Journal of Strategic Information Systems xxx (xxxx) xxx–xxx

Contents lists available at ScienceDirect

Journal of Strategic Information Systems

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

Dealing with digital traces: Understanding protective behaviors on mobile devices

France Belanger[a,*,1], Robert E. Crossler[b,1]

[a] R. B. Pamplin, Pamplin College of Business, Virginia Tech, 880 West Drillfield Drive, Suite 3007, Blacksburg, VA 24061-0101, United States
[b] Department of Management, Information Systems, and Entrepreneurship, Carson College of Business, P.O. Box 644743, Washington State University, Pullman, WA 99163, United States

ARTICLE INFO

Keywords:
Mobile information protection behaviors
Mobile information privacy
Theory of planned behavior
Information disclosure

ABSTRACT

With increasingly digitization, more and more information is collected from individuals and organizations, leading to several privacy concerns. These risks are further heightened in the mobile realm as data collection can occur continuously and ubiquitously. When individuals use their own devices in work settings, these issues become concerns for organization as well. The question then is how to ensure individuals perform proper information protection behaviors on mobile devices. In this research, we develop a model of mobile information protection based on an integration of the Theory of Planned Behavior and the information privacy literature to explore the antecedents of the attitude of individuals towards sharing information on their mobile devices, their intentions to use protective settings, and their actual practices. The model is tested with data from 228 iPhone users. The results indicate that mobile information protection intention leads to actual privacy settings practice, and that attitude towards information sharing and mobile privacy protection self-efficacy affect this intention. Determinants of attitude towards information sharing include mobile privacy concern and trust of the mobile platform. Finally, prior invasion experience is related to privacy concern. These findings provide insights into factors that can be targeted to enhance individuals' protective actions to limit the amount of digital information they share via their smartphones.

1. Introduction

The digitization of many aspects of individuals' lives in today's society, including how people interact with the new digital world, has changed how commerce and communications are conducted (Sørensen and Landau, 2015). Yet, with the ever increasing amount of data collected, stored and possibly shared, individuals often feel overwhelmed with how to control others' access to their personal information (Madden, 2014). In fact, research shows that 28% of people do not manage their privacy settings on social media (O'Connell, 2018) and do not protect their smartphones through simple steps, such as using a lock screen (28%), updating their phone's operating system (14%), or updating their apps (10%) (Rainie and Perrin, 2017). Lack of properly managed settings on a mobile device can result in unauthorized access to personal information, resulting in serious issues such as identity theft (Sullivan, 2018) or individual profiling, even profiling of children's activities (Kuzma, 2012). Of concern is the fact that even when people are made aware of large unauthorized access and abuse of their personal information, as happened in the Facebook and Cambridge

[*] Corresponding author.
E-mail addresses: belanger@vt.edu (F. Belanger), rob.crossler@wsu.edu (R.E. Crossler).
[1] Both authors contributed equally to this work.

https://doi.org/10.1016/j.jsis.2018.11.002
Received 28 September 2017; Received in revised form 7 November 2018; Accepted 13 November 2018

Analytica incident, the majority of them still do not change their information sharing settings (Weisbein, 2018).

As people have started using mobile devices in their personal lives, they have also brought these into the work environment. Allowing employees to bring their personal devices to work has resulted in increased satisfaction, mobility, and productivity, as well as cost savings for organizations (Grech, 2017). Furthermore, as digital natives (or those who grew up with always on technology) enter the work force, they expect to be able to use their devices in the workplace and often demand this perk from their employers (Wang et al., 2017), with over 50 percent of people in this generation believing that being able to use their own mobile devices in the workplace is a right (Fortinet, 2012).

However, with the increased use of mobile devices there has also been an increase in cyberattacks and data breaches using the devices as ways to enter the organizations' networks (Olmstead and Smith, 2017), increasing organizations' exposure to security and privacy threats. Risks also include increased exposure to malware and viruses that could infect the organization. In fact, the greatest concerns organizations may have with use of personal mobile devices is the inadvertent exposure of confidential data (CyberEdge Group, 2015). For organizations, protection of organizational information when employees start using their own devices within organizational boundaries requires that the right protective settings exist on the employees' devices (Allam et al., 2014; Crossler et al., 2014). However, even with the adoption of Bring Your Own Device (BYOD) policies to address mobile device use in organizations, research shows that employees often fail to comply (Eschelbeck and Schwartzbert, 2012; Molok et al., 2013) or forget to follow these policies on their own (Allam et al., 2014; Crossler et al., 2014). Yet use of privacy settings on mobile devices, such as not sharing location and other device specific *meta*-data through shared photos or the use smartphone apps (Hern, 2015) can prevent leakage of important organizational information assets, such as locations of new company operations (Molok et al., 2013).

The above discussion suggests that to achieve protection from unwilling or unintentional leakage of information via mobile devices, which can have negative consequences for both individuals and organizations, we must encourage individuals to use proper privacy protective settings on their mobile devices. Thus, the goal of this research is to explore how to foster these more protective behaviors. The research is guided by the following question: *What factors influence individuals' mobile information protection intentions and actual practices?* We argue in this paper that individuals' attitude towards the sharing of information and their perceived skills will drive their intention to use protective settings on their mobile device, and consequently their actual usage of such settings. Therefore, we draw on the Theory of Planned Behavior and the information privacy literature to develop a model of information protection on mobile devices. Using data from 228 iPhone users, this study finds that consistent with TPB, mobile information protection intention leads to mobile information protection practices. Attitude towards information sharing and mobile privacy protection self-efficacy affect mobile information protection intention, while determinants of attitude towards information sharing include mobile privacy concern and trust of the mobile platform. Finally, prior invasion experience is related to privacy concern. These findings provide insights into factors that can be targeted to enhance individuals' protective actions to limit the amount of digital information they share via their smartphones.

The remainder of this paper is organized as followed. First, we present the theoretical foundations and the proposed research model and hypotheses. We then present the methodology, analyses and results. Finally, we provide a discussion of the results, the implications of the findings and limitations of the study before ending with concluding comments.

2. Background and theoretical foundations

In this research, we focus on mobile phones, which are devices equipped with a number of information and communication technologies implemented through apps (Galluch et al., 2015). There is a significant difference between the use of mobile devices such as smartphones and tablets and other computing devices such as laptops and desktop computers, in particular with respect to types of settings "in use" on mobile devices versus laptops and desktops. For example, mobile devices tend to have many settings "on" for convenience like Bluetooth connections needed to synchronize the smartphone to various wearables like fitness trackers or wireless headsets. Furthermore, operating systems like the iOS do not have nearly the same quantity and quality of security applications that are available for laptops and desktop computers (e.g., antivirus software, firewalls, etc.). Another key difference is that mobile devices are constantly in the possession of the user and used in many public places, increasing the possible threats to the device. Unless users are cognizant of how to protect their smartphone, they are more likely to become a victim since information security is often weakly implemented in smartphones (Zhang et al., 2013). In fact, when using their smartphones, people often download apps without trying them, relying on descriptions of the apps, reviews and ratings (Franko and Tirrell, 2012). Yet, apps are executable files that can be used for mischievous acts or for unwanted sharing of user information. Research has indeed shown that individuals may not know they are giving away their information in the mobile context (Bélanger and Crossler, 2013; Conger et al., 2013; Crossler et al., 2013). Finally, in the organizational setting, employees are often provided with laptop and desktop computers preconfigured with security and privacy settings established by the organization whereas the she smartphone is the primary device brought to the workplace that is not provided by the employer (Babcock, 2016). As such, configuration of information disclosure settings on those devices is the responsibility of the users themselves, with companies hoping that users follow their policies.

The issues discussed above suggest that behaviors of users are likely different in the mobile context, which can create major privacy and security issues for not only themselves but also their employers. In fact, some key concerns of organizations include the risk of malware and ransomware, the leakage of information, and unauthorized access to organizational information via personal devices (Grech, 2017). Yet, prior research has shown that individuals are not aware of the risks related to use of smartphones, in particular lacking awareness of smartphone security issues (Allam et al., 2014), resulting in ineffective or lack of privacy protective behaviors.

2.1. Measuring actual practices

One of the premises of this research is that it is important to not only measure intentions but also individuals' actual information protective practices. While a significant portion of the behavioral research on information privacy has focused on determinants of intentions to protect one's information (Bélanger and Crossler, 2011; Smith et al., 2011), researchers have suggested that intending to protect one's information is not sufficient; actually using information protection practices is necessary for information to be protected (Bélanger and Crossler, 2013; Blythe et al., 2015). These information privacy protection practices should be holistic (limiting the amount of information provided via location-based information, browsing habits, and other settings; using a passcode; encrypting one's mobile device; etc.), as enacting only one protection is not sufficient (Crossler and Bélanger, 2014). There are few studies of actual behaviors in information privacy research with most research focusing mainly on intentions, for example by measuring students' or employees' intentions to participate in a BYOD program (e.g., Crossler et al., 2014; Lee et al., 2017; Weeger et al., 2015). Considering the importance of measuring actual practices, the present study uses a measure of mobile information protection that is an index of multiple privacy settings on smartphones. In doing so, we answer several calls for privacy research that measures actual privacy outcomes (Bélanger and Crossler, 2011; Bélanger and Xu, 2015).

Most of the theories used for privacy research revolve around the privacy calculus (Anderson and Agarwal, 2011; Dinev and Hart, 2006; Jiang et al., 2013; Krasnova et al., 2010) or privacy paradox (e.g., Sheng et al., 2008; Sutanto et al., 2013; Xu et al., 2011). However, these theories do not focus on whether intentions lead to actual behavior. We therefore draw from one well-known theory that specifically looks at this relationship, the Theory of Planned Behavior (TPB). TPB is one of the most widely accepted behavioral theories, frequently used to study the effects of beliefs on the constitution of attitude towards a behavior and the influence of that attitude on behavioral intention (Ajzen, 1991; Ajzen, 2012; Ajzen and Fishbein, 1980).

