A Multiple-Motive Heuristic-Systematic Model for Examining How Users Process Android Data and Service Access Notifications

Tabitha L. James
Virginia Tech

Jennifer L. Ziegelmayer
IESEG School of Management

Arianna Schuler Scott
University of Oxford

Grace Fox
Dublin City University

Abstract

Android access notifications are presented to users to obtain permission to access data and services on smartphones. The number of "unsafe" apps in the Android marketplaces underscores the importance of understanding what factors influence whether users engage in more effortful systematic processing of access notifications. We propose a multiple-motive heuristic-systematic model to examine how different motives impact users' processing modes. We find that the need to be accurate in making decisions (accuracy), the desire to defend preferred positions (defense), and social pressure from others (impression) influence how users process Android access notifications, and they do so in different ways.

Keywords: Theory of Heuristic and Systematic Information Processing; Persuasion and Attitude Change; Dual-mode Processing Model; Android; Data and Service Access Notifications; Mobile Smartphone Security.

Introduction

During the process of downloading and installing software applications (apps) from the Android marketplaces, individuals are presented with requests to access data and services stored on their mobile device (i.e., access notifications). Faced with these access notifications, individuals must decide whether to install an app and permit the access the app requests or abort the installation if the access requests are deemed too invasive. Apps on the Android marketplaces are not strictly vetted, which results in the proliferation of malware (e.g., Doffman, 2019). In a marketplace that cannot guarantee app security, it is critical for individuals to understand the access requests that apps make because the security of the data stored on their smartphones relies on informed download decisions. Using cursory cues about an app's reliability (i.e., heuristic processing) or actively searching for information to better understand an access request (i.e., systematic processing) are two ways individuals may process Android access notifications to make better decisions. A first step in helping individuals make better data-access decisions lies in understanding the factors that influence this information processing. Therefore, our study seeks to understand (1) how users process Android data and service access notifications and (2) what factors drive the paths they take to validate these messages. We leverage the theory of heuristic and systematic information processing (Chaiken, 1980; Chaiken & Ledgerwood, 2012) to understand the circumstances under which individuals engage in heuristic or systematic processing of the Android access

notifications that are presented to them when downloading and installing apps.

Smartphones and their apps increasingly serve the everyday computing needs of individuals. More than three-quarters of Americans own a smartphone (Pew Research Center, 2018), and over half of smartphone users worldwide access the Internet through them (Statista: The Statistics Portal, 2018a, 2018b). Recent reports have found that one in five American adults rely on their smartphone as their only form of Internet access at home (Pew Research Center, 2018) and that Americans spend 5 hours a day on mobile devices (Perez, 2017). Smartphone users downloaded approximately 178.1 billion mobile apps in 2017 (Statista: The Statistics Portal, 2018d). The worldwide smartphone market is dominated by Android, which had a market share of 85 percent as of the first quarter of 2017 (International Data Corporation, 2018). There were 3.8 million apps on the Google Play Store as of the first quarter of 2018, compared to 2 million apps on the Apple App Store (Statista: The Statistics Portal, 2018c). Android users download approximately 4.1 apps per month with an average of 3.4 being free offerings (Forrest, 2014).

The increasing use of smartphones and their apps leads to vast amounts of sensitive personal and business information being generated and stored on these devices (Honan, 2013; Isaac, 2011). Apps need to use data and services (e.g., photos, contacts, camera services, or location services) native to the smartphone and share data between apps to provide functionality that users desire. For example, data and service sharing are required when users want to post photos taken using their smartphones on Instagram or share posts from Instagram directly to Facebook. The U.S. Federal Trade Commission (FTC) warns consumers that "some apps access only the data they need to function; others access data that's not related to the purpose of the app," indicating that apps may access "your phone and email contacts, call logs, internet data, calendar data, data about the device's location, the device's unique IDs" (U.S. Federal Trade Commission, 2017). For Android apps, a message-passing mechanism referred to as inter-component communication (ICC) allows apps to access the location of a user's smartphone and pass this information on to a second app, which might then send it to an external server (Bosu et al., 2017). Such data sharing between apps can be purposeful and facilitate greater functionality, but it can also be the result of poor programming or malicious intent (Bhandari et al., 2017; Bosu et al., 2017). Smartphone users must try to determine which app access requests are purposeful and which are excessive or malicious.

The number of malicious Android apps has increased from half a million in 2013 to almost 3.5 million in 2017 (Sophos, 2017), with one report stating that "Android has more vulnerabilities because of its inherent open-source nature, the slow pace with which users update the OS and a lack of proper app vetting" (Mearian, 2017, p. 1). Malicious apps downloaded and installed from the app marketplace can compromise the data on smartphones. Information-sharing requests between apps may have malicious intent and lead to negative privacy or security events (Bhandari et al., 2017; Bosu et al., 2017), which occur when new apps downloaded onto an individual's smartphone maliciously access data from existing apps. Careful consideration of the access notifications is thus of vital importance to prevent downloads of malicious apps and protect smartphone data. In the present study, we focus on app access notifications presented when users download and install apps on the Android platform. We concentrate on the Android platform because it currently holds the larger share of the mobile market, it is more susceptible to vulnerabilities, and, unlike iOS apps, when an Android app is installed it immediately asks for access permissions (see Figure 1). While it is important for users to evaluate the information and service-sharing requests on all platforms, it represents a crucial concern on the popular and open Android platform.

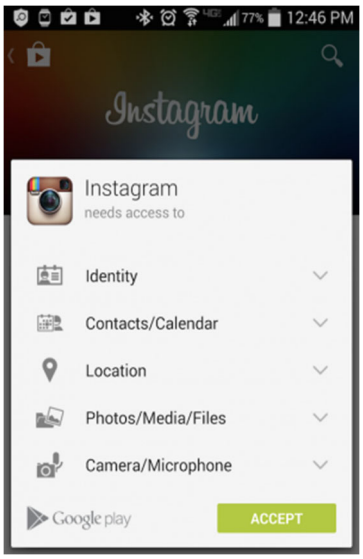

Figure 1. Example of Android Access Notification

The multiple-motive heuristic-systematic model (HSM) argues that there are three motivations that drive individuals seeking valid judgments: accuracy, defense, and impression (Chaiken & Ledgerwood, 2012). Based on the original HSM, the accuracy motive refers to individuals' desires to make accurate judgments or, in our case, to understand the access requests apps are making. The defense motive refers to individuals' desires to defend and confirm favored positions. The impression motive refers to the desire of individuals to be seen as holding positions that are

socially acceptable. The latter two motives reflect biases towards attitudinal positions. For example, an individual who desires to use a particular app may prefer not to know information suggesting the app might not be safe to install. In this case, the individual's motivation to understand the access notifications may be diminished by the desire for the app. Therefore, to defend the desired action (i.e., to download the app), the individual will be less likely to seek out information because it might provide a reason not to take that desired action. In developing a multiple-motive HSM for Android access notifications, we propose that individuals may be biased towards 1) protection of their privacy or 2) possessing the apps. Moreover, we suggest that these motives have differing effects on the type of information processing (heuristic or systematic) that individuals conduct. The question of concern in this paper thus becomes – how do accuracy, defense, and impression motivations lead to heuristic or systematic processing of Android access notifications?

We find that systematic and heuristic processing are indeed driven by different motives. Privacy concern does not drive systematic processing. However, privacy protection as a defense motive (i.e., prior privacy victimization) or impression motive (i.e., important others considering privacy to be important) does drive systematic processing. Additionally, individuals who do not feel they have sufficient information to evaluate Android access notifications yet feel they are capable of gathering additional information to help assist their understanding will employ systematic processing. These results illustrate that the desire to make accurate decisions will drive more effortful processing. In contrast, valuing the app over one's privacy will decrease the likelihood of systematic processing. If potential users strongly desire the app, they will not search for information because they may find information that could dissuade them from possessing the app. Individuals who are concerned about their privacy and feel they are capable of gathering additional information to assist their understanding of Android access notifications will employ heuristic processing. Potential users who strongly desire the apps or who feel social pressure to obtain them are also more likely to use heuristic cues. Our findings provide insight into how different motives result in different modes of information processing of Android access notifications, which has implications for both researchers and practitioners.

Our study places the HSM firmly in an information security context by exploring the effects of accuracy, defense, and impression motivations on the ways in which individuals process access notifications (i.e., heuristically or systematically). We contribute to the HSM literature by testing multiple defense and impression motivations (i.e., protection of privacy and possession of the app) against heuristic and systematic processing in a unique context. This paper also advances the privacy literature by answering the call to consider information processing (Dinev et al., 2015) and extending HSM theory to the context of privacy and access notification processing. Our findings provide insight into what factors influence the way individuals process access notifications. This has practical implications: by understanding the motivations that influence the processing of access notifications, app makers and platform providers can design more effective access notifications to assist potential users in distinguishing benevolent apps from malicious ones. Moreover, an improved understanding of what factors lead to systematic processing can be used to develop training and educational programs designed to reinforce inclinations towards privacy protection and counteract biases that favor poor security practices.

Theoretical Development

We use the theory of heuristic and systematic information processing as the foundation to develop our model to examine how individuals evaluate data and service access notifications on Android smartphones. In the sections below, we first provide an overview of the theory of heuristic and systematic information processing (Chaiken & Ledgerwood, 2012). We then develop the argumentation for the hypotheses and present the multiple-motive HSM for Android access notifications.

The Theory of Heuristic and Systematic Information Processing

The theory of heuristic and systematic information processing was first proposed by Chaiken (Chaiken, 1980, 1987; Chaiken et al., 1996; Chaiken et al., 1989). The multiple-motive HSM is classed as a dual-mode processing model within the field of persuasion and attitude change in social psychology (Wood, 2000). The core of the theory defines two types of information processing: heuristic and systematic. Heuristic processing refers to a situation in which "people exert little cognitive effort in judging the validity of a persuasive message and, instead, may base their agreement with a message on a rather superficial assessment of a variety of extrinsic persuasion cues" (Chaiken, 1987, p. 3). This means that when individuals heuristically process, they rely on simple rules and easily available information cues to guide their judgements. Individuals may heuristically process, for example, by following a simple heuristic rule to not download apps from unknown companies. As another example, they may also use easily available heuristic cues such as the star ratings of

apps to assist their decision-making. These are non-content cues because they do not explain the specific access requests the apps are making or the consequences of accepting the access requests. Heuristic processing is thus a security behavior because the individual is attempting to use easily available informational cues to vet the app maker and the app. However, it is not the ideal mode of processing because the individual may not understand the access request or the consequences of accepting it.

Systematic processing is defined as "a comprehensive, analytic orientation in which perceivers access and scrutinize all information input for its relevance and importance to their judgment task" (Chaiken et al., 1989). Examples of systematic processing in the literature include reading magazine and newspaper articles (Chaiken & Ledgerwood, 2012) or asking an expert (Chaiken et al., 1996) about the topic before rendering a decision or judgment. In our context, examples of systematic processing of the access notification in Figure 1 include clicking on each of the down arrows to read about the request (e.g., what does "Photos/Media/Files" mean exactly?), asking someone who they feel is knowledgeable (e.g., the information technology (IT) person at work), or going on the Internet to research the request (e.g., Googling why Instagram would need access to "Photos/Media/Files"). Such methods of evaluating access requests are more effortful and time-consuming than simply making a judgment from the available heuristic cues. To best protect one's data on a smartphone, systematic processing, which involves searching for context-relevant information to fully understand the access request, would be the preferred security behavior.

The Multiple Motive Heuristic-Systematic Model

The original premise of HSM was that individuals want to make accurate judgments and that their motivation in seeking out and consuming data to inform decisions is motivated by this desire. At the core of the HSM model is the concept of *information sufficiency*, described by Trumbo (2002, p. 370) as the "degree to which the individual feels that information needs for this specific decision-making circumstance have been satisfied." In our context, information sufficiency measures whether individuals feel they have the information they need to evaluate Android access notifications. Trumbo (2002) argued that information sufficiency needs to be accompanied by 1) feelings that the issue at hand is important and 2) the perceived ability to obtain additional information to assist decision-making. We follow Trumbo (2002) to model the core HSM that addresses individuals' accuracy motivations.

The accuracy motive was the focus of earlier work, but additional motives were added to HSM over time that have not received as much attention in the literature. The multiple-motive framework of HSM considers three motives: accuracy, defense, and impression (Chaiken & Ledgerwood, 2012; Chen et al., 1999). The theory of heuristic and systematic information processing suggests that all three motivations may influence information processing. However, the theory posits that accuracy motives lead to open-minded evaluation of information, whereas defense and impression motives bias information processing in favor of a particular decision (Chaiken & Ledgerwood, 2012). In our context, we argue that there are two pressures that might bias individuals' information processing: 1) pressure to protect their privacy and 2) pressure to possess the desired apps. We extend the core HSM by including defense and impression motives that may influence how individuals process Android data and service access notifications. In what follows, we first develop the hypotheses for the core HSM model, followed by those for the multiple-motive extension.

