing and about ways to mitigate those risks. This implication is especially important as recent headlines have revealed that unauthorised usage of location data is becoming more common (Angwin & Valentino-Devries, 2011). In addition, our research identifies a unique and unintended consequence of self-efficacy on trusting beliefs in other parties. We hope our findings will encourage future research into both the privacy risks of LBS-based mobile computing and other unexpected consequences of high self-efficacy.

REFERENCES

148apps (2012) App store metrics. Retrieved date: October 4, 2012, URL: http://148apps.biz/app-store-metrics/?mpage=appprice

Acquisti, A. & Grossklags, J. (2003) Losses, gains, and hyperbolic discounting: an experimental approach to information security attitudes and behavior. In: UC Berkeley 2nd Annual Workshop on Economics and Information Security, pp. 1–27. Berkeley, CA.

Acquisti, A. & Grossklags, J. (2004) Privacy attitudes and privacy behavior. In: Economics of Information Security. Vol. **12**, Camp, L. & Lewis, S. (eds.), pp. 165–178. Springer: US.

Acquisti, A. & Grossklags, J. (2005) Privacy and rationality in individual decision making. *IEEE Security & Privacy*, **3**, 26–33.

Agarwal, R., Sambamurthy, V. & Stair, R.M. (2000) Research report: the evolving relationship between general and specific computer self-efficacy: an empirical assessment. *Information Systems Research*, **11**, 418.

Ajzen, I. (1991) The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, **50**, 179–211.

Angwin, J. & Valentino-Devries, J. (2011) Apple, Google collect user data. Retrieved date: May 31, 2011, url: http://online.wsj.com/article/SB10001424052748703983704576277101723453610.html

Aspinwall, L., Sechrist, G. & Jones, P. (2005) Expect the best and prepare for the worst: anticipatory coping and preparations for Y2K. *Motivation and Emotion*, **29**, 353–384.

Awad, N. & Ragowsky, A. (2008) Establishing trust in electronic commerce through online word of mouth: an examination across genders. *Journal of Management Information Systems*, **24**, 101–121.

Ba, S.L. & Pavlou, P.A. (2002) Evidence of the effect of trust building technology in electronic markets: price premiums and buyer behavior. *MIS Quarterly*, **26**, 243–268.

Bandura, A. (1977a) Self-efficacy: toward a unifying theory of behavioral change. *Psychological Review*, **84**, 191–215.

Bandura, A. (1977b) Social Learning Theory. General Learning Press, New York, New York, USA.

Bandura, A. (1977c) Toward a unifying theory of behavior change. *Psychological Review*, **84**, 191–215.

Bandura, A. (1982) Self-efficacy mechanism in human agency. *American Psychologist*, **37**, 122–147.

Bandura, A. (1986) Social Foundations of Thought and Action. Prentice Hall, Englewood Cliffs, NJ.

Bandura, A. (1991) Social cognitive theory of self-regulation. *Organizational Behavior and Human Decision Processes*, **50**, 248–287.

Bandura, A. (2002) Social cognitive theory in cultural context. *Applied Psychology*, **51**, 269–290.

Belanger, F. & Crossler, R.E. (2011) Privacy in the digital age: a review of information privacy research in information systems. *MIS Quarterly*, **35**, 1017–1041.

Bélanger, F., Hiller, J.S. & Smith, W.J. (2002) Trustworthiness in electronic commerce: the role of privacy, security, and site attributes. *Journal of Strategic Information Systems*, **11**, 245–270.

Bernstein, N.A. (1996) Dexterity and Its Development. Lawrence Erlbaum Associates, Mahwah, NJ.

Brandimarte, L., Acquisti, A. & Loewenstein, G. (2013) Misplaced confidences privacy and the control paradox. *Social Psychological and Personality Science*, **4**, 340–347.

Brandimarte, L., Acquisti, A., Loewenstein, G. & Babcock, L. (2009) Privacy concerns and information disclosure: an illusion of control hypothesis.