TPB has been used extensively to study technology-related behavioral intentions and behaviors. Therefore, contextualizing TPB for this study, we draw from prior research to suggest that the link between mobile information protection intention and mobile information protection behavior should be positive. Mobile information protection intention refers to the intent an individual has to use protective settings on their mobile device. Mobile information protection behavior is the actual enactment of implementing protective privacy settings. However, in the case of implementing protective privacy settings, the behavior is captured as a historical decision that people make and rarely revisit. It is possible that intentions do not reflect these settings, which were established at a prior point in time and not revisited. In this study, to remain consistent with TPB, we hypothesize a positive relationship between intention and behavior.

H1. An individual's mobile information protection intention is positively related to his or her mobile information protection behavior (practice).

2.2. Determinants of mobile information protection intention (H2 and H3)

In the TPB, there are three constructs that are conceptually independent antecedents of intention to perform a behavior: attitude, subjective norm, and perceived behavioral control. However, in the context of policy compliance, some studies have found no effect for subjective norms, suggesting that policy compliance is more impacted by personal norms (e.g., Bélanger et al., in press). This lack of effect of subjective norm has also been found in the context of using new technologies (Jansson et al., 2011; Seebauer, 2015). Consistent with these context-relevant studies, we suggest that attitude and perceived behavioral control will affect intentions. We do not include subjective norm since as suggested above, there is mounting research that finds subjective norm provides inconsistent findings and is not significant in voluntary settings (e.g., Lam and Hsu, 2004; Venkatesh et al., 2003) or only affects late adopters (e.g., Bélanger et al., 2011; Bélanger et al., in press; Seebauer, 2015).

2.2.1. Attitude towards information sharing on a mobile device

In TPB, attitude is defined as the degree to which a person has a favorable or unfavorable evaluation or appraisal of a specific or target behavior (Ajzen and Fishbein, 1980), which in this research is individuals' information privacy protection on their mobile device. Therefore, attitude towards information sharing refers to individuals' assessment of their willingness to share information with various applications on their mobile device. This attitude reflects personal preferences for sharing different types of information with the mobile platform provider. Attitude towards sharing information is an evaluative disposition that can be cognitively based or affectively based (Fishbein and Ajzen, 1975). For example, some people love to share information because it makes them feel closer to others. Privacy concern (which we more fully discuss later in this paper) is a belief that an individual has about what others (in this case mobile platform providers) could do that would negatively impact his or her privacy. Beliefs represent cognitive content that the individual considers to be true (Fishbein and Ajzen, 1975). In this case, it is what the individual perceives the mobile platform provider would do, irrespective of whether or not that is truly what the provider would actually do, with their information.

Ajzen and Fishbein (1980) theorize that attitude, intention, and behavior are positively related. However, there are some mixed results in prior research. Consistent with the theory, in some research on policy compliance scholars have found that attitude does indeed play an important role in predicting behavioral intention (Bélanger et al., in press; Bulgurcu et al., 2010). For example, in two studies grounded partially on TPB, Bélanger et al. (in press) find that attitude is a strong predictor of intention to follow a new security policy and George (2004) finds that privacy attitudes are consistent with actual behaviors related to Internet purchasing. However, Herath and Rao (2009) find that attitude does not affect intention to conform with security policies in organizations where organizational commitment and monitoring of compliance are high. In another study linking attitude to intentions to disclose information, Lowry et al. (2011) find a link between attitude and intentions to disclose information on instant messaging. In the present context, mobile information protection intention focuses on protecting oneself; therefore, there should be a negative relationship between attitude towards information sharing (e.g., "I am willing to share…") and intention to protect oneself.

H2. Attitude towards information sharing on one's mobile device is negatively related to an individual's mobile information protection intention.

2.2.2. *Mobile privacy protection self-efficacy*

In TPB, perceived behavioral control represents the user's perceived ease or difficulty of performing the behavior, which is assumed to reflect past experience as well as anticipated obstacles towards a behavior. One of the most often used operationalizations of TPB's perceived behavioral control is self-efficacy. Self-efficacy is "the conviction that one can successfully execute the behavior required to produce outcomes" (Bandura, 1977). Since its initial conceptualization, a number of studies have applied the concept of self-efficacy to explain individual computer related behaviors (e.g. Compeau et al., 1999; Compeau and Higgins, 1995) and people's security behaviors (e.g., Boss et al., 2009; Herath and Rao, 2009; Johnston et al., 2015). In the information privacy literature, self-efficacy is not always considered but it has been shown to influence intentions to follow a privacy policy (Warkentin et al., 2011). Interestingly, self-efficacy has been reported to impact actual behaviors (e.g., Milne et al., 2009; Workman et al., 2008), observed behaviors (e.g., Woon et al., 2005), or intentions to perform behaviors (e.g., Ifinedo, 2012). In most cases, increased self-efficacy is directly related with more favorable intentions or behaviors. Privacy-related research suggests that with the emergence of location-based data on mobile devices, mobile self-efficacy will be important in understanding individual usage of such technologies (Keith et al., 2013). In this study, we focus on self-efficacy regarding the mobile platform's settings. Consistent with prior information systems research, we argue that mobile privacy protection self-efficacy can help determine mobile information protection intention since, for example, a person needs to believe he or she has the ability to properly setup the settings (i.e., mobile privacy protection self-efficacy) on his or her mobile device to intend to do so. These protective settings are key to ensure information on users' devices is not leaked unwillingly or unintentionally.

H3. Mobile privacy protection self-efficacy is positively related to an individual's mobile information protection intention.

2.3. *Determinants of attitude towards information sharing (H4, H5, and H6)*

Most TPB-based studies do not explore antecedents to the attitude construct of the theory. There are exceptions, such as studies that explore how technology adoption factors (e.g., perceived ease of use and usefulness, trust, website or product characteristics) determine attitude in an e-commerce setting (Herath et al., 2014; Pavlou and Fygenson, 2006). Importantly, most prior information privacy research links privacy concern and sometimes trust directly to intentions. However, in a recent study on policy compliance, the authors argue and find support for the idea that concerns and trust affect intentions to comply via attitude as opposed to directly (Bélanger et al., in press). This approach is more consistent with the original TPB foundation. Following this work, we propose that mobile privacy concern and trust of the mobile platform are two key determinants of individuals' attitude towards information sharing on their smartphone.

2.3.1. *Mobile privacy concern*

Information privacy concern is one of the most studied constructs in the privacy literature (Bélanger and Crossler, 2011). Two key conceptualizations have been proposed over time: the Concern for Information Privacy (CFIP) (Smith et al., 1996; Stewart and Segars, 2002) and the Internet Users Information Privacy Concerns (IUIPC) (Malhotra et al., 2004). More recently, CFIP has been adapted to the mobile environment as Mobile Users Information Privacy Concern (Xu et al., 2012), which is used in this study. Regardless of the context in which information privacy concern has been used or the instrument selected, privacy concern has consistently been shown to affect information privacy-related intentions or behaviors directly and indirectly (Anderson and Agarwal, 2011; Malhotra et al., 2004; Sipior et al., 2013; Smith et al., 2011; Stewart and Segars, 2002; Van Slyke et al., 2006). Dinev and Hart (2006) include internet privacy concern as an antecedent to willingness to provide personal information to transact online. This concept is used in the present study since their "willingness to share information" is conceptually the same as attitude towards sharing ("I am willing to share…"). In their study, Dinev and Hart (2006, p. 64) define information privacy concerns as "concerns about opportunistic behavior related to the personal information submitted over the Internet by the respondent in particular." They find, like other researchers (e.g., Li et al., 2014; Schwaig et al., 2013; Sipior et al., 2013), that higher concern leads to less willingness to share information. While a number of privacy studies have found that privacy concern influences sharing intentions, Hong and Thong (2013) demonstrate that it is important to conceptualize constructs to the context being studied. Consistent with this recommendation, we utilize mobile privacy concerns in this study. Building on prior research, we hypothesize that when individuals have high mobile privacy concern (i.e., possible loss of privacy due to information disclosure on mobile devices), they will have a less positive attitude towards information sharing on their smartphone.

H4. Mobile privacy concern is negatively related to an individual's attitude towards information sharing on their mobile device.

2.3.2. *Trust of the mobile platform*

Dinev and Hart (2006) argue that trust leads to willingness to share information. Research has shown that individuals are more willing to disclose information when they perceive the recipient of this information to be trustworthy (McKnight et al., 2002). While some research identifies trust as a determinant of intentions to use online technologies (e.g., Bélanger and Carter, 2008; Bélanger et al., 2002), others link trust to willingness to provide information (e.g., Dinev et al., 2006; Malhotra et al., 2004). Trust plays an important role in mobile contexts since when people trust an application, they are more likely to download it and share information with the mobile platform provider because they trust how the provider will handle their information (Keith et al., 2013). Trust also influences whether or not an individual would use personalized mobile services (Zhou, 2012), including applications that share shopping-related information between users (Wang et al., 2013). Individuals' trust can therefore lead to more information disclosure, which may not be to the advantage of the device's user.

In the context of smartphones, the object of trust is the mobile device platform. This includes the device, the apps on the device, and the cellular/data provider for the device. As this research focuses on overall practices within the mobile device ecosystem, and not interaction with one particular stakeholder, trust is focused on whether or not individuals believe this mobile device platform can properly handle their information. We therefore define trust of the mobile platform as the perception of an individual that the mobile device environment provides a reliable medium for handling information on their device. This is similar to Anderson and Agarwal (2011) who conceptualize trust as "trust in electronic storage as a medium" (p. 474). Greater trust is expected to lead to a more positive attitude toward sharing information on mobile devices.

H5. Trust of the mobile platform is positively related to an individual's attitude towards information sharing on their mobile device.