The Core Heuristic-Systematic Model: Motivation to Make Accurate Decisions

Several studies have examined how information sufficiency leads to heuristic and systematic processing in different contexts. Trumbo (1999, p. 396), in a study of cancer risk perceptions, found that individuals who felt they had sufficient information were more willing to engage in heuristic processing and less likely to systematically process. We follow this logic in the current study to propose that individuals who feel they have sufficient information will conduct heuristic processing but not systematic processing. In a subsequent study, Trumbo (2002) found that information sufficiency was a strong predictor of heuristic processing, but that it had a weakly significant ($p < 0.10$) negative relationship with systematic processing. Trumbo posited that "information sufficiency (having enough information) should be positively associated with heuristic processing." He put forth that the proposed positive association between information sufficiency and heuristic processing "is based on the argument that insufficient levels of judgmental confidence occurring under circumstances of information insufficiency will more strongly motivate systematic processing" (Trumbo, 1999, pp. 392-393).

In the information systems (IS) literature, HSM has been applied to examine IS exceptions (i.e., extreme software errors that cannot be routinely handled), phishing attacks, and cross-site scripting (Davis & Tuttle, 2013; Luo et al., 2013; Zhang et al., 2013). In their study of IS exceptions, Davis and Tuttle (2013)

proposed a decomposed view of information sufficiency, breaking it into two components: desired confidence and actual confidence. Their findings revealed that desired confidence was positively associated with systematic processing, whereas actual confidence had a negative impact on systematic processing. However, they did not include heuristic processing in their model. In another study exploring information seeking behaviors related to cross-site scripting for websites, Zhang et al. (2013) found a positive, significant relationship between information insufficiency and web risk information seeking intention.

Griffin et al. (1999b) found that individuals with higher levels of information insufficiency were more likely to systematically process and less likely to heuristically process, as did Griffin et al. (2005), Griffin et al. (2008), and Kahlor et al. (2006). Although some authors examine information insufficiency (i.e., not having enough information) (e.g., Griffin et al., 1999b), their findings are consistent with those examining information sufficiency (i.e., having enough information) (e.g., Trumbo, 2002). Specifically, the findings indicate when an individual feels that they have enough information to make an accurate decision, they will be less likely to go in search of additional information and will rely on heuristic cues. Trumbo (2002, p. 371) explains this relationship by reasoning that individuals may "economically make quick use of what they already know and perhaps also make use of a larger store of heuristic cues." By contrast, if individuals do not feel they have sufficient information to evaluate Android data and service access notifications, they will be more likely to conduct systematic processing to collect and consume additional information. Therefore, we propose the following hypotheses:

> Hypothesis 1a (H1a): Information sufficiency will be negatively associated with systematic processing.
>
> Hypothesis 1b (H1b): Information sufficiency will be positively associated with heuristic processing.

Trumbo (2002) proposes that for information sufficiency (or insufficiency) to be of concern to individuals, the issue being evaluated must be important to them. He thus reasons that individuals' perceptions of information sufficiency may differ depending on how important the issue is to them. In our context, this means users who feel the privacy of the information on their Android smartphones is important are more likely to feel they lack sufficient information about Android access notifications. To reduce their perceived information deficit, individuals who value their privacy are more likely to engage in both heuristic and systematic processing. Trumbo (2002, p. 371) argues that a negative relationship between issue importance and information sufficiency will exist because those "who feel most strongly that the issue is important […] will, on average, have higher levels of desired judgmental confidence." Individuals who are deeply concerned about their privacy will be driven to make an accurate decision, whereas those with lower concerns for privacy may feel that they have sufficient information to evaluate Android access notifications.

Trumbo (1999, 2002) found a positive, significant relationship between issue importance and systematic processing in both of his studies. Furthermore, in the IS literature it has been demonstrated that individuals' concern for their privacy often leads users to report intentions to engage in more effortful privacy protecting behaviors (Son & Kim, 2008). These practices include refusal to provide information, removal of information from databases, negative feedback about companies that mishandle information, and complaints to the company itself or third-party organizations (Son & Kim, 2008). Research has also revealed that individuals who report higher privacy concerns are less likely to report intentions to use online services or share personal information and are more likely to adopt privacy protection measures (Baruh et al., 2017). Privacy concerns have also been shown to negatively impact download intentions for mobile apps (Gu et al., 2017). Hence, privacy-concerned individuals are more cautious and rely on stronger privacy protection behaviors. Seeking more information about Android access notifications is a privacy protection behavior that helps cautious individuals make more informed decisions. In fact, Youn (2009, p. 389) found that privacy concerns impacted "risk-coping behaviors such as seeking out interpersonal advice or additional information (e.g., privacy statements) or refraining from using Web sites that ask for personal information." Systematic processing occurs when individuals exert effort to seek out advice and additional information. Therefore, there is precedent to propose that individuals with high Android privacy concerns will be more likely to seek out and consume information.

Trumbo (1999) found inconsistent results between issue importance and heuristic processing. In his first study, the relationship between issue importance and heuristic processing was insignificant. In his second study, Trumbo (2002) proposed a negative relationship between the importance of the issue and heuristic processing and found a significant, but positive, relationship. We propose that individuals with high issue importance will be more likely to rely on heuristic processing. We base this logic on the prior finding of a positive relationship between issue importance and heuristic processing (Trumbo, 2002) and on the finding

that individuals may use both processing modes to arrive at a judgment (Chaiken et al., 1989). Heuristic cues may provide indications that apps being downloaded and installed come from trusted sources and are well-regarded by other consumers (i.e., star ratings and source credibility). Potential users who have high levels of privacy concern are likely to be sensitive to such cues.

To summarize, we propose that individuals who are concerned for the privacy of their information on Android devices (i.e., have high issue importance) will be less likely to report information sufficiency and more likely to rely on both heuristic and systematic processing of Android access and service notifications. Therefore, we propose the following hypotheses:

> Hypothesis 1c (H1c): Android privacy concerns will be negatively associated with information sufficiency.
>
> Hypothesis 1d (H1d): Android privacy concerns will be positively associated with systematic processing.
>
> Hypothesis 1e (H1e): Android privacy concerns will be positively associated with heuristic processing.

Trumbo (2002) proposes that the ability to obtain additional information to make a more accurate decision is positively associated with information sufficiency. Specifically, he proposes that "those who report higher levels of self-perceived ability to acquire and handle information will also have most likely achieved greater information sufficiency" (Trumbo, 2002, pp. 370-371). This means that individuals who feel able to locate information about Android access notifications are going to be more likely to do so and thus be less likely to feel they have inadequate information. Following this logic, we also posit that individuals who are confident in their ability to gather information about Android access requests will have higher levels of information sufficiency. Therefore, we propose the following hypothesis:

> Hypothesis 1f (H1f): Information gathering capacity will be positively associated with information sufficiency.

Although the terminology used to refer to an individual's information gathering capacity has been inconsistent, HSM models often include a "capacity" construct to examine whether individuals believe they are "able" to engage in systematic processing (e.g., know whom to ask and where to look for information to assist their decisions). In various studies, "capacity" (Griffin et al., 1999a; Griffin et al., 1999b) has been referred to as "ability" or "self-efficacy" (Johnson, 2005; Trumbo, 1999, 2002). Trumbo (2002, p. 379) explored the influence of capacity, which he referred to as "information-gain self-efficacy," and found it to have only a weakly significant positive effect on systematic processing. However, while the impact of capacity on systematic processing was weak, Trumbo (2002, p. 379) found that "being 'information able' was a good predictor of the use of heuristic shortcuts in decision making." In another study, Trumbo (1999) found "self-efficacy for judgment" to positively predict both heuristic and systematic processing. These findings illustrate that individuals who feel they have the ability to obtain information to help inform decisions are more likely to use the heuristic cues available and to conduct more effortful searches to uncover information.

Other researchers have explored information gathering capacity to measure whether individuals were "able" to obtain information regarding the decisions with which they were faced. Drawing from Eagly and Chaiken (1993), Griffin et al. (1999b, p. 4) used the term "perceived information gathering capacity" to refer to individuals' assessments of their ability to learn more about a decision. They posited a positive effect of perceived information gathering capacity on systematic processing, but their findings did not support the relationship. They also hypothesized a negative relationship between information gathering capacity and heuristic processing and found the opposite. However, in subsequent studies, Griffin et al. (2005) and Griffin et al. (2008) found support for the propositions that information gathering capacity increased the likelihood of systematic processing and decreased the likelihood of heuristic processing. Although these studies provide evidence in support of a positive association between information gathering capacity and systematic processing and a negative association between information gathering capacity and heuristic processing, other findings regarding these associations have been mixed. For example, Zhang et al. (2013) found no significant relationship between perceived information gathering capacity and risk information seeking intention; yet, Kim and Paek (2009) found positive relationships between information gathering capacity and both heuristic and systematic processing.

Research consistently supports a positive relationship between information gathering capacity and systematic processing (Griffin et al., 2005; Griffin et al., 2008; Kim & Paek, 2009). Individuals who know what questions to ask and whom they should ask when seeking information about Android access requests are more likely to conduct effortful information seeking. Conversely, individuals who do not feel capable of gathering information to help interpret Android access notifications will be unlikely to attempt to do so. We posit that individuals who have a high level of perceived information gathering capacity will be more

likely to engage in systematic processing, which is in accordance with prior findings of a positive association between capacity (i.e., ability) and systematic processing (Griffin et al., 2005; Griffin et al., 2008; Kim & Paek, 2009).

Some studies have found a negative association between information gathering capacity and heuristic processing (Griffin et al., 2005; Griffin et al., 2008), yet others have found a positive association (Griffin et al., 1999b; Kim & Paek, 2009). According to the theory of heuristic and systematic processing, the two modes are not mutually exclusive (Chaiken & Ledgerwood, 2012; Johnson, 2005). Individuals who conduct effortful searches for information to assist their decisions, such as asking questions of an IT professional or searching for information on the Internet, are unlikely to ignore or dismiss available heuristic cues. In our context, it is likely that heuristic cues, such as star ratings or app maker credentials, provide supporting information that may also be useful to individuals' decision-making processes. Individuals who feel that they are capable of gathering information to help support their decisions are likely to also make use of easily available information (i.e., heuristic cues). Moreover, research has uncovered a positive association between information gathering capacity and heuristic processing (Griffin et al., 2005; Griffin et al., 2008). Trumbo (2002, p. 379) suggested that being "information able" promoted a "willingness to use heuristics." Based upon this logic, we propose that higher levels of information gathering capacity will result in higher levels of heuristic processing. Therefore, we propose the following hypotheses:

> Hypothesis 1g (H1g): Information gathering capacity will be positively associated with systematic processing.
>
> Hypothesis 1h (H1h): Information gathering capacity will be positively associated with heuristic processing.

HSM Multiple-Motive Extensions: Defense and Impression Motivations

As the theory of heuristic and systematic information processing advanced, Chaiken and her coauthors (Chaiken et al., 1996; Chaiken & Ledgerwood, 2012; Chaiken et al., 1989; Chen & Chaiken, 1999) added the defense and impression motivations to complement the accuracy motivation. Defense motivation is described as "the desire to hold attitudes and beliefs that are congruent with one's perceived material interests or existing self-definitional attitudes and beliefs" (Chen & Chaiken, 1999, p. 77). Impression motivation is described as "the desire to hold attitudes and beliefs that will satisfy current social goals" (Chen & Chaiken, 1999, p. 78), and the multiple-motive HSM posits that individuals desire to "express attitudes that are socially acceptable" (Chaiken & Ledgerwood, 2012, p. 249). The accuracy motivation reflects a desire to make the correct decision, whereas the defense and impression motivations reflect desires to make the preferred or socially acceptable decisions, respectively. The biases inherent to defense and impression motives result from either internal pressure (i.e., what the individual desires) or external pressures (i.e., what others who are important to the individual what them to do).

In the Android context, we posit that individuals may desire or feel social pressure to 1) protect their privacy or 2) possess apps. Defense motives reflect biases that could influence how an individual processes information. An individual who has previously fallen victim to a security breach may feel motivated to defend his or her privacy and thus be more likely to rely on strong security behaviors to protect his or her information on a smartphone. Conversely, individuals may strongly desire to use the apps they are considering downloading and installing, which may limit the effort they put into searching for information that may provide reasons not to install the apps. In this case, individuals may be less likely to rely on strong privacy behaviors that may uncover reasons not to obtain the desired apps.

Impression motives also reflect biases that may impact information processing. One way that impression motives have been incorporated into HSM in the literature is as a social influence mechanism through which perceived social pressure from important others influences individuals' behaviors (e.g., Dunwoody & Griffin, 2015). Others who are important to an individual (e.g., coworkers, family members) may be perceived to value privacy protection (i.e., social pressure), and this perceived social norm may result in stronger security behaviors. Conversely, important others may pressure individuals to obtain apps and that social pressure may result in less reliance on stronger security behaviors. Therefore, we posit that bias towards protecting privacy will result in more effort to obtain directly relevant information to assist the interpretation of access notifications and the consequences of accepting them (i.e., systematic processing). Conversely, we posit that bias towards obtaining apps will make individuals less likely to conduct systematic processing and more likely to rely on heuristic cues that may reinforce the social acceptability of the apps (e.g., user reviews, star ratings).

Defense and Impression Motivations: Pressures to Protect Privacy

We posit that prior privacy victimization is one potential source of bias. Having experienced a privacy violation,

individuals may be more inclined to feel protecting their privacy is important because their understanding of the consequences of not doing so has improved. The HSM literature similarly considers prior experience with hazards. Griffin et al. (1999a), following Grunig (1983), suggest that individuals employ referent criteria based upon past experiences to determine current behaviors. Specifically, they argue that past experiences with a hazard or even past experience with preventative mechanisms to avoid the hazard might influence behavior.