Carver, C.S., Scheier, M.F. & Weintraub, J.K. (1989) Assessing coping strategies: a theoretically based approach. *Journal of Personality and Social Psychology*, **56**, 267–283.

Chae, M. & Kim, J. (2004) Do size and structure matter to mobile users? An empirical study of the effects of screen size, information structure, and task complexity on user activities with standard web phones. *Behaviour and Information Technology*, **23**, 165–181.

Chin, W.W., Marcolin, B.L. & Newsted, P.R. (2003) A partial least squares latent variable modeling approach for measuring interaction effects: results from a Monte Carlo simulation study and an electronic-mail emotion/adoption study. *Information Systems Research*, **14**, 189–217.

Compeau, D., Higgins, C.A. & Huff, S. (1999) Social cognitive theory and individual reactions to computing technology: a longitudinal study. *MIS Quarterly*, **23**, 145–158.

Compeau, D.R. & Higgins, C.A. (1995a) Application of social cognitive theory to training for computer skills. *Information Systems Research*, **6**, 118–143.

Compeau, D.R. & Higgins, C.A. (1995b) Computer self-efficacy: development of a measure and initial test. *MIS Quarterly*, **19**, 189–211.

Csikszentmihalyi, M. (1977) Beyond Boredom and Anxiety. Jossey-Bass, San Francisco, CA.

Culnan, M.J. (1993) How did they get my name? An exploratory investigation of consumer attitudes toward secondary information use. *MIS Quarterly*, **17**, 341–361.

Dediu, H. (2014) Late late majority. Retrieved date: July 8, 2014, URL: http://www.asymco.com/2014/07/08/late-late-majority/

Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I. & Colautti, C. (2006) Privacy calculus model in e-commerce – a study of Italy and the United States. *European Journal of Information Systems*, **15**, 389–402.

Dinev, T. & Hart, P. (2006) An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, **17**, 61–80.

Dinev, T., Xu, H., Smith, J.H. & Hart, P. (2013) Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts. *European Journal of Information Systems*, **22**, 295–316.

Enck, W., Gilbert, P., Chun, B.-G., Cox, L., Jung, J., McDaniel, P. & Sheth, A. (2010a) TaintDroid: an information-flow tracking system for realtime privacy monitoring on smartphones. Proceedings of OSDI 2010, pp., Vancouver, BC, Canada.

Enck, W., Gilbert, P., Chun, B.-G., Cox, L., Jung, J., McDaniel, P. & Sheth, A. (2010b) TaintDroid: an information-flow tracking system for realtime privacy monitoring on smartphones. Proceedings of OSDI 2010, pp. 1–15. Vancouver, BC, Canada.

Farago, P. (2012) China now leads the world in new iOS and Android device activations. In: China Now Leads the World in New iOS and Android Device Activations, Vol. **2012** (ed. Flurry), pp. Flurry.

Fife, E. & Orjuela, J. (2012) The privacy calculus: mobile apps and user perceptions of privacy and security. *International Journal of Engineering Business Management*, **5**, 7.

Forman, C., Ghose, A. & Wiesenfeld, B. (2008) Examining the relationship between reviews and sales: the role of reviewer identity disclosure in electronic markets. *Information Systems Research*, **19**, 291–313.

Fornell, C. & Bookstein, F.L. (1982) Two structural equation models: LISREL and PLS applied to consumer exit-voice theory. *Journal of Marketing Research*, **19**, 440–452.

Friedman, B., Peter, H., Khan, J. & Howe, D.C. (2000) Trust online. *Communications of the ACM*, **43**, 34–40.

Friedman, M. (1998) Coping with consumer fraud: the need for a paradigm shift. *Journal of Consumer Affairs*, **32**, 1–12.

Gefen, D., Karahanna, E. & Straub, D.W. (2003) Trust and TAM in online shopping: an integrated model. *MIS Quarterly*, **27**, 51–90.

Gefen, D., Straub, D. & Boudreau, M.-C. (2000) Structural equation modeling and regression: guidelines for research practice. *Communications of the AIS*, **4**, 1–78.