2.3.3. *Trust of the mobile platform and mobile privacy concern*

In a study of health information disclosure decisions, Anderson and Agarwal (2011) argue that individuals base their disclosure decision on the combined "levels of trust, on risk and concern associated with the organization receiving their information" (p. 473). Trust has also been found to mitigate concerns about disclosing information in online social networks (Krasnova et al., 2010). Regarding mobile device settings, the statistics presented earlier suggest that there is an information asymmetry with individuals lacking knowledge of information protection issues and tools (Allam et al., 2014). With such information asymmetries, individuals must trust the mobile platform will protect their information; if not, there are likely to have increased concerns. Prior research has linked trust and privacy concern (e.g., Anderson and Agarwal, 2011), but the relationship is not always consistent (e.g., Sipior et al., 2013; Van Slyke et al., 2006). In fact, in developing the enhanced APCO model, Dinev et al. (2015) suggest that the link between trust and privacy concern exists, but they do not specify the direction of such a link. Therefore, consistent with some studies that find a direct negative relationship between the two constructs (e.g., Palanisamy, 2014), we argue that trust of the mobile platform has a negative direct relationship with mobile privacy concern.

H6. Trust of the mobile platform is negatively related to mobile privacy concern.

2.4. *Antecedents of mobile privacy concern (H7 and H8)*

Recent information privacy research has started to explore various antecedents to privacy concerns. In fact, in the proposed (but not tested) enhanced APCO model, Dinev et al. (2015) suggest that prior privacy experience, awareness, and various demographic, including personality and cultural differences, affect privacy concerns. To retain a nomologically complete yet relatively parsimonious model, we focus on awareness and experience, which have been the most often used in recent research.

2.4.1. *Mobile protection settings awareness*

Mobile protection settings awareness refers to the degree to which an individual is conscious of the existence of tools and practices to protect his or her information on his or her mobile device (Dinev and Hu, 2007). The more familiar a person is with the settings on his or her mobile device, the more aware he or she is that information is being shared. Studies sometimes link privacy awareness directly to intention (e.g., Dinev and Hu, 2007; Lowry et al., 2011) or attitude (e.g., Bulgurcu et al., 2010; Malandrino et al., 2013). In policy compliance studies, findings suggest that individuals are often non-compliant with security controls of their organizations because of lack of awareness (e.g., Bulgurcu et al., 2010), together with lack of management involvement and conflicts between organizational policies and organizational objectives (Hu et al., 2007). In fact, some studies (e.g., Sheehan and Hoy, 2000) demonstrate that the nature of people's choice to perform privacy related practices is driven by their awareness of the issues surrounding mobile environments. Consistent with the enhanced APCO model, we suggest that awareness of the privacy settings (controls) on one's mobile device should reduce an individual's privacy concerns.

H7. Mobile protection settings awareness is negatively related to mobile privacy concern.

2.4.2. *Prior invasion experience*

Many studies include individuals' prior privacy invasion experiences as an antecedent to their information privacy concern. The assumption is that people who have previous experiences with their information being compromised are more likely to have an increased concern about information disclosure (Smith et al., 1996; Xu et al., 2012). This relationship has been supported in studies where prior invasion experience did affect perceived risks of sharing information (Li et al., 2014; Pavlou and Gefen, 2005; Smith et al., 1996), including in mobile contexts (Xu et al., 2012; Xu et al., 2011). For example, one bad experience of information privacy violation can change a consumer's perception of all companies in the marketplace (Pavlou and Gefen, 2005). However, there are

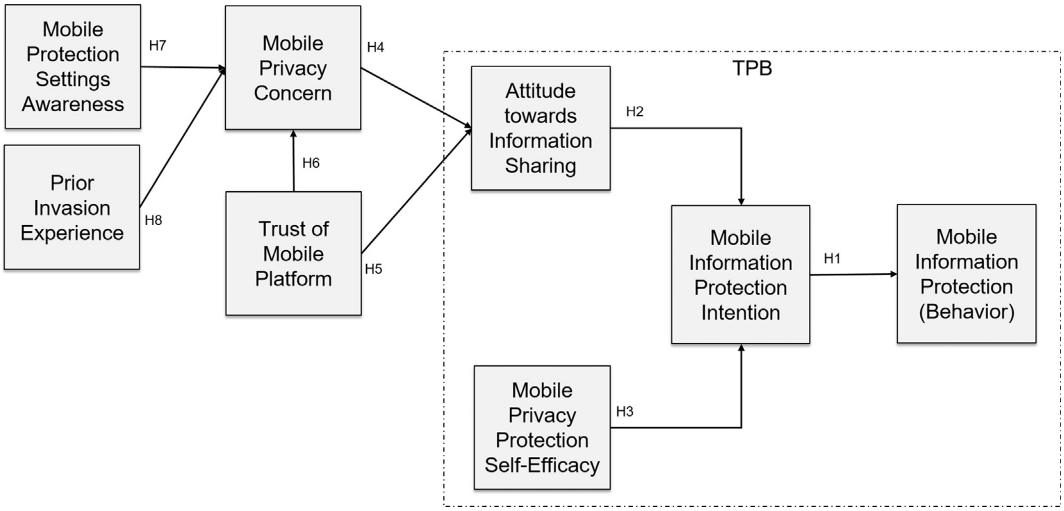
Mobile Protection Settings Awareness
H7
Prior Invasion Experience
H8
Mobile Privacy Concern
H6
Trust of Mobile Platform
H4
H5
TPB
Attitude towards Information Sharing
H2
Mobile Information Protection Intention
H1
Mobile Information Protection (Behavior)
Mobile Privacy Protection Self-Efficacy
H3

Fig. 1. Proposed research model.

some instances when the relationship is not significant, for example in a study of privacy concerns related to healthcare information (Anderson and Agarwal, 2011). Given the majority of studies that support the relationship between invasion experience and mobile privacy concerns, we expect a similar positive relationship. When it comes to mobile information protection, the controls provided by proper settings help prevent the covert collection of personal information. Therefore, we expect that those who have experienced prior invasions will be more concerned about privacy on the mobile platform (Smith et al., 1996; Xu et al., 2012).

H8. Prior invasion experience is positively related to mobile privacy concern.

2.5. *Research model*

This research is one of few focusing on actual protection practices of individuals rather than on intentions. As such, the research tests the often assumed link between intentions and behaviors. The overall model that identifies the determinants of protection behaviors on mobile devices is presented in Fig. 1.

3. Methodology

To measure information protective settings on individuals' mobile devices, this research involved several phases, which are summarized in Table 1.

3.1. *Instrument development*

Several steps were taken to ensure we had a reliable and valid instrument prior to conducting the main survey. First, 83 graduate students were invited to a laboratory setting where they were asked questions on their views of information protection and the efficacy they felt in protecting their mobile device information. We then examined their actual settings on their smartphones. Participants also reported whether they wanted to change settings and why. The findings present interesting insights. Over 50% of the

Table 1
Instrument development and surveys.

Step	Sample	Results
Controlled data collection in lab; survey and observation of actual settings	83 graduate students	● More than 50% did not know privacy settings ● When aware of settings, more than 75% wanted to change LBS settings o More than 79% had specific reasons to change each setting ● Greatest overall privacy concern: perceived lack of control
Online survey pre-test	33 iPhone users	● Instrument validation ● Initial model testing
Expert panel	3 iPhone experts	● Refined dependent variable (MIP)
Online pilot test	81 undergraduate iPhone users	● Instrument reliability and validation
Online survey	228 mTurk iPhone users	● Complete model testing

users had never been to the settings on their smartphone. Of those who had never been there, 75% wanted to change their settings. Open-ended questions revealed that people generally knew which apps they were fine with having access to their personal information, especially location. Interestingly, 79% of respondents explicitly stated why they chose the settings for specific apps that they did. Additionally, individuals' greatest concern was the lack of control they felt in how much access others have to the personal information on their mobile device. They felt there was no way to truly know that their personal information was protected, as exemplified by comments like: *"When using my phone, my greatest concerns […] is that my information is more insecure because I am not a hundred percent sure about how effective […] settings are."* These findings reiterate the importance of understanding users' mobile device information protection practices. Based on these findings, together with the literature review presented in the background section, we developed an initial survey instrument.

The initial survey instrument included items adapted from prior studies, as well as newly created items for constructs that emerged from the data collection in the lab setting. The mobile information protection (MIP) behavior measure was developed following the recommendations of MacKenzie et al. (2011), and focused on the iPhone. Details of the MIP measure items are provided in Appendix A. The measure is formative, consisting of multiple settings on the user's smartphone (Petter et al., 2007). As part of the process of collecting device level settings that must be manually entered into the survey tool, a set of step-by-step instructions were created. To ensure content validity of the newly created MIP measure and that the instructions were accurate, we had it reviewed by expert and novice users with and without their smartphone present. The process confirmed that the MIP items indeed reflected mobile device settings and the step-by-step instructions accurately led respondents to the settings of interest. We then conducted an expert panel with three iOS experts to further validate the MIP measure. They were asked open-ended questions about overall desirable settings on mobile devices and asked to show us their settings. This resulted in confirmation that MIP was a formative construct consisting of multiple measures of mobile device settings. The survey instrument for the entire research model was then pretested with 33 iPhone users and pilot tested with 81 iPhone users. Reliabilities were above 0.80 for all but the trust of the mobile platform construct, which was at 0.688. A few items cross-loaded at less than 0.50. As a result, we refined some scales prior to final execution of the survey instrument.

3.2. *Main survey*

The main data collection was conducted utilizing Amazon's Mechanical Turk (mTurk) and a gerontology center to ensure our results included more diversity in age. A total of 293 subjects began the survey. Overall, 56 responses were eliminated because they did not own an iPhone, four were eliminated because they missed the attention check question, and five because they completed the survey in less than two minutes. This resulted in 228 responses used for the data analyses, including 13 from the gerontology center. Respondents' demographics are presented in Appendix B, together with the demographics of the target population (USA) (Census Bureau, 2013). As seen from the presented demographics, the sample resembles the general composition of the target population given the study's constraints (adult only; iPhone user).