The results from an elaboration likelihood model (ELM) study in the IS literature found that justifying a permission request reduced privacy concern only for individuals that had less experience as a privacy victim (Gu et al., 2017). The ELM is a dual-mode information processing model similar to HSM that has become popular in the IS literature (e.g., Angst & Agarwal, 2009; Gu et al., 2017; Kim & Benbasat, 2009; Lowry et al., 2012; Puhakainen & Siponen, 2010). The results of the study by Gu et al. (2017) lend support to the assertion that individuals who have prior experience as a privacy victim may need more than simple heuristic cues to assist their decision-making process with regard to Android access notifications.

In a study of optimistic bias with regard to online privacy risks, the authors argued that individuals who have not been victimized tend to think that the world is safe, whereas victims see the world as a more dangerous place (Cho et al., 2010). Using this reasoning, they examined prior privacy victimization as a moderator of optimistic bias regarding online privacy risk and found that increased levels of privacy victimization resulted in increased perceptions of personal and societal vulnerability (Cho et al., 2010). Prior experience as a privacy victim therefore reduces perceptions of invulnerability to privacy risks and may lead such individuals to put more effort into determining the meaning and consequences of Android access notifications. Following this logic, we propose that individuals with past privacy invasion experiences will be more likely to conduct systematic processing of Android access notifications. Therefore, we propose the following hypothesis:

> Hypothesis 2a (H2a): Prior experience of being a privacy victim will be positively associated with systematic processing.

In the HSM literature, it has been shown that impression-motivated participants are more likely to "go along to get along" and that this tendency will bias their systematic processing (Chen et al., 1996, p. 262). One operationalization of the impression category of motivation is via the concept of subjective norm (e.g., Dunwoody & Griffin, 2015), which is defined as "the person's perception that most people who are important to him think he should or should not perform the behavior in question" (Fishbein & Ajzen, 1975, p. 302). Studies in IS have explored different normative pressures in relation to security and privacy behaviors. For example, subjective and descriptive norms were both found to have positive impacts on security policy compliance intention (Herath & Rao, 2009). Subjective norm was used in the heuristic-systematic information processing context by Davis and Tuttle (2013), who did not consider a multiple-motive model but instead used subjective norm as an antecedent to accuracy concerns in the context of IS exceptions. Dunwoody and Griffin (2015, p. 113) tested informational subjective norms, which they defined as "the perception that others believe one should learn about [impersonal risks]." They argued that even if individuals feel no personal involvement with a particular topic, such as an environmental issue, they nonetheless "may ramp up their information seeking and processing behaviors when they believe that others feel they should do so" (Dunwoody & Griffin, 2015, p. 113). In fact, they found that informational subjective norms had a significant, positive effect on systematic processing and a negative impact on heuristic processing (Dunwoody & Griffin, 2015).

Griffin et al. (1999b, p. 3) argue "one's perception that valued others expect one to keep on top of information about the risk (the subjective normative component) could also affect one's judgment about how much information one needs to have about the risk." In several of their models, they suggest that the subjective norm influences information processing through information sufficiency. However, Griffin et al. (2005) tested the relationship between informational subjective norms and heuristic and systematic processing directly. They found informational subjective norms to have a significant positive influence on systematic processing, but a significant negative influence on heuristic processing, as did Griffin et al. (2008). In addition, Kahlor et al. (2006) found a positive relationship between informational subjective norms and systematic processing, as well as a negative relationship between informational subjective norms and heuristic processing. Describing the Kahlor et al. (2006) study, Griffin et al. (2005, p. 12) state that "a respondent's perception that others expected her/him to 'stay on top of information' […] was by far the strongest predictor of that individual's likelihood of engaging in more effortful seeking and processing of information about that threat." Kahlor (2007) also found a significant, positive relationship between informational subjective norms and behavioral intent to seek information. Additionally, Zhang et al. (2013) found informational subjective norms to be a positive, significant predictor of risk information seeking intention in the cross-site scripting context.

We thus follow the multiple-motive approach suggested in Chaiken and Ledgerwood (2012) and the logic of Griffin et al. (2005) and Zhang et al. (2013) to suggest that individuals may experience normative pressure to protect the privacy of the information on their Android smartphones. Moreover, we posit that the normative pressure to protect the privacy of the information on Android smartphones will increase the likelihood of systematic processing of Android access notifications. For example, an individual may discuss the downsides of apps sharing data for marketing purposes with a privacy-conscious friend or family member. Such conversations, formal or informal, may cause users to feel social pressure to protect the personal information on their Android smartphone. We propose individuals will engage in more effortful systematic processing, such as looking up the details of the access notification or asking an expert, if the importance of protecting the information on the Android smartphone is socially reinforced by important others. Therefore, we propose the following hypothesis:

> Hypothesis 2b (H2b): Privacy protection subjective norm will be positively associated with systematic processing.

Defense and Impression Motivations: Pressures to Possess Apps

Individuals may also feel internal or external pressure to possess apps. Whether stemming from an internal desire or external social pressure, pressures to possess apps should bias individuals in a manner opposite to pressures to protect privacy. Pressures to protect privacy should lead to more effortful processing to collect and consume information that will explain the access notifications and their consequences. Conversely, pressures to possess apps should discourage individuals from searching for information that could potentially provide evidence against obtaining the apps they desire.

The theory of heuristic and systematic information processing argues that heuristic cues will be considered sufficient unless an individual is motivated to conduct systematic processing (Chaiken et al., 1989). Research on the defense motivation of the multiple-motive HSM indicates that in situations where defense motives are present, the occurrence of systematic processing depends on whether heuristic cues support or contradict the individual's preference (Giner-Sorolila & Chaiken, 1997). Specifically, it has been argued that "if the information is congenial, heuristic processing is likely to confer sufficient defensive confidence, so that systematic processing will be minimal or unnecessary," but that if "heuristic information is [unsupportive of the] individual's preferred conclusion […] individuals will be more likely to engage in biased systematic processing of information" (Giner-Sorolila & Chaiken, 1997, p. 86). For example, if the heuristic cues provide support for downloading and installing the app (e.g., high star ratings), then the potential user can use the cues to justify doing so without seeking further information on the access requests. Conversely, if the heuristic cues contradict the individual's preference to obtain the app (e.g., low star ratings), then the individual may go in search of information that will support their desire to obtain the app. Thus, the desire for apps will likely result in minimal information processing (i.e., weaker security behaviors) as long as the heuristic cues support the preferred decision (e.g., high star ratings, good company reputation). Following this logic, pressures to download apps may reduce the likelihood of more effortful (i.e., systematic) information processing to avoid information that could include reasons not to obtain the desired apps.

To examine internal pressure to possess apps, we borrow the concept of the privacy calculus from the IS literature (Dinev & Hart, 2006; Li, 2012; Pavlou, 2011). The privacy calculus examines the extent to which individuals are willing to trade one value (e.g., privacy) to obtain benefits or objects of desire (e.g., apps). In our context, individuals must relinquish some control over their information to obtain something they want (i.e., apps). The privacy calculus has been extensively studied in the IS literature (Li, 2012) and typically leads to individuals disclosing information (e.g., Dinev & Hart, 2006; James et al., 2015; Keith et al., 2013), which is an undesirable security behavior. We expect that individuals who favor apps more than their privacy will find heuristic cues sufficient.

Dinev and Hart (2006) operationalized the privacy calculus concept as *personal Internet interest* in their study of e-commerce transactions. We similarly call our construct *personal app interest* and use it to examine the impact of internal pressure (desire) for apps on individuals' information processing modes. Dinev and Hart (2006) found that personal Internet interest had a positive impact on the intention to disclose personal information to conduct a transaction over the Internet. James et al. (2015) similarly used this concept to explore information and interaction management behaviors in online social networks (OSN). They explored four different benefits (i.e., information seeking, socialization, self-expression, and pleasing others) for which users might trade some of their privacy. They argue that the desire to seek information, socialize, express oneself, or please others may be more desired than users' privacy, leading users to meet their needs by releasing information to others on the OSN.

The defense motivation suggests that individuals will try to defend their preferred decision (e.g., to obtain

apps) (Chaiken & Ledgerwood, 2012). The privacy calculus posits that individuals may accept that they are trading something they value (e.g., some of their information) for something else they value more (e.g., apps) (Dinev & Hart, 2006). The more individuals accept this trade-off, the less likely they will be to go in search of information that might be unsupportive of their preferred action. In the e-commerce study by Dinev and Hart (2006), personal Internet interest made users more likely to provide personal information even when privacy concern was shown to decrease the likelihood of providing that same information. Similarly, individuals who report high levels of personal app interest have no need to seek out and consume information regarding access notifications because they have already determined what they want to do and are willing to accept the negative consequences.

We propose that desire for apps will influence how individuals process information related to Android access notifications. Specifically, we propose that individuals who are willing to relinquish some control over their information to possess apps will be less likely to systematically process. Moreover, we propose that individuals who desire to possess apps will be more likely to rely on heuristic cues. Therefore, we propose the following hypotheses:

> Hypothesis 3a (H3a): Personal app interest will be negatively associated with systematic processing.
>
> Hypothesis 3b (H3b): Personal app interest will be positively associated with heuristic processing.

IS research has examined different normative pressures in relation to adoption behaviors for Internet-enabled smartphones and smartphone applications. Social influences (i.e., subjective norm and image) were found to have an impact on the perceived usefulness and ease of use of wireless Internet services via mobile technology (Lu et al., 2005). Additionally, Teo and Pok (2003) found subjective norm to have a positive influence on the adoption of wireless application protocol-enabled phones. Dai and Palvi (2009) also found subjective norm to have a positive impact on the use of mobile commerce. Moreover, a knowledge sharing subjective norm was found to have a positive impact on intention to share knowledge (Chow & Chan, 2008). Research has thus indicated that not only may individuals feel social pressure to protect their privacy, but they may also feel social pressure to adopt and use technology. In our context, important others may recommend apps to individuals. For example, a person may find an app that they feel does a great job editing photos and may recommend it to friends. Notably, some apps are social (e.g., OSNs, games), and important others may encourage individuals to obtain these apps to further social communication and interaction.

The role of important others in influencing individuals to adopt technologies has been the subject of much research. The idea that important others could influence individuals' technology adoption decisions is a component of the technology acceptance models in the IS literature (Venkatesh & Davis, 2000; Venkatesh et al., 2003; Venkatesh et al., 2016). While personal app interest represents internal pressure to obtain apps, app subjective norm represents external pressure (i.e., perceived pressure from important others to possess apps). We posit that external pressure to possess apps will reduce the likelihood of individuals going in search of information that may be unsupportive of the socially desirable position of possessing the apps. This logic follows findings in the IS adoption literature that indicate users are more likely to use technology if they perceive social pressure to do so (e.g., Teo & Pok, 2003; Venkatesh & Davis, 2000; Venkatesh et al., 2003). We thus propose that individuals who feel social pressure to obtain apps will be less likely to engage in systematic processing. Individuals who desire to comply with or impress important others by obtaining the recommended apps will be less likely to search for information that would lead them to question the advice. Similar to the logic behind internal pressure to possess apps whereby individuals primarily rely on heuristic cues that favor the biased decision, we posit that individuals who feel social pressure to possess apps will be more likely to heuristically process. Therefore, we propose the following hypotheses. Our model is shown in Figure 2.

> Hypothesis 3c (H3c): App subjective norm will be negatively associated with systematic processing.
>
> Hypothesis 3d (H3d): App subjective norm will be positively associated with heuristic processing.

Methods and Analysis

Scale Development and Pilot Testing

In developing our scales, we used existing items where possible. However, it was necessary to contextualize most of the scales to adapt for the Android access notification context. In the case of heuristic processing, it was necessary to develop a new scale for our context. Table 1 provides references for each scale that was adapted from existing literature; all of the scale items are provided in the online appendix. In cases for which new items were developed or existing items adapted, care was taken to follow accepted procedural methods (Churchhill Jr., 1979; MacKenzie et al., 2011).