Gefen, D. & Straub, D.W. (2005) A practical guide to factorial validity using PLS-graph: tutorial and annotated example. *Communications of the AIS*, **16**, 91–109.

Gingrich, A. (2011) The mother of all Android malware has arrived: stolen apps released to the market that root your phone, steal your data, open backdoor. Retrieved date: May 20, 2011, URL: http://www.androidpolice.com/2011/03/01/the-mother-of-all-android-malware-has-arrived-stolen-apps-released-to-the-market-that-root-your-phone-steal-your-data-and-open-backdoor/

Goel, S. & Karri, R. (2006) Entrepreneurs, effectual logic, and over-trust. *Entrepreneurship: Theory and Practice*, **30**, 477–493.

Grace, G.D. & Schill, T. (1986) Social support and coping style differences in subjects high and low in interpersonal trust. *Psychological Reports*, **59**, 584–586.

Grazioli, S. & Jarvenpaa, S.L. (2003) Consumer and business deception on the Internet: content analysis of documentary evidence. *International Journal of Electronic Commerce*, **7**, 93–118.

Grillon, C., Baas, J.P., Lissek, S., Smith, K. & Milstein, J. (2004) Anxious responses to predictable and unpredictable aversive events. *Behavioral Neuroscience*, **118**, 916–924.

Hardin, A. M., Chang, J. C.-J. & Fuller, M. A. (2008) Formative vs. reflective measurement: comment on Marakas, Johnson, and Clay (2007). Journal of the Association for *Information Systems*, **9**, 519–534.

Hauser, R., Paul, R. & Bradley, J. (2012) Computer self-efficacy, anxiety, and learning in online versus face to face medium. *Journal of Information Technology Education: Research*, **11**, 141–154.

Heath, C. & Tversky, A. (1991) Preference and belief: ambiguity and competence in choice under uncertainty. *Journal of Risk and Uncertainty*, **4**, 5–28.

Herath, T., Chen, R., Wang, J., Banjara, K., Wilbur, J. & Rao, H.R. (2014) Security services as coping mechanisms: an investigation into user intention to adopt an email authentication service. *Information Systems Journal*, **24**, 61–84.

Hilary, G. & Menzly, L. (2006) Does past success lead analysts to become overconfident? *Management Science*, **52**, 489–500.

Hsu, M.-H. & Chiu, C.-m. (2004) Internet self-efficacy and electronic service acceptance. *Decision Support Systems*, **38**, 369–381.

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.

Hui, K.L., Teo, H.H. & Lee, S.Y.T. (2007) The value of privacy assurance: an exploratory field experiment. *MIS Quarterly*, **31**, 19–33.

IDG (2010) Worldwide and U.S. mobile applications, storefronts, and developer 2010–2014 forecasts and

year-end 2010 vendor market shares: the 'appification' of everything. Retrieved date: URL: http://www.idg.com/www/pr.nsf/0/1280307E4BE966E8852577F8004FA500

Junglas, I.A., Johnson, N.A. & Spitzmuller, C. (2008) Personality traits and concern for privacy: an empirical study in the context of location-based services. *European Journal of Information Systems*, **17**, 387–402.

Kalichman, S.C. & Nachimson, D. (1999) Self-efficacy and disclosure of HIV-positive serostatus to sex partners. *Health Psychology*, **18**, 281.

Keith, M. J., Babb, J. S., Furner, C. P. & Abdullat, A. (2010) Privacy assurance and network effects in the adoption of location-based services: an iPhone experiment. In: Proceedings of the International Conference on Information Systems (ICIS 2010), pp. paper 237. St. Louis, MI.

Keith, M.J., Thompson, S.C., Hale, J., Benjamin Lowry, P. & Greer, C. (2013) Information disclosure on mobile devices: re-examining privacy calculus with actual user behavior. *International Journal of Human-Computer Studies*, **71**, 1163–1173.