3.3. *Measurement model testing*

To test the measurement model, we assessed convergent and discriminant validity, as well as the reliability of the survey instrument. Convergent validity was assessed with three *ad hoc* tests: standardized loadings, variance-extracted estimates, and construct composite reliabilities (Anderson and Gerbing, 1988). Factor loadings are presented in Appendix A, together with average variance extracted (AVE), composite reliabilities, and Cronbach's alpha. All factor loadings exceed 0.50 (0.513–0.912) (Fornell and Bookstein, 1982) and all AVE estimates exceed the recommended lower limit of 0.50 (Fornell and Bookstein, 1982) with a range of 0.606–0.713. Composite reliabilities are all above 0.70 (0.849–0.934) (Netemeyer et al., 1990) as are Cronbach' alphas (0.756–0.926) (Nunnally, 1978). All tests support the convergent validity of the measurement instrument.

To assess discriminant validity, we examined item-total correlations and each item posited to form a given sub-construct had a stronger correlation with it than with another construct (Anderson and Gerbing, 1988). An additional discriminant validity criterion is that the variance shared by a construct with its indicators should be greater than the variance shared with other constructs (Anderson and Gerbing, 1988). All constructs have the square root of their average variance extracted (Fornell and Bookstein, 1982) greater than their correlations with other constructs (Chin, 1988), as shown in Table 2. Finally, since prior invasion experience and MIP are formative constructs, we confirmed that their dimensions were significant ($p < 0.01$).

Table 2
Correlations and squared roots of AVEs.

Construct	AW	INT	MPC	PPSE	ATT	TRUST
Mobile Protection Settings Awareness (AW)	**0.814**					
Mobile Information Protection Intention (INT)	0.365	**0.801**				
Mobile Privacy Concern (MPC)	0.082	0.405	**0.811**			
Mobile Privacy Protection Self-efficacy (PPSE)	0.548	0.176	−0.144	**0.809**		
Attitude Towards Information Sharing (ATT)	−0.113	−0.534	−0.387	0.116	**0.778**	
Trust of Mobile Platform (TRUST)	0.088	−0.100	−0.168	0.287	0.304	**0.844**

Bolded diagonal values are square root of the average variance extracted (AVE).

Common method variance (CMV) can force constructs to be highly correlated with each other. The design of the survey included efforts to control for CMV by randomizing items. Nevertheless, we conducted two popular tests for CMV. First, we included all reflective indicators into a factor analysis to conduct the Harman's one-factor test (Podsakoff et al., 2003). Results show the maximum covariance explained by any one factor is 27%. A further test is to ensure that no correlations are above 0.90, which would also be a possible indicator of CMV (Pavlou et al., 2007). As can be seen in Table 2, all correlations were much lower than this cutoff, further reducing concerns over CMV. Finally, we also determined our model was free from common method variance by running a full collinearity test and ensuring that all factor-level VIFs were lower than 3.3 (Kock, 2015).

3.4. Structural model testing

SmartPLS (Ringle et al., 2005) was used to test the research model[2] since it is an appropriate to use when a model includes both reflective and formative measures (Chin et al., 2008). Fig. 2 shows the research model test results.

Most of the research hypotheses are supported by the collected data. Results indicate mobile information protection intention leads to mobile information protection behavior (settings) (H1). Because mobile information protection was measured as the ratios of less protective settings over possible settings (detailed in Appendix A), the negative coefficient is consistent with our hypothesis. We also find that a more positive attitude towards information sharing leads to a decreased intention to protect mobile information (H2). Higher mobile privacy protection self-efficacy leads to higher mobile information protection intention (H3). The antecedents to attitude include both mobile privacy concern and trust, with more concern leading to a less positive attitude towards sharing information (H4) while a higher level of trust leads to a more positive attitude towards sharing information (H5). Trust of the mobile platform is also negatively related to mobile privacy concern (H6). Finally, prior invasion experience is positively related to mobile privacy concern (H8), as expected. The only relationship that is not significant is between awareness of settings and mobile privacy concern (H7).

4. Discussion

The findings of this study provide insights into what factors lead to individuals enacting proper information protection practices on their mobile devices. The research provides a number of key theoretical contributions, as well as implications for research and practice.

4.1. Measuring information protection behaviors

This research explored an important behavior of individuals that can affect their own as well as their organization's information privacy: the use of protective settings on mobile devices. Importantly, for this research a measure of actual settings was developed. We labeled this the mobile information protection (MIP) construct. The index was composed of most information protection settings on an iPhone. For example, an individual was considered better protected if he or she had "do not track" turned on and/or used a passcode to access the device. The list of all settings used in the index are shown in Table 3 with their descriptive statistics. Importantly, the MIP construct represents a holistic view of these settings since it was conceptualized as formative of all of these protective measures. Therefore, the MIP index is the combination of all settings necessary to protect the information on a respondent's device. Few studies have looked at holistic behaviors in information security or privacy since most research focuses on one specific behavior at one point in time (Crossler et al., forthcoming).

4.2. Intentions and behaviors

While there is abundant research using the TPB as its theoretical foundation, most studies stop at intentions, including in information privacy research (Smith et al., 2011). Yet, in the domain of mobile information privacy, intending to protect oneself is not sufficient (Xu and Bélanger, 2013). Therefore, the present study is one of few that goes beyond measuring intentions to also measure practices of individuals towards protecting their mobile device information. We found strong support for the relationship between intentions and behaviors. We therefore add to the few studies that have explored this relationship in policy compliance contexts (e.g., Bélanger et al., in press). While the MIP index is based on self-reported settings, we asked users to report their "actual" settings on their iPhones, and developed measures based on these answers. Even though the measures are self-reported, they are based on factual data (e.g., number of apps in LBS setting) with precise instructions to find these data as opposed to asking perceptual measures of what one does (e.g., recalling how often one shares information or what overall practices one performs). In addition to attention traps, we designed questions that served as validation checks. For example, if an individual answered that LBS was off in one question but included a number of apps in a later question on LBS that obviously requires LBS to be turned on, then we considered this data point invalid. We also conducted independent samples *t*-test on our data from the preliminary controlled experiment. The results showed that individuals reported settings accurately when we compared what they reported to the settings we observed on the respondents' devices.

The MIP measure was developed for the iPhone platform, but the approach used and the concepts presented in this paper can help

[2] The PLS analysis was accomplished with 1,000 bootstrapping sub-samples to estimate path coefficients.

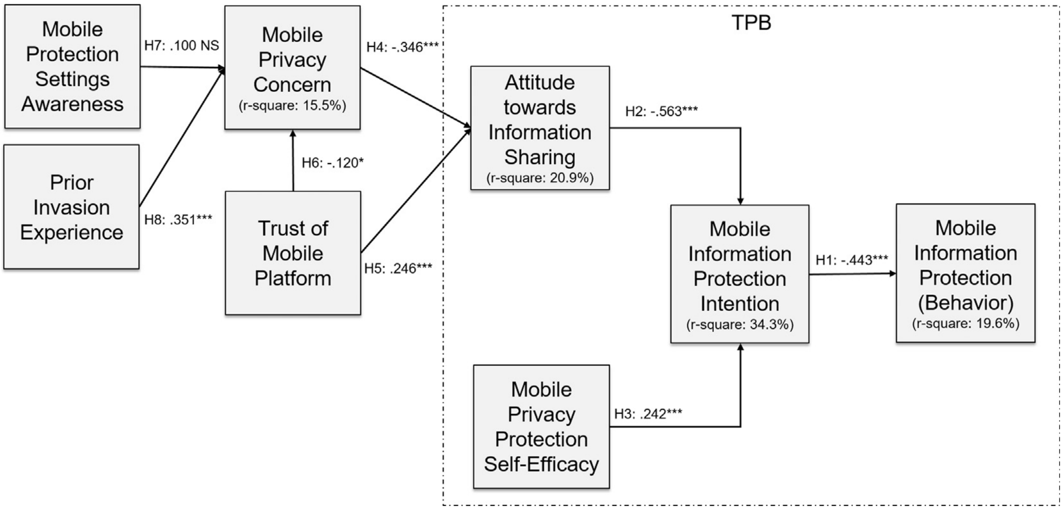
Mobile Protection Settings Awareness
H7: .100 NS
Mobile Privacy Concern
(r-square: 15.5%)
H4: -.346***
TPB
Prior Invasion Experience
H8: .351***
H6: -.120*
Trust of Mobile Platform
H5: .246***
Attitude towards Information Sharing
(r-square: 20.9%)
H2: -.563***
Mobile Information Protection Intention
(r-square: 34.3%)
H1: -.443***
Mobile Information Protection (Behavior)
(r-square: 19.6%)
Mobile Privacy Protection Self-Efficacy
H3: .242***

Fig. 2. Research results.

Table 3
Settings for mobile information protection measure.

Setting		Mean (Standard Dev.)	
Percentage of apps that allow access to location based services over total apps that could		44.0% (0.313)	
Percentage of system services enabled over total system services available		60.9% (0.332)	
Percentage of apps that have microphone access over total number of apps that could		49.3% (0.375)	
		Setting	% of Subjects
Dichotomous score; is “do not track” on or off?		ON	40.6%
		OFF	59.4%
Dichotomous score; is passcode used or not?		ON	66.7%
		OFF	33.3%
Dichotomous score; is “ad tracking” on or off?		ON	40.4%
		OFF	59.6%
Three scores for storing passwords and autofill information:	1. Use Contact Info	OFF	3.1%
		ON; NO DATA STORED	27.5%
		ON; DATA STORED	69.4%
	2. Names and Password	OFF	3.1%
		ON; NO DATA STORED	83.1%
		ON; DATA STORED	13.8%
	3. Credit Cards	OFF	4.4%
		ON; NO DATA STORED	43.8%
		ON; DATA STORED	51.8%
One of three settings for blocking cookies:		Always block	10.1%
		Block from third parties	80.6%
		Never block	9.3%

researchers develop such an index measure for different platforms. Researchers interested in focusing on the iOS platform (e.g., iPad) can use the MIP construct as it is described in this study. For other platforms, such as the Android environment, researchers need to identify all possible settings and develop measures that indicate “better” (i.e. more protective) settings. With the release and increased adoption of the Android operating system Marshmallow and later versions, device settings similar to the iPhone were implemented (Gruman, 2015), providing an opportunity to apply this research more easily in the Android ecosystem.