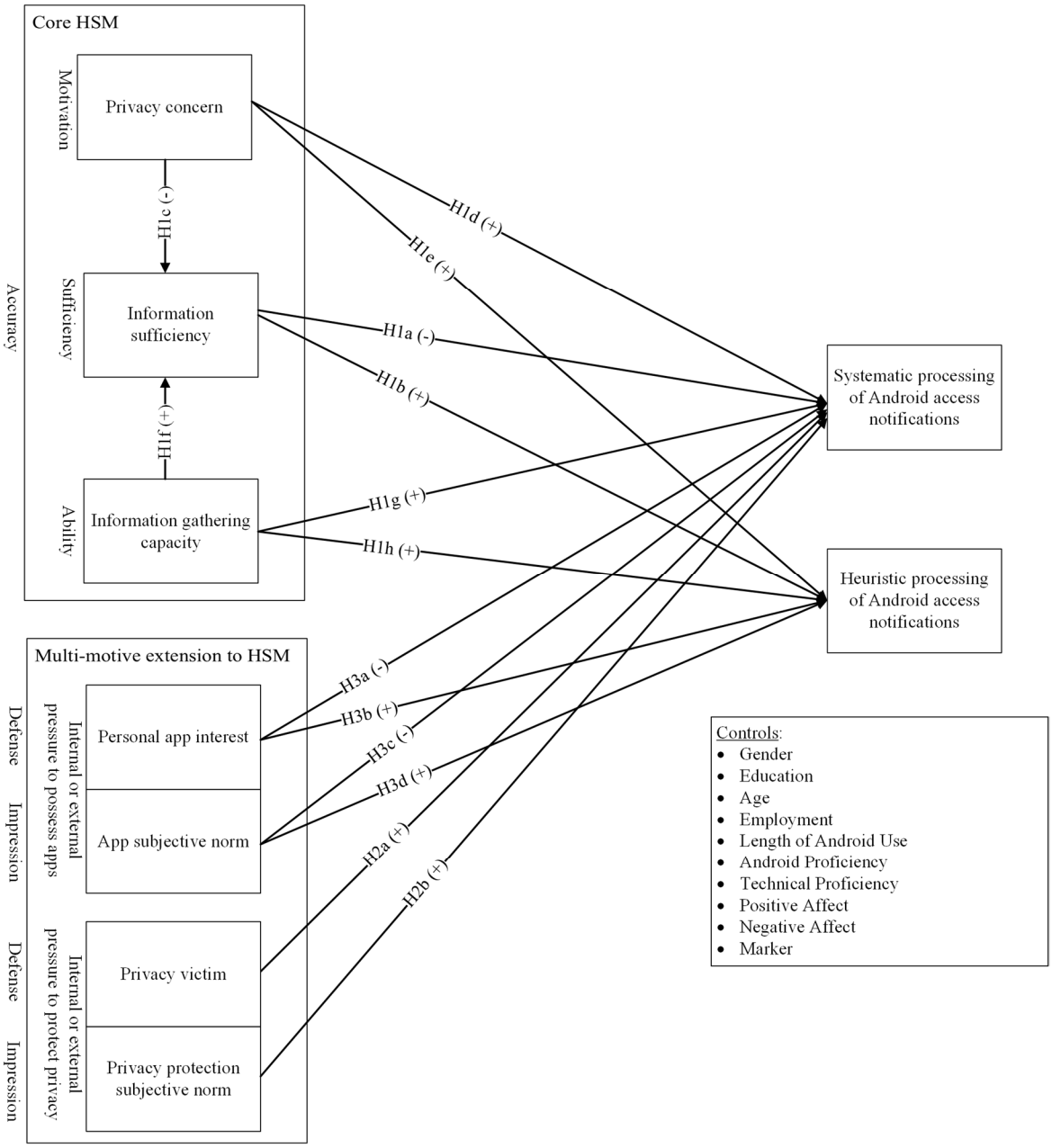

Figure 2. Multiple-Motive Heuristic-Systematic Model for Android Access Notifications

It has been suggested that the use of expert panels to obtain multiple perspectives on the formulation of the items may help reduce common method bias (Podsakoff et al., 2003; Spector, 2006). Our instrumentation was presented to an expert panel of smartphone users. Approximately 20 graduate students were asked to review the survey for both comprehensibility and grammar. Their advice was compiled and evaluated by the researchers, resulting in several minor wording changes to the instrument. Next, a pilot test of the survey was conducted using responses collected from Amazon's Mechanical Turk (mTurk)[1] crowdsourcing platform. Data from mTurk provides variance in demographic characteristics (e.g., age, education level) that may not be obtainable using other common populations (e.g., students) (Buhrmester et al., 2011). Using mTurk is a reliable option to collect data for behavioral research (Mason & Suri, 2012), and its use has been recommended to advance data collection methods (Lowry et al., 2016a). For the first pilot, 150 usable responses were collected. The statistical analysis of the pilot data indicated minor issues with a few items. After minor adjustments, another 150 usable responses were collected from mTurk, and the second statistical analysis revealed an acceptable factor structure.

For the pilot tests and the final data collection, Qualtrics[2] was used to administer the survey. The

survey was designed not to collect identifying information so that the respondents could be assured of anonymity. This is a common practice in survey administration because anonymity decreases the tendency of the respondents to answer in a way they think might be preferred by the researchers and thus may diminish common method bias (Podsakoff et al., 2003). A unique code was generated by Qualtrics and provided to each of the mTurk respondents at the end of the survey in order for the respondents to obtain a small monetary payment ($0.40 USD) for participating. Following recommendations by Steelman et al. (2014), we set a criterion in mTurk to restrict the sample to respondents geographically located in the United States (U.S.).

Two filter questions were posed at the beginning of the survey to determine whether the respondents were frequent Android smartphone users and at least 18 years old as required by the Institutional Review Board (IRB). The survey items were randomized to decrease common method bias (Podsakoff et al., 2003). In addition, "attention trap" items were used to determine whether the respondents were cognitively engaged in answering the questions (Oppenheimer et al., 2009). The "attention trap" items are provided in the online appendix and specified that, for example, the respondent select a particular response scale choice.

Final Data Collection and Participant Profile

The final data collection yielded 958 responses, of which 751 were usable. Responses were discarded due to the following reasons: 50 respondents did not finish the survey, 18 respondents were not frequent Android smartphone users, 2 respondents were not at least 18 years old (i.e., did not pass the filter questions), and 137 did not pass one of the "attention trap" items. Therefore, our final sample size is n = 751. Demographic information for the sample is provided in Table 2.

Table 1. Survey Items and Item Statistics

Construct	Source
Systematic processing	adapted from Davis and Tuttle (2013)
Heuristic processing	developed for the current study
Information sufficiency	adapted from Trumbo (2002)
Information gathering capacity	adapted from Zhang et al. (2013)
Personal app interest	adapted from Dinev and Hart (2006)
Privacy victim	adapted from Malhotra et al. (2004)
Android privacy concerns	adapted from Dinev and Hart (2006)
Privacy protection subjective norm	adapted from Davis and Tuttle (2013), Venkatesh and Davis (2000), Venkatesh et al. (2003)
App subjective norm	adapted from Davis and Tuttle (2013), Venkatesh and Davis (2000), Venkatesh et al. (2003)
Positive affect	adapted from Terpstra et al. (2014); Yang and Kahlor (2012)
Negative affect	adapted from Terpstra et al. (2014); Yang and Kahlor (2012)

Table 2. Demographic Information for Sample

Gender		Number		Employment		Education	
Male	275	18-20	26	Employed full time	464	Grade school (k-8 grade)	1
Female	476	21-25	114	Employed part time	168	High school or equivalent (e.g. GED)	73
		26-30	181	Not employed	119	Some college credit, no degree	196
		31-35	152			Trade/technical/vocational training	33
		36-40	98			Associate degree	95
		41-45	58			Bachelor's degree	252
		46-50	45			Master's degree	82
		51-Older	77			Professional degree	13
						Doctorate degree	6
Technology proficiency		**Android proficiency**		**Length of Android use**			
Novice	19	Novice	21	Less than 6 months	27		
Intermediate	326	Intermediate	292	6 months to 1 year	50		
Advanced	332	Advanced	333	1 to 2 years	95		
Expert	74	Expert	105	2 to 4 years	266		
				5 or more years	313		

Structural Model

We tested the path model using SmartPLS Version 3.2.1 (Ringle et al., 2014). We used this approach because multiple relationships between multiple independent and dependent variables can be tested concurrently using partial least squares regression (PLS) (Anderson & Gerbing, 1988; Gefen et al., 2000). It is appropriate to use PLS for theory development or exploratory causal modeling (Chin et al., 2003; Fornell & Larcker, 1981; Hair et al., 2017; Lowry & Gaskin, 2014; Peng & Lai, 2012). In the IS literature, PLS has often been employed to study behavioral phenomena (e.g., Leimeister et al., 2008; Lowry et al., 2016b; Wasko & Faraj, 2005). SmartPLS outputs an R2 value for the endogenous variable in the model (see Figure 3). The R2 values for information sufficiency (0.331) and systematic processing (0.360) are respectable, whereas the R2 value for heuristic processing (0.146) is lower than might be desired (Hair et al., 2017). PLS also provides path coefficients, t-values, and p-values for each relationship in the model. These results are given in Figure 3 and Table 3.

Table 3. Summarized Results

Hypothesis	Support?	Path Coefficient	t-value	p-value
H1a: Information sufficiency → systematic processing	Yes	-0.109	2.545	0.011
H1b: Information sufficiency → heuristic processing	No	0.024	0.493	0.622
H1c: Privacy concern → information sufficiency	Yes	-0.265	8.305	<0.001
H1d: Privacy concern → systematic processing	No	0.056	1.428	0.154
H1e: Privacy concern → heuristic processing	Yes	0.114	2.503	0.012
H1f: Information gathering capacity → information sufficiency	Yes	0.497	16.210	<0.001
H1g: information gathering capacity → systematic processing	Yes	0.288	7.323	<0.001
H1h: Information gathering capacity → heuristic processing	Yes	0.100	2.138	0.033
H3a: Personal app interest → systematic processing	Yes	-0.223	6.383	<0.001
H3b: Personal app interest → heuristic processing	Yes	0.225	4.761	<0.001
H3c: App subjective norm → systematic processing	No	0.052	1.303	0.193
H3d: App subjective norm → heuristic processing	Yes	0.137	3.263	0.001
H2a: Privacy victim → systematic processing	Yes	0.089	2.560	0.011
H2b: Privacy protection subjective norm → systematic processing	Yes	0.164	3.992	<0.001
Controls				
Gender → systematic processing		0.078	2.403	0.016
Gender → heuristic processing		0.078	2.166	0.031
Education → systematic processing		-0.044	1.369	0.171
Education → heuristic processing		-0.047	1.250	0.212
Age → systematic processing		0.055	1.689	0.092
Age → heuristic processing		-0.109	2.801	0.005
Employment → systematic processing		-0.093	2.922	0.004
Employment → heuristic processing		-0.034	0.848	0.396
Length of Android use → systematic processing		-0.069	2.197	0.028
Length of Android use → heuristic processing		-0.010	0.265	0.791
Android proficiency → systematic processing		0.039	0.829	0.407
Android proficiency → heuristic processing		-0.005	0.098	0.922
Technical proficiency → systematic processing		0.027	0.581	0.561
Technical proficiency → heuristic processing		0.031	0.618	0.537
Positive affect → systematic processing		0.244	5.562	<0.001
Positive affect → heuristic processing		0.091	1.977	0.048
Negative affect → systematic processing		0.027	0.550	0.582
Negative affect → heuristic processing		0.000	0.004	0.997
Marker → systematic processing		-0.009	0.276	0.783
Marker → heuristic processing		0.010	0.223	0.824

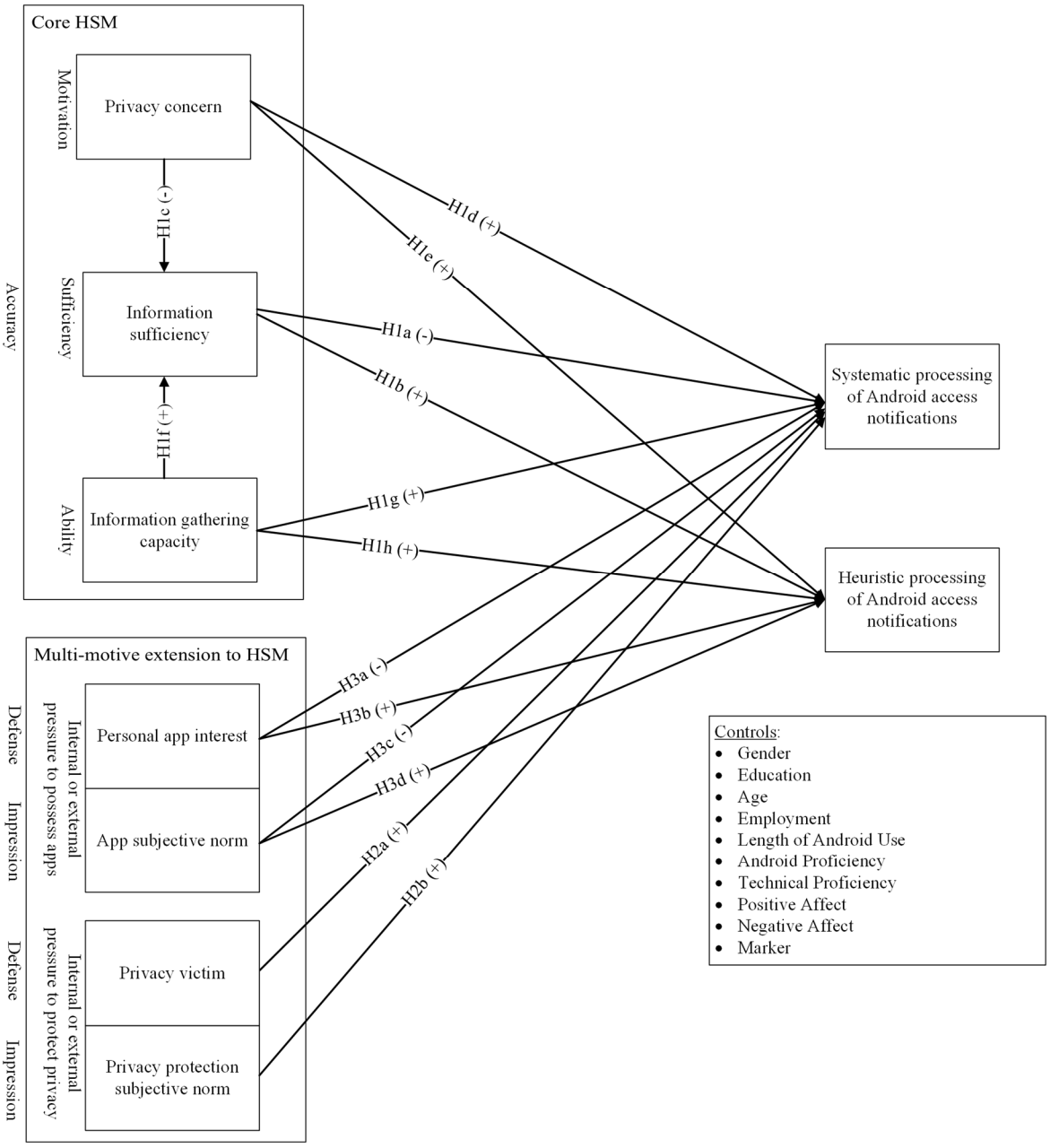

Figure 3. Multiple-Motive Heuristic-Systematic Model of Android Access Notifications