Kim, D. (2008) Self-perception-based versus transference-based trust determinants in computer-mediated transactions: a cross-cultural comparison study. *Journal of Management Information Systems*, **24**, 13–45.

Kim, D.J., Ferrin, D.L. & Rao, H.R. (2008) A trust-based consumer decision-making model in electronic commerce: the role of trust, perceived risk, and their antecedents. *Decision Support Systems*, **44**, 544–564.

Kim, Y. H. & Kim, D. J. (2005) A study of online transaction self-efficacy, consumer trust, and uncertainty reduction in electronic commerce transaction. System Sciences, 2005. HICSS'05. Proceedings of the 38th Annual Hawaii International Conference on, pp. 170c–170c. IEEE.

Komiak, S.Y.X. & Benbasat, I. (2006) The effects of personalization and familiarity on trust and adoption of recommendation agents. *MIS Quarterly*, **30**, 941–960.

Krasnova, H., Spiekermann, S., Koroleva, K. & Hildebrand, T. (2010) Online social networks: why we disclose. *Journal of Information Technology*, **25**, 109–125.

Krohne, H.W. (1989) The concept of coping modes: relating cognitive person variables to actual coping behavior. *Advances in Behaviour Research and Therapy*, **11**, 235–248.

Krueger, N. & Dickson, P.R. (1994) How believing in ourselves increases risk taking: perceived self-efficacy and opportunity recognition. *Decision Sciences*, **25**, 385–400.

Laufer, R.S. & Wolfe, M. (1977) Privacy as a concept and a social issue: a multidimensional developmental theory. *Journal of Social Issues*, **33**, 22–42.

Lending, D. & Dillon, T.W. (2007) The effects of confidentiality on nursing self-efficacy with information systems. *International Journal of Healthcare Information Systems and Informatics*, **2**, 49–64.

Li, X., Hess, T.J. & Valacich, J.S. (2008) Why do we trust new technology? A study of initial trust formation with organizational information systems. *The Journal of Strategic Information Systems*, **17**, 39–71.

Li, Y. (2012) Theories in online information privacy research: a critical review and an integrated framework. *Decision Support Systems*, **54**, 471–481.

Lowry, P.B., Cao, J. & 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*, **27**, 165–204.

Lowry, P.B. & Gaskin, J. (2014) Partial least squares (PLS) structural equation modeling (SEM) for building and testing behavioral causal theory: when to choose it and how to use it. *IEEE Transactions on Professional Communication*, **57**, 123–146.

Lowry, P.B., Moody, G., Vance, A., Jensen, M., Jenkins, J.L. & Wells, T. (2012) Using an elaboration likelihood approach to better understand the persuasiveness of website privacy assurance cues for online consumers. *Journal of the American Society for Information Science and Technology*, **63**, 755–766.

Lowry, P.B., Romano, N.C., Jenkins, J.L. & Guthrie, R.W. (2009) The CMC interactivity model: how interactivity enhances communication quality and process satisfaction in lean-media groups. *Journal of Management Information Systems*, **26**, 159–200.

Lowry, P.B., Vance, A., Moody, G., Beckman, B. & Read, A. (2008) Explaining and predicting the impact of branding alliances and web site quality on initial consumer trust of e-commerce web sites. *Journal of Management Information Systems*, **24**, 201–227.

Lowry, P.B., Wilson, D.W. & Haig, W.L. (2014) A picture is worth a thousand words: source credibility theory applied to logo and website design for heightened credibility and consumer trust. *International Journal of Human-Computer Interaction*, **30**, 63–93.

Luo, X., Li, H., Zhang, J. & Shim, J.P. (2010) Examining multi-dimensional trust and multi-faceted risk in initial acceptance of emerging technologies: an empirical study of mobile banking services. *Decision Support Systems*, **49**, 222–234.

Madhavan, P. & Phillips, R.R. (2010) Effects of computer self-efficacy and system reliability on user interaction with decision support systems. *Computers in Human Behavior*, **26**, 199–204.