While the MIP index focuses on information privacy settings, one’s information privacy cannot be ensured if the security of the information is not achieved through use of proper security settings. Looking at the descriptive data from Table 3, one can see that many individuals have poor information protection on their device. It is possible that use of less protective settings is due to individuals believing that smartphone “privacy” settings is much more about protection of their information privacy than their information security. Researchers have proposed that there is a possible privacy-security knowledge gap where individuals believe sharing information is appropriate (and have lower protective setting) when they think of this sharing as a privacy action but if they thought that this sharing of information would result in identity theft, a security issue, then they would not allow such sharing of information (Crossler and Bélanger, 2017). By considering all of the mobile device’s settings holistically in this research, we provide an avenue for ensuring that independent of why they do it, we can measure the overall use of settings for protection of individuals’ information. Nevertheless, future research is needed to explore whether there is indeed a perceived difference between protecting one's information privacy and one's information security, and whether this makes a difference in enactment of protective behaviors.

4.3. Determinants of intentions

Consistent with the theoretical foundation of TPB, attitude towards information sharing and mobile privacy protection self-efficacy are positively related to mobile information protection intention, thereby supporting H2 and H3. Individuals who have a more positive attitude towards information sharing on their mobile device are less likely to intend to protect their information on their device. In fact, this is the strongest path in the model, suggesting that attitude towards information sharing is key in determining mobile information protection intention and ultimately behavior. This provides strong support for the theoretical foundation used in this research and provides support for the need to better understand the determinants of attitude towards information sharing. As discussed in the background section, there appears to be some confusion in policy compliance research using TPB with respect to the role of attitude with some studies including attitude and some not including the construct in their models. Our results support going back to the original foundation and considering the important role of attitude in influencing users' intentions to perform a behavior, in this case a holistic set of information protective settings on their mobile device.

Perceived behavioral control, conceptualized as mobile privacy protection self-efficacy, is also a strong determinant of mobile information protection intention, but in this case it has a positive relationship, where a higher perception of one's ability to protect oneself leads to greater intentions to do so. The relationship between self-efficacy and intention has not been consistent in prior research. We argue that the results were consistent with TPB in this research because the constructs were clearly contextualized to mobile information protection. A meta-analysis of TPB-based research might explore the contextualization of the scales used in measuring self-efficacy and intentions to validate this possibility. Another interesting avenue for future research would be to explore the determinants of individuals' perceptions of their mobile privacy protection self-efficacy to identify practical steps that can be undertaken by organizations to increase this perceived behavioral control variable. This would also be valuable to mobile technology platform providers, so that they can design their platforms with increased possibilities for higher self-efficacy perceptions (i.e., giving users greater perceptions of their abilities).

4.4. Antecedents to attitude towards information sharing

Attitude towards information sharing is the strongest predictor of mobile information protection intention (and strongest path in the overall model). Therefore, it is important to consider what its antecedents are, so that there could possibly be practical actions to improve individuals' attitudes towards the protection of their information on their mobile device (i.e., decrease their willingness to share information broadly via their smartphones). In this study, we hypothesized that mobile privacy concern and trust of the mobile platform would influence attitude towards information sharing. These relationships were supported, which shows that it is important to focus on individuals' concerns to make them less likely to feel comfortable sharing information. Interestingly though, as they develop trust in the mobile platform, individuals increase their comfort with sharing personal information. This is consistent with some prior research (e.g., Jiang et al., 2013; Wang et al., 2013). The take away from this finding is that more effort needs to be put into increasing privacy concern than in building trust. While we would not suggest that we should "lower" trust of individuals, organizations should at least ensure that individuals are well aware of the risks for all of the components of the mobile platform (e.g., device, apps, and providers) so that if they choose to trust the platform, they do so with appropriate knowledge.

The fact that the influence of privacy concern on attitude is greater than that of trust on attitude further supports this recommendation. It also suggests more avenues for future research to explore the possible use of fear appeals in organizational security and privacy training of employees (e.g., Johnston et al., 2015). For example, organizations could explore if presenting how a password can get cracked easily using one of many available password-cracking tools on the Internet (i.e., a fear appeal) could affect behaviors. This could include showing the consequences of one password being compromised by using data from one of the many publicly available breaches, such as the Equifax breach of, 143 million records in the USA[3] or the Aadhaar breach of 1.1 billion records in India.[4] Showing employees how much the breaches end up costing the organization, and possibly explaining who lost their jobs as the result of the breach, would be a persuasive message, which is the core of a fear appeal. This is similar to health warnings where showing the poor health of someone who smoked all their lives is intended to deter people from smoking.

Knowing that raising individuals' privacy concern can lead to less positive attitudes towards information sharing on their mobile device, which ultimately raises their intentions to protect themselves and their use of protective settings on their mobile device, provides a valuable outcome that needs further investigation in future research. One finding of the present study that can allow researchers to move in that direction is the influence of prior invasion experience on mobile privacy concern. It makes sense that those with invasion experience would be more concerned about mobile privacy. As instances of people's privacy being invaded continue to increase in all sorts of technological contexts, researchers may find that changes in privacy concerns have an impact on people's willingness to share information and ultimately their protective practices. In this study, we modeled prior invasion experience as an antecedent to privacy concerns, consistent with prior research (Dinev et al., 2015). Future research could explore how this experience moderates other relationships in understanding privacy behaviors.

[3] https://www.ftc.gov/equifax-data-breach.

[4] https://www.tribuneindia.com/news/nation/rs-500-10-min-and-you-have-access-to-billion-aadhaar-details/523361.html.

One surprising result is the lack of effect of awareness on privacy concern. A possible explanation is how awareness was contextualized for this study. Awareness was contextualized as awareness of privacy settings. If instead it had been contextualized as awareness of the risks associated with the use of mobile devices in general, the relationship might have been supported. As future research draws on these findings, it will be important to ensure that awareness is contextualized in such a way that it is directly related to the constructs of interest in the study (Hong and Thong, 2013). At the same time, while several studies highlight lack of employee awareness towards their organization's policies (Allam et al., 2014; Mahindru, 2013), they also caution that creating awareness is not a one-time effort and that organizations need to make a concerted effort to monitor compliance with policies and employee awareness of the policies (Allam et al., 2014). A longitudinal study of how to raise and sustain information privacy protection on mobile devices, and other platforms, is needed to better understand the enactment of privacy protective behaviors over time. Such a study could also evaluate possible fluctuations over time in both policy compliance and awareness.

Finally, as suggested in prior research and supported in this study, there is a relationship between trust of the mobile platform and mobile privacy concern. Individuals with greater trust of the mobile platform are also those with lower concerns for information privacy. Because of this relationship, it is important for researchers to include both of them in models investigating attitudes, intentions, and/or behaviors. Studies using only trust might overstate the overall impact of trust on attitude while studies using only mobile privacy concern could be missing the mitigating effect of trust on its relationship with attitude and/or intentions.

4.5. *Implications for practice*

In this study, we developed and measured a series of mobile information protection practices that industry experts agreed reflected the settings on an individual's device. These include the location based-information shared via apps and system services as well as the use of passcodes, do not track feature, private browsing, cookie related settings, and the storing of password information. Combined, these settings work together to determine how well individuals are protecting their information. As people take control of these settings in a manner consistent with the information they want to share, they will increase their awareness of the amount of their personal information that is being digitized, collected and shared.

Another important implication of this study for practice is in its applicability to the creation and use of BYOD policies. Organizations' biggest concerns over allowing personal devices into the work environment include data leakage or data loss as well as unauthorized access to the organization's information and systems (Grech, 2017). To embrace the use of personal smartphones inside corporate walls by employees, many organizations have created "bring your own device" (BYOD) policies. BYOD policies focus on steps individuals should take to protect information available through their personal devices while in the workplace (van der Meulen and Rivera, 2013), providing some level of control over how mobile devices can be used within organizational boundaries (Crossler et al., 2014; Dang-Pham and Pittayachawan, 2015; Zahadat et al., 2015). As previously discussed, mobile devices offer additional risks when compared to other computing platforms; yet, while 75 percent of workers are provided company-owned computers (with secured settings) only 23 percent of workers are provided mobile devices by their employer (Babcock, 2016). According to Babcock (2016), only 21% of employees use tablets in the workplace, resulting in the vast majority of devices brought into the organization being smartphones. Therefore, with increased use of personal devices, our results suggest key factors that organizations need to concern themselves with when designing BYOD policies.

Cognitive dissonance theory suggests that individuals try to avoid dissonance between their attitudes and their behaviors (Festinger, 1962). Since both attitude about sharing information and mobile privacy protection self-efficacy affect intentions to protect mobile information, and since intention is related to actual mobile information protection behavior, those factors should be designed into BYOD policies. However, designing policies is not sufficient; organizations need to not only recommend appropriate settings (policy level) but explain how to control these settings and where they are located (i.e., procedure level). This involves offering proper training that focuses on attitudes about sharing information and mobile privacy protection self-efficacy. In the first step towards this two-pronged approach toward educating and training of individuals to improve their protective behaviors, organizations can target ways to influence changes in attitudes of employees towards sharing information. This means rendering employees more reluctant to share information. Such an approach would be similar to implementing a fear appeal as performed in an information security setting (e.g., Johnston et al., 2015). The second element of an education and training program should focus on raising individuals' self-efficacy or confidence at protecting their privacy on their mobile devices. Increasing self-efficacy could be done via privacy education and training (PETA) programs, including showing individuals how to utilize privacy protective tools (Crossler and Bélanger, 2009).