Discussion

Our findings illustrate that systematic processing is influenced by accuracy, defense, and impression motives. Testing of the core HSM confirmed the majority of the proposed hypotheses. As expected, individuals who feel that they have sufficient information to evaluate Android access notifications are less likely to conduct systematic processing (i.e., the effortful search for and incorporation of information into the evaluation process). However, no significant relationship was uncovered between information sufficiency and heuristic processing. As was the case in prior studies (e.g., Trumbo, 1999; Trumbo, 2002), individuals who strongly felt the issue was important were less likely to feel they had sufficient information. Specifically, individuals who reported high privacy concern were less likely to feel they had sufficient information regarding Android access notifications. Although issue importance (i.e., privacy concern) predicted higher levels of heuristic processing as expected, no significant relationship was uncovered between privacy concern and systematic processing. Individuals who reported high levels of information gathering capacity were more likely to feel they had sufficient information about the access notifications and were also more likely to conduct both heuristic and systematic information processing. Therefore, we find

support for the premise that individuals are more likely to engage in systematic processing if they feel they lack sufficient information to make a decision and think they are able to obtain additional information to assist a more accurate decision. We also find that individuals will rely on heuristic cues when they feel an issue is important and when they feel they have the ability to gather data to better inform a decision. These results largely confirm the findings of other studies that have examined the core HSM relationships.

We extended the core HSM model to include defense and impression motives for two types of pressures that might bias individuals' information processing: 1) protecting their privacy and 2) possessing the apps. We proposed that prior privacy victimization would result in a desire to protect one's privacy and thus would increase systematic processing. That is, prior privacy victims would be intent on defending their privacy and thus would be more likely to conduct an effortful search and thoroughly consume information that would help them understand the Android access notifications and the consequences of accepting them. We also posited that perceived pressure from important others to protect the data on their smartphones would lead individuals to engage in systematic processing of Android access notifications. In other words, if important others encouraged data protection, individuals would be more likely to make an effort to understand the access requests. Both hypotheses are supported; individuals who were prior privacy victims and those who perceived social pressure from important others to protect their privacy were both more likely to engage in systematic processing.

We posited that the defense and impression motives for possessing apps would increase heuristic but decrease systematic processing. Specifically, we proposed that individuals who are willing to let apps access their information to be able to fulfill their desire to use them would be less likely to engage in systematic processing. The logic behind this is that individuals would not spend extra time and effort to possibly uncover information that could cause them to doubt their preferred actions (i.e., to obtain the apps). Moreover, in agreeing to the privacy calculus trade-off, such users have determined that they value the apps over their privacy. We further proposed that individuals who desire to possess apps would rely on heuristic processing. We found support for our hypotheses. Specifically, individuals who reported high levels of personal app interest were more likely to rely on heuristic processing. A negative, significant relationship between personal app interest and systematic processing was revealed. We also posited that individuals who perceived social pressure from important others to possess apps would be more likely to rely on heuristic cues. We found support for the relationship between app subjective norm and heuristic processing; that is, individuals who perceived social pressure to possess apps were more likely to heuristically process. We also proposed that external pressure to possess apps would discourage systematic processing. The relationship between app subjective norm and systematic processing was not significant.

Some of our controls were significantly associated with heuristic or systematic processing of Android access notifications. Females are slightly more likely to report engaging in both heuristic and systematic processing than males. Older individuals are more likely to engage in systematic processing, but less likely to report utilizing heuristic cues. Individuals who are employed are more likely to report engaging in systematic processing. The longer individuals have used an Android phone, the less likely they are to engage in systematic processing. Finally, the more positive affect individuals feel when confronted with Android access notifications, the more likely they are to engage in heuristic and systematic processing.

Contributions to Research and Theory

Our multiple-motive HSM provides insight into factors influencing the heuristic and systematic processing of Android access notifications. Our results illustrate the promise of integrating the theory of heuristic and systematic information processing into IS security and privacy research. While heuristic processing is better than giving no thought to a decision, security and privacy researchers often presume that more thoughtful consideration of security and privacy decisions is occurring. Popular privacy macromodels (e.g., Li, 2011; Smith et al., 2011) assume that "individuals reflect thoughtfully and deliberately on their behaviors involving privacy options; however, none of these macromodels consider the nontrivial impact of low-effort thinking and extraneous influence of default heuristic processes and biases when a decision is made" (Dinev et al., 2015, p. 642). Our study advances this call to action by considering both more effortful information processing and heuristic cues. By examining antecedents to the information processing mode employed, we pave the way for the theory of heuristic and systematic information processing to be further integrated into IS security and privacy research.

Paying attention to heuristic cues such as star ratings or company reputation is good practice, but deliberately seeking out information to better understand Android access requests and their consequences is a stronger security behavior that security and privacy researchers and practitioners hope to encourage. Dinev et al. (2015, p. 640) state

that "sometimes behaviors are emotion-laden, spontaneous, or performed without complete information." Furthermore, they state that "prior work on information privacy has rarely accounted for these types of behaviors, and the process involved in such biases, incomplete decision making and information processing have not been considered" (Dinev et al., 2015, p. 640). We contribute to this conversation by illustrating factors that induce individuals to engage in systematic processing, as well as some conditions under which these factors emphasize heuristic processing of Android access notifications. Moreover, by examining defense and impression motives, we take a first step toward examining how biases affect the effort individuals exert to determine the extent of the security risks they face.

Research suggests that there are two main methods of coping when faced with online privacy threats (Youn, 2009). Individuals may either employ approach (or confrontative) strategies in which they actively attempt to accommodate or master the situation, or they may employ avoidance strategies in which they ignore the issue or avoid the situation (Youn, 2009). Youn (2009, p. 399) suggests that approach coping strategies include providing fabricated information or seeking information or support, whereas avoidance strategies include not using a website to avoid providing personal information. Systematic processing in our context equates to users employing an approach coping strategy (i.e., seeking information), which would be preferred behavior from a security and privacy standpoint. However, few studies have examined knowledge seeking, information sharing, or literacy in the privacy context (Baruh et al., 2017). Our study provides insight into what may encourage or discourage systematic processing and thus contributes to filling this gap.

There have been few attempts and little consistency in testing structural models for the theory of heuristic and systematic processing (e.g., Davis & Tuttle, 2013; Ferran & Watts, 2008; Kellens et al., 2012; Luo et al., 2013; Trumbo, 2002; Zhang et al., 2013), despite its usefulness for many types of technology studies. The theory may be especially useful in the security and privacy context because notifications (i.e., informational messages) from applications have become increasingly frequent. Interest in dual-mode processing models in the IS literature can be inferred through the increasing use of the ELM (e.g., Angst & Agarwal, 2009; Gu et al., 2017; Kim & Benbasat, 2009; Lowry et al., 2012; Puhakainen & Siponen, 2010). The ELM was proposed around the same time as the theory of heuristic and systematic information processing and includes some similar concepts (Chaiken & Ledgerwood, 2012; Wood, 2000). Also, in a recent research commentary, Dinev et al. (2015) suggested the relevance of incorporating ELM into privacy research, and a recent study explored ELM in the mobile application context (Gu et al., 2017). Our study complements the few studies in IS that have applied the theory of heuristic and systematic information processing to videoconferencing, exceptions, and phishing (Davis & Tuttle, 2013; Ferran & Watts, 2008; Luo et al., 2013).

The theory of heuristic and systematic information processing differs from ELM in two important ways. First, although it also proposes two different types of information processing, unlike ELM, it posits that they can co-occur and interact. Second, it "jointly considers the influence of multiple modes of processing on the one hand and multiple motives on the other" (Chaiken & Ledgerwood, 2012, p. 257). These multiple motives provide a richness to the theory that is particularly useful in exploring complex decision-making in IS. Chaiken and Ledgerwood (2012, p. 257) add that "the tripartite analysis of motives in the heuristic-systematic model has its historical roots in the literature on attitude function, although it should be noted that similar classes of motives that center on understanding, protecting the self, and affiliating with others are echoed across multiple domains." By contextualizing the theory to examine processing of Android access notifications, our study takes a first step at a privacy application of a multiple-motive HSM. We do not suggest that our operational model or our constructs are definitive versions of the theory. We intended to use the theory to test antecedents to the information processing of a very particular type of message (Android access notifications), and our model provides insight into this phenomenon. Our results are encouraging and support the use of this theory, especially in privacy and security, where it is important to have individuals put effort into making informed, security-conscious decisions. The theory of heuristic and systematic information processing is very rich and has not been widely applied in IS literature. Future work may benefit by further integrating a rich body of work in social psychology (e.g., Chaiken & Ledgerwood, 2012; Wood, 2000) on the theory of heuristic and systematic information processing into IS studies of privacy and security.

Implications for Society and Practice

Our finding that the privacy protection subjective norm is a predictor of systematic processing is encouraging and concurs with previous findings in the HSM literature that "information subjective norms may be a powerful predictor of seeking and processing when individuals face impersonal risks" (Kahlor et al., 2006, p. 163). This result suggests that perceived social pressure to protect the privacy of information on one's Android smartphone could be leveraged to encourage

security and privacy knowledge-seeking behaviors. One ramification of this is that if key individuals in a social network are educated regarding the importance of smartphone security and privacy concerns, the knowledge may permeate in a positive way through the social network. For example, if management is convinced of the importance of particular smartphone security and privacy practices, employees that consider management to be "important others" may also adopt such practices. In fact, similar conclusions have been reached in the IS privacy literature, where Li (2011, p. 472) stated that "firms may use the influence of peers to address privacy concerns, as social norms may change a person's privacy belief." However, our examination of impression motives also considered social pressure to possess apps, which does not directly impact systematic processing, but is positively associated with heuristic processing. Therefore, the target of the social pressure is important. It is extremely important that the perceived social pressure is for the desired behavior, which in our case is protecting data stored on smartphones, rather than social pressure that may not encourage good security practice (e.g., social pressure to possess apps).

Our findings also point to the importance of training and experience. The positive relationship between information gathering capacity and systematic processing points to the importance of users feeling confident in their ability to obtain information to assist security and privacy decisions. Although training programs may not be able to teach individuals about every security risk, training could include teaching users how to investigate privacy and security issues that they do not understand and the importance of doing so to fully understand the risks of the privacy and security decisions they are making. It may not be surprising, but it is concerning, that users' desires to possess apps reduced the likelihood of systematic processing. Users may not be able to correctly estimate the risks associated with accepting access requests. The misestimation of the costs associated with accepting access requests may result in users trading their privacy to use the desired apps without a robust understanding of the consequences. Training regimes may want to take this into consideration by specifically explaining the consequences of accepting access notifications. Platform providers (e.g., Google Play) may want to consider that stricter vetting of apps may be necessary. Moreover, our findings revealed that simply being concerned about one's privacy did not directly encourage more effortful attempts to understand access requests, but prior experience of being a privacy victim did. Security and privacy researchers and practitioners should explore ways of encouraging good privacy and security behaviors that do not require the actual experience of a privacy breach. Training regimes that simulate security or privacy attacks and specifically explain the consequences of such breaches could be used to make outcomes more visceral for users.

Finally, our results indicate that individuals rely heavily on heuristic cues to process Android access notifications. Users are exposed to a variety of heuristic cues, such as the star rating, popularity of the application (e.g., the number of downloads), aesthetics of the download page, and name of the company providing the app. However, most of these cues indicate reliability or popularity of the app rather than providing information directly relevant to the security or privacy protections it offers. Practitioners could consider ways to design heuristic cues that better indicate security and privacy risks. Websites indicate secure browsing (e.g., through a lock and a colored search bar) or trust assurances (e.g., security seals or badges awarded by companies that evaluate security). App makers and platform providers could consider placing heuristic cues on access notifications that help the users evaluate different apps with regard to security or privacy. Another possibility might be to add a heuristic cue to particular access requests that indicates where in the range of typical access requests the request the user is considering falls. For example, data could be collected on the access requests made by particular categories of apps and a heuristic cue could be added to an access notification that indicates to the potential user whether or not the app is asking for more, less, or typical amounts of access to the smartphone. Determining how to design heuristic cues that encourage the best security or privacy practices is an interesting area for future study. If researchers can tease out what kinds of heuristic cues might best encourage good security or privacy practices, the download and notification screens could be redesigned by the app marketplaces to present individuals with the most useful set of heuristic cues to encourage security-conscious decisions.