Marakas, G.M., Johnson, R.D. & Clay, P.F. (2007) The evolving nature of the computer self-efficacy construct:

an empirical investigation of measurement construction, validity, reliability and stability over time. *Journal of the Association for Information Systems*, **8**, 15–46.

Marakas, G.M., Yi, M.Y. & Johnson, R.D. (1998) The multilevel and multifaceted character of computer self-efficacy: toward clarification of the construct and an integrative framework for research. *Information Systems Research*, **9**, 126–163.

Mathieson, K. (1991) Predicting user intentions: comparing the technology acceptance model with the theory of planned behavior. *Information Systems Research*, **2**, 173–191.

McKnight, D.H., Choudhury, V. & Kacmar, C. (2002) Developing and validating trust measures for e-commerce: an integrative typology. *Information Systems Research*, **13**, 334–359.

Milne, G.R., Labrecque, L.I. & Cromer, C. (2009) Toward an understanding of the online consumer's risky behavior and protection practices. *Journal of Consumer Affairs*, **43**, 449–473.

Mogg, K., Holmes, A., Garner, M. & Bradley, B.P. (2008) Effects of threat cues on attentional shifting, disengagement and response slowing in anxious individuals. *Behaviour Research and Therapy*, **46**, 656–667.

Moody, G.D., Galletta, D.F. & Lowry, P.B. (2014) When trust and distrust collide: the engendering and role of ambivalence in online consumer behavior. *Electronic Commerce Research and Applications*, **13**, 266–282.

Moores, T.T. & Chang, J.C.-J. (2009) Self-efficacy, overconfidence, and the negative effect on subsequent performance: a field study. *Information & Management*, **46**, 69–76.

Nisbett, R.E. & Wilson, T.D. (1977) Telling more than we can know: verbal reports on mental processes. *Psychological Review*, **84**, 231–258.

Passyn, K. & Sujan, M. (2006) Self-accountability emotions and fear appeals: motivating behavior. *Journal of Consumer Research*, **32**, 583–589.

Pavlou, P.A. (2002) Institution-based trust in interorganizational exchange relationships: the role of online B2B marketplaces on trust formation. *The Journal of Strategic Information Systems*, **11**, 215–243.

Pavlou, P.A. & Fygenson, M. (2006) Understanding and predicting electronic commerce adoption: an extension of the theory of planned behavior. *MIS Quarterly*, **30**, 115–143.

Pavlou, P.A. & Gefen, D. (2004) Building effective online marketplaces with institution-based trust. *Information Systems Research*, **15**, 37–59.

Pedersen, E.P. (2005) Adoption of mobile internet services: an exploratory study of mobile commerce early adopters. *Journal of Organizational Computing and Electronic Commerce*, **15**, 203–222.

Pitt, L.F., Parent, M., Junglas, I., Chan, A. & Spyropoulou, S. (2011) Integrating the smartphone into a sound environmental information systems strategy: principles, practices and a research agenda. *The Journal of Strategic Information Systems*, **20**, 27–37.

Rainie, L. (2010) Internet, Broadband, and Cell Phone Statistics. Pew Research Center, pp. Pew Internet & American Life Project, In.

Reed, M. (2011) The surprise behind the mobile app numbers. Huffington Post, Retrieved date: July 15, 2011, URL: http://www.huffingtonpost.com/morgan-reed/the-surprise-behind-the-m_b_895397.html

Ringle, C. M., Wende, S. & Will, S. (2005) SmartPLS 2.0 (M3) Beta. Retrieved date: October 30, 2010, url: http://www.smartpls.de.

Rogers, E.M. (1962) Diffusion of Innovations. Free Press, Glencoe.

Sadka, G. (2006) The economic consequences of accounting fraud in product markets: theory and a case from the U.S. telecommunications industry (WorldCom). *American Law and Economics Review*, **8**, 439–475.

Schweitzer, M.E., Hershey, J.C. & Bradlow, E.T. (2006) Promises and lies: restoring violated trust. *Organizational Behavior and Human Decision Processes*, **101**, 1–19.