4.6. *Limitations*

This research involved the thorough and systematic development and testing of a model to explain mobile information protection practices of individuals. Nevertheless, there are some limitations that need to be discussed. We developed a model that was comprehensive while remaining parsimonious. As such, we did not include some potentially relevant constructs. For example, it was suggested that pre-existing trust might have an impact on trust-related privacy research (Li et al., 2014). The research was also conducted in an online unsupervised environment so that we could not observe actual settings. The design of the survey questions was done in a way as to measure factual information (number of apps in [this] setting) as opposed to perceptions, which limit this concern. The pretest also revealed that the respondents answered these questions in line with their actual mobile device settings. Nevertheless, future research could attempt to conduct a large-scale controlled environment study to observe actual settings. Another possibility is to use technology to capture actual settings on mobile devices, which is currently not possible in the iOS platform but is possible in the Android environment.

5. Conclusion

Citizens' understanding of threats to information are necessary to provide more secure organizations and a better protected society, particularly since individuals are the weakest link in security (Crossler et al., 2013) and the last line of defense in information privacy (Bélanger and Xu, 2015). Recent research has highlighted that the risks to information in the mobile device context are greater than in the general online environment (Mylonas et al., 2013; Zhang et al., 2013). In this research, we explored determinants of mobile information protective behaviors since individuals are often willing to share much information, even when their organizations would prefer they do not. The research provides a model explaining individual practices with respect to protecting their information on mobile devices. The research develops new instruments that can be used in future research on information protection in the context of other mobile environments but also for new technologies individuals are starting to encounter, such as ubiquitous computing devices (e.g., fitness trackers, augmented reality devices). The research provides key contributions such as measuring individuals' actual information protection practices, validating the relationship between behavioral intentions and behaviors, and exploring antecedents to TPB-derived constructs. Furthermore, as more and more organizations consider BYOD programs (Allam et al., 2014; Crossler et al., 2014; Mahindru, 2013; Weeger et al., 2015), this study provides a better understanding of the privacy protective behaviors of individuals.

Acknowledgments

The research was partially supported by a grant from the Institute for Society, Culture and the Environment at Virginia Tech. We also wish to thank the Center for Gerontology at Virginia Tech for access to respondents. We wish to thank the review team at *JSIS* and participants at seminars we conducted and at the 2013 Dewald Roode Workshop on Information Systems Security Research for their helpful feedback on earlier versions of this paper.

Appendix A. Survey items, measurement model validity testing, and MIP instrument development details

A.1. Reflective and formative study items

Dimensions of prior invasion experience (formative) (adapted from Xu et al. (2012)).

1. How often have you personally been victim of what you felt was an invasion of privacy? (coeff. = 0.723; T value = 5.272; $p < .001$)
2. How much have you heard or read during the last year about the use and potential misuse of consumer personal information? (coeff. = 0.496; T value = 2.982; $p < .01$). Reflective items for this study are shown in Table A.1 while formative items are described below.

A.2. Mobile information protection (MIP) scale development and items

To develop the Mobile Information Protection (MIP) scale, we followed the procedures outlined in MacKenzie et al. (2011), which started with an examination of the conceptual definition of the construct. Using existing information from practitioners and experts, we identified relevant settings on an iPhone for information protection. To ensure content validity, the MIP scale was reviewed by expert and novice users with and without their iPhones present. As explained in the body of the paper, it was also pre-tested and pilot tested several times.

A number of ratios and scores were calculated using settings on the iPhone as reported by respondents. We ensured that we provided clear step by step instructions so that asked factual questions so that we did not create biases in responses. For example, we asked respondents to count the number of apps within their location-based settings (if they had first answered that this setting was "on"). We then asked them to count the number of such apps that indicated "never". Then we had a similar question for "always" and another for "while using". We did this for several settings, and then calculated ratios from those raw data. The ratios and scores were then included as formative dimensions for the MIP measure. As a result, MIP represents an overall measure of various protective settings. It is not an absolute number but rather an index where higher scores show relatively lower protection based on the types and number of apps one has on their iPhone.

Items for MIP were shown in Table 3 in the paper. They include:

1. Percentage of apps that allow access to location based services over total apps that could.
2. Percentage of system services enabled over total system services available
3. Percentage of apps that have microphone access over total number of apps that could
4. Whether "do not track" setting is on or off.
5. Whether iPhone requires a passcode or not.
6. Whether "ad tracking" setting is on or off.
7. All settings for storage of "Use Contact Info", "Names and Password," and "Credit Cards."

Table A.1
Survey instrument items.

Construct items	Load.	AVE	CR	Alpha
Attitude Towards Information Sharing (on Mobile Devices) (Self-Developed)		0.606	0.900	0.864
I am fine with sharing my location with map apps	0.815			
I am fine with sharing my location with weather apps	0.818			
I am fine with sharing my location with the safari browser	0.823			
I am fine with sharing my location with shopping apps	0.513			
I am fine with sharing my location with game apps	0.825			
I am fine with sharing my location with other apps that do not fit one of the above categories	0.827			
Mobile Information Protection Intention (Adapted from Keith et al. (2013))		0.641	0.877	0.812
I will limit the location-based information I share from my mobile device	0.852			
I plan to limit the access applications have to location-based information on my mobile device	0.856			
It is likely that I will enable private browsing on my mobile device	0.753			
I will limit the ability of advertisers to track me on my mobile device	0.733			
Mobile Privacy Concern (Adapted from Xu et al. (2012))		0.658	0.934	0.926
I am concerned that mobile device apps are collecting too much information about me	0.829			
I am concerned that mobile device apps may monitor my activities on my mobile device	0.846			
I feel that as a result of my using mobile device apps, others know about me more than I am comfortable with	0.806			
I believe that as a result of my using mobile device apps, information about me that I consider private is now more readily available to others than I would want	0.803			
I feel that as a result of my using mobile device apps, information about me is out there that, if used, will invade my privacy	0.793			
I am concerned that apps may use my personal information for other purposes without notifying me or getting my authorization	0.846			
When I give personal information to use mobile device apps, I am concerned that apps may use my information for unintended purposes	0.810			
I am concerned that mobile device apps may share my personal information with other entities without getting my authorization	0.753			
Mobile Protection Settings Awareness (Adapted from Bulgurcu et al. (2010))		0.663	0.854	0.781
I am aware that there are privacy controls on my mobile device	0.824			
I understand that there are privacy controls on my mobile device	0.691			
I am aware of location-based settings on my mobile device	0.912			
Mobile Privacy Protection Self-efficacy (Adapted from LaRose and Rifon (2007))		0.654	0.849	0.756
I am confident I know how to protect my personal information on a mobile device	0.743			
I know how to evaluate privacy policies on mobile device apps	0.804			
I know how to change the settings on my mobile device to protect my privacy	0.873			
Trust of the Mobile Platform (Adapted from Dinev and Hart (2006))		0.713	0.882	0.799
Mobile devices are reliable for sharing personal information	0.861			
Apps on mobile devices are reliable for sharing personal information	0.863			
Websites I access via my mobile device are reliable for sharing personal information.	0.809			

8. One of three settings for use of cookies.

Appendix B. Sample and target population demographics

Data was collected from Amazon Mechanical Turk (mTurk). Data collection was restricted to United States respondents who owned iPhones using advanced filtering features of mTurk. The survey included three separate attention check questions and several validation checks.[5] Respondents were paid $1.00 each. The higher income of the sample compared to the US population is expected as 40% of iPhone users make over $100,000.[6] Similarly, there is a larger percentage of smartphone users among the more highly educated population[7] (see Table B.1).

Appendix C. Supplementary material

Supplementary data associated with this article can be found, in the online version, at https://doi.org/10.1016/j.jsis.2018.11.002.

[5] Additional validation checks included cross-matched questions. For example, if an individual answered that LBS was off in one question but included a number of apps in a latter question on LBS that obviously requires LBS to be turned on, then we considered this data point invalid.

[6] https://www.comscore.com/lat/Insights/Blog/Android-vs-iOS-User-Differences-Every-Developer-Should-Know and http://www.pewinternet.org/2015/04/01/us-smartphone-use-in-2015/.

[7] http://www.pewinternet.org/2015/04/01/us-smartphone-use-in-2015/.

Table B.1
Sample demographics and the U.S. population (Census Bureau, 2013).

Demographic (228 respondents) (note: US population data excludes < 18 and > 85 years)		Sample (%)	US Population (%)
Age	18–20	4.41	5.9
	21–24	22.03	7.5
	25–34	44.49	17.9
	35–44	16.30	17.9
	45–54	7.49	19.6
	55–64	2.64	15.9
	65–74	2.64	9.5
Gender (18 years and over)	Female	48.67	50.8
	Male	51.33	49.2
Ethnicity (all ages)	African, AA	7.05	12.6
	Asian, Hispanic	14.54	22.1
	White Caucasian European	76.21	72.4
	Other (American Indian, Alaska native, Hawaii, other)	2.20	1.1
Education (18 years and older)	High school certificate/diploma/Associate	29.52	57.7
	Bachelor	55.95	17.6
	Masters	7.93	6.5
	Doctoral	2.64	1.2
	Other (professional)	3.96	1.3
Income (census breakdown in parentheses)	< 12	5.80	(< 15 K) 12.7
	12–24	11.16	(15–24 K) 11.3
	24–50	35.27	(25–50 K) 23.9
	50–100	36.61	29.6
	Over 100	11.16	22.5

References

Ajzen, I., 1991. The theory of planned behavior. Organ. Behav. Hum. Decis. Process. 50 (2), 179–211.

Ajzen, I., 2012. The theory of planned behavior. In: In: Van Lange, P.A.M., Kruglanski, E., Higgins, E.T. (Eds.), Handbook of Theories of Social Psychology, vol. 1 Sage Publications Ltd., London.

Ajzen, I., Fishbein, M., 1980. Understanding Attitudes and Predicting Social Behavior. Prentice-Hall, Englewood Cliffs, NJ.

Allam, S., Flowerday, S.V., Flowerday, E., 2014. Smartphone information security awareness: a victim of operational pressures. Comput. Security (42), 56–65.

Anderson, C.L., Agarwal, R., 2011. The digitization of healthcare: boundary risks, emotion, and consumer willingness to disclose personal health information. Inf. Syst. Res. 22 (3), 469–490.