Limitations and Directions for Future Research

The importance of heuristic cues in the Android access notification context provides many avenues for interesting future research. As previously mentioned, researchers may want to explore in detail which heuristic cues are the most useful to users or which are most likely to encourage good security or privacy decisions. Researchers may also want to examine the attenuation, additivity, and bias hypotheses in the theory of heuristic and systematic information processing in the Android access notification context. These hypotheses explore in detail how heuristic and systematic processing may co-occur and interact (Chaiken et al., 1989), and they may provide interesting avenues of exploration for researchers

considering how to present heuristic information to individuals downloading smartphone apps that may encourage desired security-conscious behaviors.

We also discovered a positive relationship between positive affect and systematic processing. Some prior research has suggested that negative affect should have a positive relationship with information processing (Griffin et al., 1999a). However, Jepson and Chaiken (1990) found fear to decrease systematic processing. Hence, there are mixed findings for the affect variables in prior studies. We included the affect variables as controls in our model because our primary interest was in the multiple motives. In our model, the relationship between negative affect and systematic processing was not significant, but the relationship between positive affect and systematic processing was positive. One explanation for this finding may be that the appearance of the Android access notification gives the users a sense of transparency because the app is stating what it wants access to on the smartphone. In addition, the Android access notification provides a list of access requests that could make it easier for individuals to look up more information. Thus, individuals may have positive feelings from the sense of transparency and direct presentation of access requests, which leads to more systematic processing. Moreover, in studying the influence of affect on online self-disclosure, Yu et al. (2015) found that positive affect was positively associated with motivators but not inhibitors. They suggested that positive affect indirectly influenced self-disclosure by adjusting the perceptions of benefits and costs. A similar effect may be at work in increasing the perceived benefits of systematic processing. Future research may want to explore emotional reactions to such notifications in more detail, especially since our findings are not strictly intuitive. Interesting insight may be obtained from a better understanding of users' emotional reactions to access notifications to determine if, for example, notifications are perceived as helpful, are resented, or are fear-enhancing.

We also focused on what drives heuristic and systematic processing of Android access notifications using a survey-based approach with self-reported measures. Future work could extend our study by conducting an experiment to tease out the effects of particular heuristic cues or to examine the impact of heuristic and/or systematic processing on the actual decision to install a specific Android application. We would also encourage researchers to look at outcomes associated with heuristic and systematic processing. Although some studies have focused on heuristic and systematic processing as the dependent variables as we did (e.g., Davis & Tuttle, 2013; Griffin et al., 1999b), others have examined how heuristic or systematic processing is associated with perceptions of risk, willingness to disclose information, or decision-making (e.g., Trumbo, 2002). Future research should examine other antecedents to the processing types, different security or privacy contexts, and outcomes associated with the type of information processing (i.e., heuristic versus systematic).

Conclusion

We developed and tested a multiple-motive HSM to examine individuals' heuristic and systematic processing of Android access notifications. The theory of heuristic and systematic information processing suggests that there are two types of information processing. Heuristic processing is the use of easily available cues to help inform decisions. In the Android context, heuristic cues are the information that can be easily seen during the downloading and installation processes of apps (e.g., the app's star-rating, the reputation of the company providing the app, and user reviews). With sufficient motivation, individuals may conduct more effortful systematic processing to assist their evaluation of the messages (i.e., access notifications). In the Android context, systematic processing includes actively searching for, collecting, and consuming information to assist in the evaluation of access notifications (e.g., locating and asking someone deemed knowledgeable about Android access notifications or consulting the user manual or Internet for more information about them).

Our model examined how the three motivations (accuracy, defense, and impression) described in the theory of heuristic and systematic information processing influence heuristic and systematic processing in the Android access notification context. We discovered that users who feel they have sufficient information about Android access notifications are less likely to engage in systematic processing. Users who feel able to obtain information about Android access notifications are more likely to report having sufficient information, but are also more likely to engage in both heuristic and systematic processing of Android access notifications. Individuals who report high issue importance (i.e., privacy concern) are less likely to report having sufficient information regarding access notifications and are more likely to rely on heuristic cues. These findings lend support to users' accuracy motivations driving their information processing in the Android access notification context and largely confirm the core HSM.

We also uncovered how defense and impression motivations influence how users process information. If users value apps more than they value their privacy, they are less likely to engage in systematic processing and more likely to rely on heuristic cues. We found that if users felt social pressure from important others to possess apps, they were also more likely to rely on

heuristic cues. Strategies to make heuristic cues stand out to users, creation of more informative heuristic cues, education to increase users' awareness of such cues, and approaches to educate users regarding how to find additional information about Android access notifications and better understand the consequences of accepting access requests may all be helpful in encouraging better privacy and security behaviors in smartphone users. Our findings also revealed that internal and external pressures to protect privacy resulted in more effortful search and consumption of context-relevant information. This means that training individuals on the importance of protecting the data stored on Android smartphones could be a useful means to encourage better security behaviors because such privacy protection norms could propagate through the population. Our study provides a privacy application of the theory of heuristic and systematic information processing and findings that can be used by researchers and practitioners to better understand how users process Android access notifications.

References

Anderson, J. C., & Gerbing, D. W. (1988). Structural equation modeling in practice: A review and recommended two-step approach. *Psychological Bulletin, 103*(3), 411-423.

Angst, C. M., & Agarwal, R. (2009). Adoption of electronic health records in the presence of privacy concerns: The elaboration likelihood model and individual persuasion. *MIS Quarterly, 33*(2), 339-370.

Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online privacy concerns and privacy management: A meta-analytical review. *Journal of Communication, 67*(1), 26-53.

Bhandari, S., Jaballah, W. B., Jain, V., Laxmi, V., Zemmari, A., Gaur, M. S., et al. (2017). Android inter-app communication threats and detection techniques. *Computers & Security, 70*(1), 392-421.

Bosu, A., Liu, F., Yao, D. D., & Wang, G. (2017). *Collusive data leak and more: Large-scale threat analysis of inter-app communications.* Paper presented at the Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security, Abu Dhabi, United Arab Emirates.

Buhrmester, M., Kwang, T., & Gosling, S. D. (2011). Amazon's Mechanical Turk a new source of inexpensive, yet high-quality, data? *Perspectives on Psychological Science, 6*(1), 3-5.

Chaiken, S. (1980). Heuristic versus systematic information processing and the use of source versus message cues in persuasion. *Journal of Personality and Social Psychology, 39*(5), 752-766.

Chaiken, S. (1987). The heuristic model of persuasion. In M. P. Zanna, J. Olson, M. & C. P. Herman (Eds.), *Social Influence: The Ontario Symposium* (Vol. 5, pp. 3-39). New York, NY: Psychology Press.

Chaiken, S., Giner-Sorolla, R., and Chen, S. (1996). Beyond accuracy: Defense and impression motive in heuristic and systematic information processing. In P. M. Gollwitzer & J. A. Bargh (Eds.), *The Psychology of Action: Linking Cognition and Motivation to Behavior*. New York, NY: The Guilford Press.

Chaiken, S., & Ledgerwood, A. (2012). A theory of heuristic and systematic information processing. In P. A. M. Van Lange, A. W. Kruglanski & E. T. Higgins (Eds.), *Handbook of Theories of Social Psychology* (Vol. 1, pp. 246-266). London, UK: SAGE Publications Ltd.

Chaiken, S., Liberman, A., & Eagly, A. H. (1989). Heuristic and systematic information processing within and beyond the persuasion context. In J. S. Uleman & J. A. Bargh (Eds.), *Unintended Thought*. New York, NY: Guilford Press.

Chen, S., & Chaiken, S. (1999). The heuristic-systematic model in its broader context. In S. Chaiken & Y. Trope (Eds.), *Dual-Process Theories in Social Psychology* (pp. 73-96). New York, NY: Guilford Press.

Chen, S., Duckworth, K., & Chaiken, S. (1999). Motivated heuristic and systematic processing. *Psychological Inquiry, 10*(1), 44-49.

Chen, S., Shechter, D., & Chaiken, S. (1996). Getting at the truth or getting along: Accuracy-versus impression-motivated heuristic and systematic processing. *Journal of Personality and Social Psychology, 71*(2), 262.

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*(2), 189-217.

Cho, H., Lee, J.-S., & Chung, S. (2010). Optimistic bias about online privacy risks: Testing the moderating effects of perceived controllability and prior experience. *Computers in Human Behavior, 26*(5), 987-995.

Chow, W. S., & Chan, L. S. (2008). Social network, social trust and shared goals in organizational knowledge sharing. *Information & Management, 45*(7), 458-465.

Churchhill Jr., G. A. (1979). A paradigm for developing better measures of marketing constructs. *Journal of Marketing Research, 16*(1), 64-73.

Dai, H., & Palvi, P. C. (2009). Mobile commerce adoption in China and the United States: A cross-cultural study. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems, 40*(4), 43-61.

Davis, J. M., & Tuttle, B. M. (2013). A heuristic–systematic model of end-user information processing when encountering IS exceptions. *Information & Management, 50*(2), 125-133.

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research, 17*(1), 61-80.

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

Doffman, Z. (2019). New Android warning: 500M+ users have installed apps hiding nasty malware—uninstall now. Retrieved September 23, 2019, from https://www.forbes.com/sites/zakdoffman/2019/09/20/new-android-warning-500m-users-have-installed-apps-hiding-nasty-malwareuninstall-now/#42de602112be

Dunwoody, S., & Griffin, R. J. (2015). Risk information seeking and processing model. In H. Cho, T. Reimer & K. McComas (Eds.), *The SAGE Handbook of Risk Communication* (pp. 102-116). Thousand Oaks, CA: Sage Publications.

Eagly, A. H., & Chaiken, S. (1993). *The psychology of attitudes*. Orlando, FL: Harcourt Brace Jovanovich College Publishers.

Ferran, C., & Watts, S. (2008). Videoconferencing in the field: A heuristic processing model. *Management Science, 54*(9), 1565-1578.

Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention, and behavior: An introduction to theory and research*. Reading, MA: Addison-Wesley.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18*(1), 39-50.

Forrest, C. (2014). Google Play v Apple App Store: The battle for the mobile app market. Retrieved April 13, 2015, from http://www.techrepublic.com/article/google-play-v-apple-app-store-the-battle-for-the-mobile-app-market/

Gefen, D., Straub, D., & Boudreau, M.-C. (2000). Structural equation modeling and regression: Guidelines for research practice. *Communications of the Association for Information Systems, 4*(1), 2-77.

Giner-Sorolila, R., & Chaiken, S. (1997). Selective use of heuristic and systematic processing under defense motivation. *Personality and Social Psychology Bulletin, 23*(1), 84-97.

Griffin, R. J., Dunwoody, S., & Neuwirth, K. (1999a). Proposed model of the relationship of risk information seeking and processing to the development of preventive behaviors. *Environmental Research, 80*(2), S230-S245.

Griffin, R. J., Dunwoody, S., Neuwirth, K., & Giese, J. (1999b). *The relationship of information sufficiency to seeking and processing risk information.* Paper presented at the International Communication Association, San Francisco, CA.

Griffin, R. J., Yang, Z., Boerner, F., Bourassa, S., Darrah, T., Knurek, S., et al. (2005). *Applying an information seeking and processing model to a study of communication about energy.* Paper presented at the Association for Education in Journalism and Mass Communication Annual Conference, San Antonio, Texas.

Griffin, R. J., Yang, Z., ter Huurne, E., Boerner, F., Ortiz, S., & Dunwoody, S. (2008). After the flood anger, attribution, and the seeking of information. *Science Communication, 29*(3), 285-315.

Grunig, J. E. (1983). Communication behaviors and attitudes of environmental publics: Two studies. *Journalism and Communication Monographs, 81*.

Gu, J., Xu, Y. C., Xu, H., Zhang, C., & Ling, H. (2017). Privacy concerns for mobile app download: An elaboration likelihood model perspective. *Decision Support Systems, 94*(1), 19-28.

Hair, J. F., Hult, G. T. M., Ringle, C., & Sarstedt, M. (2017). *A primer on partial least squares structural equation modeling (PLS-SEM)*. Thousand Oaks, CA: Sage.

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems, 18*(2), 106-125.

Honan, M. (2013). Break out a hammer: You'll never believe the data 'wiped' smartphones store. *Wired*. Retrieved June 26, 2018, from https://www.wired.com/2013/04/smartphone-data-trail/

International Data Corporation (2018). Smartphone OS. Retrieved June 26, 2018, from https://www.idc.com/promo/smartphone-market-share/os

Isaac, M. (2011). Survey finds smartphone apps store too much personal data. *Wired*. Retrieved November 1, 2019, from https://www.wired.com/2011/08/smartphone-local-data-storage/

James, T. L., Warkentin, M., & Collignon, S. E. (2015). A dual privacy decision model for online social networks. *Information & Management, 52*(8), 893-908.

Jepson, C., & Chaiken, S. (1990). Chronic issue-specific fear inhibits systematic processing of persuasive communications. *Journal of Social Behavior and Personality, 5*(2), 61-84.

Johnson, B. B. (2005). Testing and expanding a model of cognitive processing of risk information. *Risk Analysis, 25*(3), 631-650.

Kahlor, L. (2007). An augmented risk information seeking model: The case of global warming. *Media Psychology, 10*(3), 414-435.