Security, L. M. (2011) App genome report. In: App Genome Report – February 2011, Vol. 2011, pp. Lookout Mobile Security.

Serino, C. M., Furner, C. P. & Smatt, C. (2005) Making it personal: how personalization affects trust over time. Hawaiian International Conference on System Sciences, pp. IEEE, Waikaloa, HI.

Seriot, N. (2010) iPhone privacy. Black Hat DC 2010, pp. 30. Black Hat, January 3, Arlington, VA, USA.

Smith, A. (2012) Nearly half of American adults are smartphone owners. Pew Research, Retrieved date: url:

Smith, H.J., Milberg, S.J. & Burke, S.J. (1996) Information privacy: measuring individual's concerns about organizational practices. *MIS Quarterly*, **20**, 167–196.

Straub, D.W., Boudreau, M.C. & Gefen, D. (2004) Validation guidelines for IS positivist research. *Communications of the AIS*, **14**, 380–426.

Ter Huurne, E. & Gutteling, J. (2008) Information needs and risk perception as predictors of risk information seeking. *Journal of Risk Research*, **11**, 847–862.

ter Huurne, E.F.J. & Gutteling, J.M. (2009) How to trust? The importance of self-efficacy and social trust in public responses to industrial risks. *Journal of Risk Research*, **12**, 809–824.

Thompson, R., Compeau, D.R. & Higgins, C. (2006) Intentions to use information technologies: an integrative model. *Journal of Organizational and End User Computing*, **18**, 25–46.

Vance, A., Elie-Dit-Cosaque, C. & Straub, D.W. (2008) Examining trust in information technology artifacts: the effects of system quality and culture. *Journal of Management Information Systems*, **24**, 73–100.

Venkatesh, V. & Bala, H. (2008) Technology acceptance model 3 and a research agenda on interventions. *Decision Sciences*, **39**, 273–315.

Venkatesh, V. & Davis, F.D. (2000) A theoretical extension of the technology acceptance model: four longitudinal field studies. *Management Science*, **46**, 186–204.

Venkatesh, V., Morris, M.G., Davis, G.B. & Davis, F. D. (2003) User acceptance of information technology: toward a unified view. *MIS Quarterly*, **27**, 425–478.

Viosca, R.C. Jr., Bergiel, B.J. & Balsmeier, P. (2004) Effects of the electronic Nigerian money fraud on the brand equity of Nigeria and Africa. *Management Research News*, **27**, 11–20.

Wang, E.T.G., Ju, P.-H., Jiang, J.J. & Klein, G. (2008) The effects of change control and management review on software flexibility and project performance. *Information & Management*, **45**, 438–433.

Wang, W.Q. & Benbasat, I. (2005) Trust in and adoption of online recommendation agents. *Journal of the Association for Information Systems*, **6**, 72–101.

Wang, W.Q. & Benbasat, I. (2007) Recommendation agents for electronic commerce: effects of explanation facilities on trusting beliefs. *Journal of Management Information Systems*, **23**, 217–246.

Wang, Y.-S., Lin, H.-H. & Luarn, P. (2006) Predicting consumer intention to use mobile service. *Information Systems Journal*, **16**, 157–179.

Wei, M., Russell, D.W. & Zakalik, R.A. (2005) Adult attachment, social self-efficacy, self-disclosure, loneliness, and subsequent depression for freshman college students: a longitudinal study. *Journal of Counseling Psychology*, **52**, 602.

Xu, H. (2010) Locus of control and location privacy: an empirical study in Singapore. *Journal of Global Information Technology Management*, **13**, 63–87.

Xu, H., Teo, H.H., Tan, B.C.Y. & Agarwal, R. (2010) The role of push–pull technology in privacy calculus: the case of location-based services. *Journal of Management Information Systems*, **26**, 135–173.

SUPPORTING INFORMATION

Additional supporting information may be found in the online version of this article at the publisher's website.