Anderson, J.C., Gerbing, D.W., 1988. Structural equation modeling in practice: a review and recommended two-step approach. Psychol. Bull. 103 (3), 411–423.

Babcock, C., 2016. Gartner: Enterprise Mobile Devices yet to Show Their Strength. Retrieved August 8, 2018, from < https://www.informationweek.com/strategic-cio/it-strategy/gartner-enterprise-mobile-devices-yet-to-show-their-strength-/d/d-id/1327594 > .

Bandura, A., 1977. Self-efficacy: toward a unifying theory of behavioral change. Psychol. Rev. 84 (2), 191–215.

Bélanger, F., Carter, L., 2008. Trust and risk in e-government adoption. J. Strategic Inf. Syst. 17 (2), 165–176.

Bélanger, F., Collignon, S., Enget, K., Negangard, E., 2011. User Resistance to Mandatory Security Implementation, IFIP WG8.11/11.13 Dewald Roode Workshop on Information Security, Blacksburg, VA.

Bélanger, F., Collignon, S., Enget, K., Negangard, E., 2017;al., in press. Determinants of early conformance with information security policies. Inf. Manage. 294 (in press).

Bélanger, F., Crossler, R.E., 2011. Privacy in the digital age: a review of information privacy research in information systems. MIS Q. 35 (4), 1017–1041.

Bélanger, F., Crossler, R.E., 2013. Research in progress: the privacy helper ©2013: a tool for mobile privacy. Workshop for Information Technology and Systems (WITS), Milan, Italy, 2013.

Bélanger, F., Hiller, J., Smith, W.J., 2002. Trustworthiness in electronic commerce: the role of privacy, security, and site attributes. J. Strategic Inf. Syst. 11 (3/4), 245–270.

Bélanger, F., Xu, H., 2015. The role of information systems research in shaping the future of information privacy. Inf. Syst. J. 26 (6), 573–578.

Blythe, J.M., Coventry, L., Little, L., 2015. Unpacking security policy compliance: the motivators and barriers of employees' security behaviors. Symposium on Usable Privacy and Security (SOUPS).

Boss, S., Kirsch, L., Angermeier, I., Shingler, R., Boss, R., 2009. If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security. Eur. J. Inf. Syst. 18 (2), 151–164.

Bulgurcu, B., Cavusoglu, H., Benbasat, I., 2010. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS Q. 34 (3), 523–548.

Census Bureau, 2013. 2010 Census of Population and Housing CPH-1-1. U.S. Department of Commerce, Washington, DC.

Chin, W., 1988. The partial least squares approach for structural equation modeling. In: Marcoulides, G.A. (Ed.), Modern Methods for Business Research. Lawrence Erlbaum Associates, Mahwah, NJ.

Chin, W.W., Peterson, R.A., Brown, S.P., 2008. Structural equation modeling in marketing: some practical reminders. J. Market. Theory Pract. 16 (4), 287–298.

Compeau, D., Higgins, C.A., Huff, S., 1999. Social cognitive theory and individual reactions to computing technology: a longitudinal study. MIS Q. 23 (2), 145–158.

Compeau, D.R., Higgins, C.A., 1995. Application of social cognitive theory to training for computer skills. Inf. Syst. Res. 6 (2), 118–143.

Conger, S., Pratt, J.H., Loch, K.D., 2013. Personal information privacy and emerging technologies. Inf. Syst. J. (23), 401–417.

Crossler, R., Long, J., Loraas, T., Trinkle, B., 2014. Understanding compliance with BYOD (Bring Your Own Device) policies utilizing protection motivation theory: bridging the intention-behavior gap. J. Inf. Syst. 28 (1), 209–226.

Crossler, R.E., Bélanger, F., 2009. The effects of security education training and awareness programs and individual characteristics on end user security tool usage. J. Inf. Syst. Security 5 (3), 3–22.

Crossler, R.E., Bélanger, F., 2014. An extended perspective on individual security behaviors: protection motivation theory and a Unified Security Practices (USP) instrument. ACM SIGMIS Database 45 (4), 51–71.

Crossler, R.E., Bélanger, F., 2017. The mobile privacy-security knowledge gap model: understanding behaviors. Proceedings of the 50th Hawaii International

Conference on System Sciences.

Crossler, R.E., Bélanger, F., Ormond, D., 2017;al., forthcoming. The quest for complete security: an empirical analysis of users' multi-layered protection from security threats. Inf. Syst. Front (forthcoming).

Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M., Baskerville, R., 2013. Future directions for behavioral information security research. Comput. Security 32 (1), 90–101.

CyberEdge Group, 2015. 2015 Cyberthreat Defense Report. Retrieved April 14, 2016, from < https://www.threattracksecurity.com/resources/2015-cyberthreat-defense-report.aspx > .

Dang-Pham, D., Pittayachawan, S., 2015. Comparing intention to avoid malware across contexts in a BYOD-enabled Australian University: a protection motivation theory approach. Comput. Security 48, 281–297.

Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., Colautti, C., 2006. Internet users' privacy concerns and beliefs about government surveillance: an exploratory study of differences between Italy and the United States. J. Global Inf. Manage. 14 (4), 57–93.

Dinev, T., Hart, P., 2006. An extended privacy calculus model for e-commerce transactions. Inf. Syst. Res. 17 (1), 61–80.

Dinev, T., Hu, Q., 2007. The centrality of awareness in the formation of user behavioral intention toward protective information technologies. J. Assoc. Inf. Syst. 8 (7), 386–408.

Dinev, T., McConnell, A.R., Smith, H.J., 2015. Research commentary—informing privacy research through information systems, psychology, and behavioral economics: thinking outside the "APCO" box. Information Systems Research 26 (4), 639–655.

Eschelbeck, G., Schwartzbert, D., 2012. BYOD Risks and Rewards. Retrieved April 24, 2013, from < http://www.sophos.com/en-us/security-news-trends/security-trends/byod-risks-rewards.aspx > .

Festinger, L., 1962. Cognitive Dissonance. Sci. Am. 207 (4), 93–107.

Fishbein, M., Ajzen, I., 1975. Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research. Addison-Wesley, Reading, MA.

Fornell, C., Bookstein, F., 1982. Two structural equation models: LISREL and PLS applied to consumer exit-voice theory. J. Mark. Res. (19), 440–452.

Fortinet. 2012. Fortinet® Global Survey Reveals 'First Generation' BYOD Workers Pose Serious Security Challenges to Corporate IT Systems. Retrieved April 27, 2013, from < http://www.fortinet.com/press_releases/120619.html > .

Franko, O.I., Tirrell, T.F., 2012. Smartphone app use among medical providers in ACGME training programs. J. Med. Syst. (36), 3135–3139.

Galluch, P.S., Grover, V., Thatcher, J.B., 2015. Interrupting the workplace: examining stressors in an information technology context. J. Assoc. Inf. Syst. 16 (1), 1–47.

George, J.F., 2004. the theory of planned behavior and internet purchasing. Internet Res. 14 (3), 198–212.

Grech, M., 2017. The State of Byod in 2017: How to Secure Your Security Nightmare. Retrieved August 7, 2018, from < https://getvoip.com/blog/2017/03/10/byod-in-2017/ > .

Gruman, G., 2015. Why the Boring Android M Is Good News for IT. Retrieved April 15, 2016, from < http://www.infoworld.com/article/2927411/android/why-the-boring-android-m-is-good-news-for-it.html > .

Herath, T., Chen, R., Wang, J.G., Banjara, K., Wilbur, J., Rao, H.R., 2014. Security services as coping mechanisms: an investigation into user intention to adopt an email authentication service. Inf. Syst. J. 24 (1), 61–84.

Herath, T., Rao, H., 2009. Protection motivation and deterrence: a framework for security policy compliance in organisations. Eur. J. Inf. Syst. 18 (2), 106–125.

Hern, A., 2015. Six Ways Your Tech Is Spying on You – and How to Turn It Off. Retrieved April 14, 2016, from < http://www.theguardian.com/commentisfree/2015/feb/10/six-ways-tech-spying-how-turn-off > .

Hong, W., Thong, J.Y.L., 2013. Internet privacy concerns: an integrated conceptualization and four empirical studies. MIS Q. 37 (1), 275–298.

Hu, Q., Hart, P., Cooke, D., 2007. The role of external and internal influences on information systems security - a neo-institutional perspective. J. Strateg. Inf. Syst. 16 (2), 153–172.

Ifinedo, P., 2012. Understanding information systems security policy compliance: an integration of the theory of planned behavior and the protection motivation theory. Comput. Security 31 (1), 83–95.

Jansson, J., Marell, A., Nordlund, A., 2011. Exploring consumer adoption of a high involvement eco-innovation using value-belief-norm theory. J. Consumer Behav. 10 (1), 51–60.

Jiang, Z., Heng, C.S., Choi, B.C.F., 2013. Privacy concerns and privacy-protective behavior in synchronous online social interactions. Inf. Syst. Res. 24 (3), 579–595.

Johnston, A.C., Warkentin, M., Siponen, M., 2015. An enhanced fear appeal rhetorical framework: leveraging threats to the human asset through sanctioning rhetoric. MIS Q. 39 (1), 113–134.

Keith, M.J., Thompson, S.C., Hale, J., Lowry, P.B., Greer, C., 2013. Information disclosure on mobile devices: re-examining privacy calculus with actual user behavior. Int. J. Hum Comput Stud. 71 (12), 1163–1173.

Kock, N., 2015. Common method bias in PLS-SEM: a full collinearity assessment approach. Int. J. e-Collaboration 11 (4), 1–10.

Krasnova, H., Spiekermann, S., Koroleva, K., Hildebrand, T., 2010. Online social networks: why we disclose. J. Inf. Technol. 25 (2), 109–125.

Kuzma, J.M., 2012. Children and geotagged images: quantitative analysis for security risk assessment. Int. J. Electron. Secur. Digit. Forensics 4 (1), 54–64.