Kahlor, L., Dunwoody, S., Griffin, R. J., & Neuwirth, K. (2006). Seeking and processing information about impersonal risk. *Science Communication, 28*(2), 163-194.

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. *International Journal of Human-Computer Studies, 71*(12), 1163-1173.

Kellens, W., Zaalberg, R., & De Maeyer, P. (2012). The informed society: An analysis of the public's information-seeking behavior regarding coastal flood risks. *Risk analysis, 32*(8), 1369-1381.

Kim, D., & Benbasat, I. (2009). Trust-assuring arguments in B2C e-commerce: Impact of content, source, and price on trust. *Journal of Management Information Systems, 26*(3), 175-206.

Kim, J., & Paek, H. J. (2009). Information processing of genetically modified food messages under different motives: An adaptation of the multiple-motive heuristic-systematic model. *Risk Analysis, 29*(12), 1793-1806.

Leimeister, J. M., Schweizer, K., Leimeister, S., & Krcmar, H. (2008). Do virtual communities matter for the social support of patients? Antecedents and effects of virtual relationships in online communities. *Information Technology & People, 21*(4), 350-374.

Li, Y. (2011). Empirical studies on online information privacy concerns: Literature review and an integrative framework. *Communications of the Association for Information Systems, 28*(28), 453-496.

Li, Y. (2012). Theories in online information privacy research: A critical review and an integrated framework. *Decision Support Systems, 54*(1), 471-481.

Lowry, P. B., D'Arcy, J., Hammer, B., & Moody, G. D. (2016a). "Cargo Cult" science in traditional organization and information systems survey research: A case for using nontraditional methods of data collection, including Mechanical Turk and online panels. *The Journal of Strategic Information Systems, 25*(3), 232-240.

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*(2), 123-146.

Lowry, P. B., Moody, G., Vance, A., Jensen, M., Jenkins, J., & 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*(4), 755-776.

Lowry, P. B., Zhang, J., Wang, C., & Siponen, M. (2016b). Why do adults engage in cyberbullying on social media? An integration of online disinhibition and deindividuation effects with the social structure and social learning (SSSL) model. *Information Systems Research, 27*(4), 962-986.

Lu, J., Yao, J. E., & Yu, C.-S. (2005). Personal innovativeness, social influences and adoption of wireless Internet services via mobile technology. *Journal of Strategic Information Systems, 14*(3), 245-268.

Luo, X. R., Zhang, W., Burd, S., & Seazzu, A. (2013). Investigating phishing victimization with the Heuristic–Systematic Model: A theoretical framework and an exploration. *Computers & Security, 38*, 28-38.

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 Quarterly, 35*(2), 293-334.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research, 15*(4), 336-355.

Mason, W., & Suri, S. (2012). Conducting behavioral research on Amazon's Mechanical Turk. *Behavior Research Methods, 44*(1), 1-23.

Mearian, L. (2017). Android vs iOS security: Which is better?. Retrieved June 25th, 2018, from https://www.computerworld.com/article/3213388/mobile-wireless/android-vs-ios-security-which-is-better.html

Oppenheimer, D. M., Meyvis, T., & Davidenko, N. (2009). Instructional manipulation checks: Detecting satisficing to increase statistical power. *Journal of Experimental Social Psychology, 45*(4), 867-872.

Pavlou, P. A. (2011). State of the information privacy literature: Where are we now and where should we go? *MIS Quarterly, 35*(4), 977-988.

Peng, D. X., & Lai, F. (2012). Using partial least squares in operations management research: A practical guideline and summary of past research. *Journal of Operations Management, 30*(6), 467-480.

Perez, S. (2017). U.S. consumers now spend 5 hours per day on mobile devices. Retrieved June 26, 2018, from https://techcrunch.com/2017/03/03/u-s-consumers-now-spend-5-hours-per-day-on-mobile-devices/

Pew Research Center (2018). Mobile fact sheet. Retrieved June 21, 2018, from http://www.pewinternet.org/fact-sheet/mobile/

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. *Journal of Applied Psychology, 88*(5), 879-903.

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly, 34*(4), 757-778.

Ringle, C. M., Wende, S., & Becker, J.-M. (2014). SmartPLS 2. Retrieved June 18, 2015, from http://www.smartpls.com

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly, 35*(4), 989-1016.

Son, J.-Y., & Kim, S. S. (2008). Internet users' information privacy-protective responses: A taxonomy and a nomological model. *MIS Quarterly, 32*(3), 503-529.

Sophos (2017). 2018 malware forecast: The onward march of Android malware. Retrieved June 26, 2018, from https://nakedsecurity.sophos.com/2017/11/07/2018-malware-forecast-the-onward-march-of-android-malware/

Spector, P. E. (2006). Method variance in organizational research: Truth or urban legend? *Organizational Research Methods, 9*(2), 221-232.

Statista: The Statistics Portal (2018a). Mobile Internet user penetration rate in selected countries as of 3rd quarter 2017. Retrieved June 26, 2018, from https://www.statista.com/statistics/239114/global-mobile-internet-penetration/

Statista: The Statistics Portal (2018b). Mobile phone internet user penetration worldwide from 2014 to 2019. Retrieved June 21, 2018, from https://www.statista.com/statistics/284202/mobile-phone-internet-user-penetration-worldwide/

Statista: The Statistics Portal (2018c). Number of apps available in leading app stores as of 1st quarter 2018. Retrieved June 25, 2018, 2018, from https://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/

Statista: The Statistics Portal (2018d). Number of mobile app downloads worldwide in 2017, 2018 and 2022 (in billions). Retrieved June 26, 2018, from https://www.statista.com/statistics/271644/worldwide-free-and-paid-mobile-app-store-downloads/

Steelman, Z. R., Hammer, B. I., & Limayen, M. (2014). Data collection in the digital age: Innovative alternatives to student samples. *MIS Quarterly, 38*(2), 355-378.

Teo, T. S., & Pok, S. H. (2003). Adoption of WAP-enabled mobile phones among Internet users. *Omega, 31*(6), 483-498.

Terpstra, T., Zaalberg, R., Boer, J., & Botzen, W. (2014). You have been framed! How antecedents of information need mediate the effects of risk communication messages. *Risk Analysis, 34*(8), 1506-1520.

Trumbo, C. W. (1999). Heuristic-systematic information processing and risk judgment. *Risk Analysis, 19*(3), 391-400.

Trumbo, C. W. (2002). Information processing and risk perception: An adaptation of the heuristic-systematic model. *Journal of Communication, 52*(2), 367-382.

U.S. Federal Trade Commission (2017). Understanding mobile apps. Retrieved June 21, 2018, from https://www.consumer.ftc.gov/articles/0018-understanding-mobile-apps

Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management Science, 46*(2), 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*(3), 425-478.

Venkatesh, V., Thong, J. Y., & Xu, X. (2016). Unified theory of acceptance and use of technology: A synthesis and the road ahead. *Journal of the Association for Information Systems, 17*(5), 328-376.

Wasko, M. M., & Faraj, S. (2005). Why should I share? Examining social capital and knowledge contribution in electronic networks of practice. *MIS Quarterly, 29*(1), 35-57.

Wood, W. (2000). Attitude change: Persuasion and social influence. *Annual Review of Psychology, 51*(1), 539-570.

Yang, Z. J. & Kahlor, L. (2012). What, me worry? The role of affect in information seeking and avoidance. *Science Communication, 35*(2), 189-212.

Youn, S. (2009). Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. *Journal of Consumer Affairs, 43*(3), 389-418.

Yu, J., Hu, P. J.-H., & Cheng, T.-H. (2015). Role of affect in self-disclosure on social network websites: A test of two competing models. *Journal of Management Information Systems, 32*(2), 239-277.

Zhang, L., Pavur, R., York, P., & Amos, C. (2013). Testing a model of users' web risk information seeking intention. *Informing Science: The International Journal of an Emerging Transdiscipline, 16*(1), 1-18.

About the Authors

Tabitha L. James is an Associate Professor in the Pamplin College of Business at Virginia Tech. She holds a Ph.D. from the University of Mississippi in Management Information Systems. Her current research interests include behavioral information privacy and security, psychological impacts of technology use, and analytics focused on the development of metaheuristics for combinatorial optimization problems. Her research has been accepted for publication in outlets such as *MIS Quarterly*, *Information Systems Research*, *Journal of Management Information Systems, European Journal of Information Systems, European Journal of Operational Research, Information Systems Journal, IEEE Intelligent Systems, Information & Management*, *Computers & Security, Expert Systems with Applications*, and *Decision Support Systems*. She has served as an AE for ICIS and ECIS, as well as a mini-track chair and junior faculty consortium co-chair for AMCIS. She also serves as a senior editor for *Engineering Applications of Artificial Intelligence* and is on the editorial review board of the *Journal of the Association for Information Systems*.

Jennifer L. Ziegelmayer is an Assistant Professor of Management Information Systems at IÉSEG School of Management. She earned her Ph.D. in Business Administration with a concentration in Management Information Systems from the University of Mississippi. Her research interests focus on privacy and behavioral security, disclosure in social media, and cross-cultural issues in IS and accounting. Her research has appeared in journals including *European Journal of Information Systems*, *Information Technology and Management*, *Journal of Computer Information Systems*, *Information Systems Frontiers*, and *Accounting & Finance*. She is a member of the Association of Information Systems (AIS), Association for Computing Machinery (ACM), Decision Sciences Institute (DSI), and Association of Information Technology Professionals (AITP).

Arianna Schuler Scott is a DPhil Candidate at the Centre for Doctoral Training in Cyber Security at the University of Oxford. She is working towards her Ph.D. with the Cyber Analytics Group based in Computer Science and the Centre for Health, Law and Emerging Technologies (HeLEX), where her work focuses on dynamic consent as a mechanism for data minimization. Her research interests include data protection, information security, and the regulation of data and privacy.

Grace Fox is an Assistant Professor of Digital Business at Dublin City University Business School. She holds a Ph.D. in Management Information Systems from Dublin City University. Her research interests include information privacy and behavior, technology adoption and usage behaviors, older adults and technology use, and data literacy. Her research has been published or is forthcoming in *Information Systems Journal, Communications of the Association for Information Systems (CAIS), Journal of Cloud Computing* and *Health Informatics Journal.* She has served as an AE for ECIS and as a mini-track chair for AMCIS.

Appendix A

Table A.1. Measurement Item Details and Sources

Construct (Source)	Construct indicator	Item	Mean	Std. Dev.
Systematic processing; adapted from Davis and Tuttle (2013)	**Prompt:** Please think of the Android access notification screen, such as the one above (Figure 1 in the main manuscript), and answer to what extent you agree with the following statements. When applications on my Android phone present notifications asking to access information on my device, I: 7-point Likert-type scales from 1 = "Strongly disagree" to 7 = "Strongly agree"			
	SProc1	search online documentation for information about what the application is trying to access.	3.855	1.879
	SProc2	read the user manual for information about what the application is trying to access.	3.226	1.846
	SProc3	ask someone I consider knowledgeable to help me understand what information the application is trying to access.	3.786	1.903
	SProc4	click each notification to read more details about the information the application is asking to access.	4.411	1.821
	SProc5	go to the website of the application to research what information the application is asking to access.	3.688	1.874
	SProc6	read comments written by other users to find out about the information the application is trying to access.	4.615	1.807
Heuristic processing; developed for the current study	**Prompt:** Please think of the Android access notification screen, such as the one above (Figure 1 in the main manuscript), and answer to what extent you agree with the following statements. When applications on my Android phone present notifications asking to access information on my device, I consider: 7-point Likert-type scales from 1 = "Strongly disagree" to 7 = "Strongly agree"			
	HProc1	the star rating information for the application.	5.439	1.453
	HProc2	the consumer reviews for the application.	5.510	1.361
	HProc3	the reputation of the company that is providing the application.	5.762	1.195
	HProc4	what other people have said about the application.	5.406	1.357
	HProc5	the popularity of the application.	5.117	1.602
	HProc6	the appearance of the application design.	4.320	1.767
	HProc7	what I have heard in the media about allowing an application to access my information.	4.921	1.556
Information sufficiency; adapted from Trumbo (2002)	**Prompt:** Keeping in mind the Android access notifications you see when downloading or using an app, such as (Figure 1 in the main manuscript): Rate the degree to which you agree or disagree with each statement: 7-point Likert-type scales from 1 = "Strongly disagree" to 7 = "Strongly agree"			
	Suff1	The information I have at this time meets all of my needs for knowing what the Android access notifications are telling me.	4.345	1.705
	Suff2	I have all the information I currently need regarding the Android access notifications.	4.269	1.681
	Suff3	I know all I need to know about the Android access notifications.	4.153	1.722
	Suff4	I do not need more information than I currently have about the Android access notifications.	4.088	1.704
	Suff5	I have sufficient information about what the Android access notifications mean.	4.449	1.703
	Suff6	I do not require more information about the Android access notifications.	4.117	1.716
	Suff7	I currently have enough information about the Android access notifications.	4.338	1.698
Information gathering capacity;	**Prompt:** Please think of the Android access notification screen, such as the one above (Figure 1 in the main manuscript), and answer to what extent you agree with the following statements:			