Lam, T., Hsu, C.H., 2004. Theory of planned behavior: potential travelers from China. J. Hospitality Tourism Res. 28 (4), 463–482.

LaRose, R., Rifon, N.J., 2007. Promoting I-safety: effects of privacy warnings and privacy seals on risk assessment and online privacy behavior. J. Consumer Affairs 41 (1), 127–149.

Lee, J., Warkentin, M., Crossler, R.E., Otondo, R.F., 2017. Implications of monitoring mechanisms on bring your own device adoption. J. Comput. Inf. Syst. 57 (4), 309–318.

Li, H., Gupta, A., Zhang, J., Sarathy, R., 2014. Examining the decision to use standalone personal health record systems as a trust-enabled fair social contract. Decis. Support Syst. 57 (January), 376–386.

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. J. Manage. Inf. Syst. 27, 163–200.

MacKenzie, S.B., Podsakoff, P.M., Podsakoff, N.P., 2011. Construct measurement and validation procedures in MIS and behavioral research: integrating new and existing techniques. MIS Q. 35 (2), 293–334.

Madden, M., 2014. Public Perceptions of Privacy and Security in the Post-Snowden Era. Pew Internet and American Life Project.

Mahindru, R., 2013. Bring Your Own Device (BYOD): an empirical study across industries. CLEAR Int. J. Res. Commerce Manage. 4 (12), 54–57.

Malandrino, D., Scarano, V., Spinelli, R., 2013. Impact of privacy awareness on attitudes and behaviors online. Science 2 (2), 65–82.

Malhotra, N.K., Kim, S.S., Agarwal, J., 2004. Internet Users' Information Privacy Concerns (IUIPC): the construct, the scale, and a causal model. Inf. Syst. Res. 15 (4), 336.

McKnight, H., Choudhury, V., Kacmar, C., 2002. Developing and validating trust measures for e-commerce: an integrative typology. Inf. Syst. Res. 13 (3), 334–359.

Milne, G.R., Labrecque, L.I., Cromer, C., 2009. Toward an understanding of the online consumer's risky behavior and protection practices. J. Consumer Affairs 43 (3), 449–473.

Molok, A., Nuha, N., Chang, S., Ahmad, A., 2013. Disclosure of organizational information on social media: perspectives from security managers. Pacific Asia Conference on Information Systems (PACIS) 2013.

Mylonas, A., Meletiadis, V., Mitrou, L., Gritzalis, D., 2013. Smartphone sensor data as digital evidence. Comput. Security 38, 51–75.

Netemeyer, R.G., Johnston, M.W., Burton, S., 1990. Analysis of role conflict and role ambiguity in a structural equations framework. J. Appl. Psychol. 75 (April), 148–157.

Nunnally, J., 1978. Psychometric Theory. McGraw Hill, New York.

O'Connell, B., 2018. How to Manage Your Privacy Settings on Social Media. Retrieved April 27, 2018, from < https://www.experian.com/blogs/ask-experian/how-to-manage-your-privacy-settings-on-social-media/ > .

Olmstead, K., Smith, A., 2017. Americans and Cybersecurity. Retrieved September 27, 2017, from < http://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/ > .

Palanisamy, R., 2014. The impact of privacy concerns on trust, attitude and intention of using a search engine: an empirical analysis. Int. J. Electronic Bus. 11 (3), 274–296.

Pavlou, P.A., Fygenson, M., 2006. Understanding and predicting electronic commerce adoption: an extension of the theory of planned behavior. MIS Q. 30 (1), 115–143.

Pavlou, P.A., Gefen, D., 2005. Psychological contract violation in online marketplaces: antecedents, consequences, and moderating role. Inf. Syst. Res. 16 (4), 372–399.

Pavlou, P.A., Liang, H., Xue, Y., 2007. Understanding and mitigating uncertainty in online exchange relationships: a principal-agent perspective. MIS Q. 31 (1), 105.

Petter, S., Straub, D., Rai, A., 2007. Specifying formative constructs in information systems research. MIS Q. 31 (4), 623–656.

Podsakoff, P.M., MacKenzie, S.B., Lee, J.-Y., Podsakoff, N.P., 2003. Common method biases in behavioral research: a critical review of the literature and recommended remedies. J. Appl. Psychol. 88 (5), 879–903.

Rainie, L., Perrin, A., 2017. 10 Facts About Smartphones as the iPhone Turns 10. Retrieved April 27, 2018, from < http://www.pewresearch.org/fact-tank/2017/06/28/10-facts-about-smartphones/ > .

Ringle, C., Wende, S., Will, A., 2005. SmartPLS 2.0 (M3) Beta. University of Hamburg, Germany. < http://www.smartpls.de > .

Schwaig, K.S., Segars, A.H., Grover, V., Fiedler, K.D., 2013. A model of consumers' perceptions of the invasion of information privacy. Inf. Manage. 50 (1), 1–12.

Seebauer, S., 2015. Why early adopters engage in interpersonal diffusion of technological innovations: an empirical study on electric bicycles and electric scooters. Transport. Res. Part A: Policy Pract. 78, 146–160.

Sheehan, K.B., Hoy, M.G., 2000. Dimensions of privacy concern among online consumers. J. Public Policy Market. 19 (1), 62–73.

Sheng, H., Nah, F.F.-H., Siau, K., 2008. An experimental study on ubiquitous commerce adoption: impact of personalization and privacy concerns. J. Assoc. Inf. Syst. 9 (6), 344–376.

Sipior, J.C., Ward, B.T., Connolly, R., 2013. Empirically assessing the continued applicability of the IUIPC construct. J. Enterprise Inf. Manage. 26 (6), 661–678.

Smith, H.J., Dinev, T., Xu, H., 2011. Information privacy research: an interdisciplinary review. MIS Q. 35 (4), 989–1015.

Smith, H.J., Milberg, S.J., Burke, S.J., 1996. Information privacy: measuring individuals' concerns about organizational practices. MIS Q. 20 (2), 167–196.

Sørensen, C., Landau, J.S., 2015. Academic agility in digital innovation research: the case of mobile ICT publications within information systems 2000–2014. J. Strategic Inf. Syst. 24 (3), 158–170.

Stewart, K.A., Segars, A.H., 2002. An empirical examination of the concern for information privacy instrument. Inf. Syst. Res. 13 (1), 36–49.

Sullivan, B., 2018. Identity Theft Is Skyrocketing, and Getting More Sophisticated. Retrieved November 6, 2018, from < https://www.marketwatch.com/story/identity-theft-is-skyrocketing-and-getting-more-sophisticated-2018-02-27 > .

Sutanto, J., Palme, E., Tan, C.H., Phang, C.W., 2013. Addressing the personalization-privacy paradox: an empirical assessment from a field experiment on smartphone users. MIS Q. 37 (4), 1141–1164.

van der Meulen, R., Rivera, J., 2013. Gartner Predicts by 2017, Half of Employers Will Require Employees to Supply Their Own Device for Work Purposes. Retrieved August 8, 2018, from < https://www.gartner.com/newsroom/id/2466615 > .

Van Slyke, C., Shim, J.T., Johnson, R., Jiang, J., 2006. Concern for information privacy and online consumer purchasing. J. Assoc. Inf. Syst. 7 (6), 415–444.

Venkatesh, V., Morris, M., Davis, G.B., Davis, F.D., 2003. User acceptance of information technology: toward a unified view. MIS Q. 27 (3), 425–478.

Wang, N., Shen, X.-L., Sun, Y., 2013. Transition of electronic word-of-mouth services from web to mobile context: a trust transfer perspective. Decis. Support Syst. 54 (3), 1394–1403.

Wang, X., Weeger, A., Gewald, H., 2017. Factors driving employee participation in corporate BYOD programs: a cross-national comparison from the perspective of future employees. Aust. J. Inf. Syst. 21, 1–22.

Warkentin, M., Johnston, A.C., Shropshire, J., 2011. The influence of the informal social learning environment on information privacy policy compliance efficacy and intention. Eur. J. Inf. Syst. 20 (3), 267–284.

Weeger, A., Xuequn, W., Gewald, H., 2015. IT consumerization: BYOD-program acceptance and its impact on employer attractiveness. J. Comput. Inf. Syst. 56 (1), 1–10 (Fall2015).

Weisbein, J., 2018. Report: 53% Did Not Delete Facebook or Tighten Their Privacy Settings after Cambridge Analytica Scandal. Retrieved April 27, 2018, from < https://www.besttechie.com/report-majority-did-not-delete-facebook-or-tighten-their-privacy-settings/ > .

Woon, I.M.Y., Tan, G.W., Low, R.T., 2005. A protection motivation theory approach to home wireless security. In: Twenty-Sixth International Conference on Information Systems (ICIS), pp. 367–380.

Workman, M., Bommer, W.H., Straub, D.W., 2008. Security lapses and the omission of information security measures: a threat control model and empirical test. Comput. Hum. Behav. 24 (6), 2799–2816.

Xu, H., Bélanger, F., 2013. Information systems journal special issue on: reframing privacy in a networked world. Inf. Syst. J. 23 (4), 371–375.

Xu, H., Gupta, S., Rosson, M.B., Carroll, J.M., 2012. Measuring mobile users' concerns for information privacy. Thirty Third International Conference on Information Systems (ICIS). Association for Information Systems, Orlando, FL.

Xu, H., Luo, X., Carroll, J.M., Rosson, M.B., 2011. The personalization privacy paradox: an exploratory study of decision making process for location-aware marketing. Decis. Support Syst. 51 (1), 42–52.

Zahadat, N., Blessner, P., Blackburn, T., Olson, B.A., 2015. BYOD security engineering: a framework and its analysis. Comput. Security (55), 81–99.

Zhang, R., Chen, J.Q., Lee, C.J., 2013. Mobile commerce and consumer privacy concerns. J. Comput. Inf. Syst. 53 (4), 31–38.

Zhou, T., 2012. Understanding users' initial trust in mobile banking: an elaboration likelihood perspective. Comput. Hum. Behav. 28 (4), 1518–1525 2012/07/01/.