adapted from Zhang et al. (2013)	7-point Likert-type scales from 1 = “Strongly disagree” to 7 = “Strongly agree”			
	IGC1	If I wanted to, I could easily get all the information I need about Android access notifications.	4.639	1.592
	IGC2	I would know where to go for more information about Android access notifications.	4.382	1.726
	IGC3	I would know what questions to ask of the experts about Android access notifications.	4.252	1.643
Android privacy concerns; adapted from Dinev and Hart (2006)	**Prompt:** Indicate the extent to which you are concerned about the following: 7-point Likert-type scales from 1 = “Very unconcerned” to 7 = “Very concerned”			
	APC1	I am concerned that my personal information on my Android phone could be misused.	4.748	1.582
	APC2	I am concerned that someone may be able to access my personal information from my Android phone.	4.706	1.581
	APC3	I am concerned about what others may do with access to the personal information on my Android phone.	4.826	1.607
	APC4	I am concerned that personal information obtained from my Android phone may be used in ways I did not foresee.	4.795	1.569
Privacy victim; adapted from Malhotra et al. (2004)	**Prompt:** Please select the choice that best applies to you: 7-point Likert-type scales from 1 = “Very infrequently” to 7 = “Very frequently”			
	PRIV1	How frequently have you personally been the victim of what you felt was an improper invasion of privacy?	2.390	1.408
Privacy protection subjective norm; adapted from Davis and Tuttle (2013), Venkatesh and Davis (2000), Venkatesh et al. (2003)	**Prompt:** Please answer to what extent you agree with the following statements: 7-point Likert-type scales from 1 = “Strongly disagree” to 7 = “Strongly agree”			
	PSN1	People who are important to me believe that I should protect the information on my Android phone.	4.778	1.480
	PSN2	People I respect think that I should protect the information on my Android phone.	4.843	1.502
	PSN3	People whose opinions I value think that I should protect the information on my Android phone.	4.799	1.491
	PSN4	In general, people who are important to me think that protecting information on my Android phone is essential.	4.802	1.476
Personal app interest; adapted from Dinev and Hart (2006)	**Prompt:** Read each of the following statements carefully and indicate the extent to which you agree with the following statements: 7-point Likert-type scales from 1 = “Strongly disagree” to 7 = “Strongly agree”			
	PAI1	The more I want to use an application, the more likely I am to let it access information on my Android phone.	5.482	1.242
	PAI2	If I want to use an application, I am willing to let it access information on my Android phone.	5.156	1.225
	PAI3	I am willing to let an application access information on my Android phone so that I can use the application.	5.125	1.233
	PAI4	In order to be able to use an application, I will allow it to access information on my Android phone.	5.204	1.191
Application subjective norm; adapted from Davis and Tuttle (2013), Venkatesh and Davis	**Prompt:** Please answer to what extent you agree with the following statements: 7-point Likert-type scales from 1 = “Strongly disagree” to 7 = “Strongly agree”			
	ASN1	I often feel influenced by people who are important to me to install applications on my Android phone.	3.601	1.750
	ASN2	People who are important to me often advise me to install applications on my Android phone.	3.836	1.672
	ASN3	I am often encouraged to install applications on my Android phone by people whose opinions I value.	3.915	1.720
	ASN4	People whose opinions I value often suggest that I install applications	3.981	1.665

(2000), Venkatesh et al. (2003)		on my Android phone.		
Positive affect; adapted from Terpstra et al. (2014); Yang and Kahlor (2012)	**Prompt:** Keeping in mind the Android access notifications you see when downloading or using an app, such as (Figure 1 in the main manuscript): Rate the degree to which you agree or disagree with each of the following statements. Receiving an Android access notification when I'm downloading or using an app… 7-point Likert-type scales from 1 = "Strongly disagree" to 7 = "Strongly agree"			
	PA1	Gives me a safe feeling.	3.265	1.489
	PA2	Gives me a good feeling.	3.471	1.550
	PA3	Gives me an excited feeling.	2.959	1.490
	PA4	Gives me a confident feeling.	3.558	1.551
	PA5	Gives me a positive feeling.	3.518	1.562
Negative affect; adapted from Terpstra et al. (2014); Yang and Kahlor (2012)	**Prompt:** Keeping in mind the Android access notifications you see when downloading or using an app, such as (Figure 1 in the main manuscript): Rate the degree to which you agree or disagree with each of the following statements. Receiving an Android access notification when I'm downloading or using an app… 7-point Likert-type scales from 1 = "Strongly disagree" to 7 = "Strongly agree"			
	NA1	Gives me a concerned feeling.	4.298	1.651
	NA2	Gives me an unsafe feeling.	3.903	1.701
	NA3	Gives me a worried feeling.	3.993	1.689
	NA4	Gives me an anxious feeling.	4.025	1.673
	NA5	Gives me a negative feeling.	3.855	1.656
Marker; Job satisfaction; (Posey et al., 2015) adapted from (Cammann et al., 1983)	**Prompt:** Consider your current job and for each of the statements below, indicate the degree to which you agree or disagree with the statement: 5-point Likert-type scales from 1 = "Strongly disagree" to 5 = "Strongly agree"			
	Marker1	All in all, I am satisfied with my job.	3.636	1.171
	Marker2	In general, I don't like my job. (R)	3.674	1.223
	Marker3	In general, I like working here.	3.708	1.112
Attention traps	**At1**	Please answer "Strongly Agree" to this question.		
	At2	The United States is on the continent of Asia.		
	At3	If two plus three is equal to five, select the second choice from the left or if taking the survey on a mobile phone the second from the top.		
	At4	Answer "Somewhat Disagree" to this question.		

(R) = reverse scaled

Appendix B

Convergent and Discriminant Validity for Factorial Validity

We examined our model for convergent and discriminant validity in order to establish factorial validity. Convergent and discriminant validity are interrelated concepts that should coexist (Straub et al., 2004). Methods to test for convergent validity establish that all items "thought to reflect a construct converge, or show significant, high correlations with one another, particularly when compared to the items relevant to other constructs" (Straub et al., 2004, p. 391). Discriminant validity methods establish that "measurement items posited to reflect (i.e., 'make up') that construct differ from those that are not believed to make up the construct" (Straub et al., 2004, p. 389). Following accepted practice, we used two techniques to establish convergent validity and two techniques to establish discriminant validity.

To begin our examination of convergent validity, we examine the outer model loadings that are shown in Table B.1. To establish convergent validity, outer model loadings exceeding 0.700 are desired. Most of the loadings for our items exceed this recommendation. For large sample sizes, loadings above 0.300 are adequate (Hair et al., 2006), and all of our loadings surpass this cutoff. Table B.1 provides the outer model loadings, the t-values, and the significance level for each item. All of our items had t-values above 1.96 and were significant at the $p < 0.05$ level.

As a second check for convergent validity, we examined the cross-loading matrix obtained from

SmartPLS. We show the cross-loading matrix in Table B.2. To establish convergent validity, each item should load highest on its associated latent variable, which is also a method to help establish discriminant validity. In addition, no substantial cross loading should be seen. The general recommendation is that the difference between any two loadings for an item should be > 0.10 (Lowry & Gaskin, 2014). An examination of Table B.2 reveals that all of our items load highest on their primary latent variable and that there are no problematic cross loadings. The results from the application of these two methods support the convergent validity of the scales employed in our study.

We also employed two techniques to establish discriminant validity following recommended statistical guidelines (Gefen & Straub, 2005; Lowry & Gaskin, 2014). Because convergent and discriminant validity are interdependent, they help establish each other. Hence, the first check for discriminant validity is to examine the cross loadings shown in Table B.2. Again, it is recommended that the loading on the primary latent variable should be an order of magnitude greater than the loadings on any other latent variable (i.e., the difference between the loading for the primary latent variable and the next highest loading should be > 0.10) (Lowry & Gaskin, 2014). No problematic cross loadings were discovered for any of our items, which helps establish discriminant validity. As a second check for discriminant validity, we calculated the square roots of the average variance extracted (AVE). The square root of the AVE is shown in Table B.3 as the bold and underlined value in the diagonal of the correlation matrix for the latent variables. The guideline for using this value to establish discriminant validity is that the square root of the AVE should be larger than any of the correlations appearing in the column below it (Fornell & Larcker, 1981; Staples et al., 1999). An examination of Table B.3 shows that this condition is true for all of our latent variables, which further supports the discriminant validity of the scales employed in our study.

Establishing the Lack of Common Methods Bias

We followed the leading literature (Bagozzi, 2011; MacKenzie & Podsakoff, 2012; Podsakoff et al., 2003) to design our research method to counteract common methods bias. We also performed several statistical checks to mitigate concerns over common method bias.

First, we examined the correlation matrix for the latent variables shown in Table B.3 to determine whether any of the latent variables were highly correlated with each other. It is recommended that the correlations should not be > 0.90 (Pavlou et al., 2007), which was true for all the latent variable correlations for our model.

Second, we performed a Harman's single factor test, in which a factor analysis is run constraining the number of factors to one. A single factor accounted for 19.72 percent of the variance, which is well below the suggested threshold of 50 percent. This technique has been disputed in the literature (Podsakoff et al., 2003), and therefore, we employed a third test.

For the third test, we used the marker variable method for PLS (Rönkkö & Ylitalo, 2011). This technique requires the inclusion of "a measure of the assumed source of method variance as a covariate in the statistical analysis" (Podsakoff et al., 2003, p. 889). Hence, we collected data for a marker variable, in our case job satisfaction (see Table A.1) that is theoretically unrelated to our dependent variable, but could be subject to social desirability bias (Lindell & Whitney, 2001; Rönkkö & Ylitalo, 2011). The recommendation is that the marker variable should not be correlated with the dependent variable (i.e., systematic processing) and should have low correlations with the other latent variables. We included the job satisfaction scale in our model and found that it was not significantly associated with systematic processing. We discovered the range of correlations of the marker items to all the other items in the model to be -0.130 to 0.232, with the average of all the item correlations between the marker items and all other items being 0.041. The guideline suggests that the average correlation between the marker items and all other items should be below 0.05 (Rönkkö & Ylitalo, 2011), which is true for our data. The results of our statistical tests conclude that it is unlikely that common method bias is an issue in our study.

Checking for Multicollinearity

The variance inflation factor (VIF), which is a statistic commonly employed to check for multicollinearity, is provided for each item in our model in Table B.4. The statistical guidelines are that the VIFs should be < 5.0 (Cenfetelli & Bassellier, 2009; Peng & Lai, 2012), with VIFs > 5.0 indicating moderate multicollinearity and VIFs > 10.0 indicating severe multicollinearity (Larose & Larose, 2015). All of our items have VIFs well under 10.0 (the highest VIF for our items is 6.083), with most < 5.0, which suggests that multicollinearity is not an issue for our model.

Establishing the Lack of Common Methods Bias

Three reliability statistics are provided in Table B.3 for each of the scales in our instrument. The reliability statistics indicate how consistently a scale will perform over time (Straub, 1989). SmartPLS provides the Cronbach's alphas, composite reliabilities, and AVEs for each scale as part of its output. The guidelines suggest that for each scale the composite reliability should be >= 0.70 (Hair et al., 2006), the Cronbach's

alpha should be >= 0.70 (Davis, 1964; Peterson, 1994), and the AVE should be >= 0.50 and less than the composite reliability (Fornell & Larcker, 1981; Hair et al., 2006). The composite reliabilities for all of our scales exceed 0.70, as do the Cronbach's alphas for our scales. The AVEs are all greater than 0.50 and less than the corresponding composite reliability. Hence, the statistical results suggest our scales are reliable.

Summary of Pre-analysis Validation

Our statistical analyses described in this appendix indicate strong support for convergent and discriminant validity, no multicollinearity issues, good scale reliabilities, and a lack of common method bias concern. Hence, our data meets or exceeds the expected standards for a PLS-based analysis of our model (Cenfetelli & Bassellier, 2009; Diamantopoulos & Siguaw, 2006; Lowry & Gaskin, 2014; Peng & Lai, 2012; Petter et al., 2007).

Table B.1. Outer Model Loadings to Establish Convergent Validity

Latent construct	Items	Outer loading	t-statistic
Systematic processing; adapted from Davis and Tuttle (2013)	**SProc1**	0.873	85.376***
	SProc2	0.776	42.221***
	SProc3	0.726	33.775***
	SProc4	0.739	34.393***
	SProc5	0.871	85.228***
	SProc6	0.763	37.878***
Heuristic processing; developed for the current study	**HProc1**	0.816	47.555***
	HProc2	0.815	46.049***
	HProc3	0.661	18.120***
	HProc4	0.773	30.229***
	HProc5	0.743	27.997***
	HProc6	0.595	17.926***
	HProc7	0.645	19.429***
Information sufficiency; adapted from Trumbo (2002)	**Suff1**	0.920	80.331***
	Suff2	0.939	124.337***
	Suff3	0.925	100.560***
	Suff4	0.902	40.961***
	Suff5	0.912	75.633***
	Suff6	0.897	44.339***
	Suff7	0.937	108.326***
Information gathering capacity; adapted from Zhang et al. (2013)	**IGC1**	0.814	38.377***
	IGC2	0.897	82.088***
	IGC3	0.847	41.902***
Personal app interest; adapted from Dinev and Hart (2006)	**PAI1**	0.852	58.481***
	PAI2	0.901	57.055***
	PAI3	0.923	116.125***
	PAI4	0.914	85.085***
Android privacy concerns; adapted from Dinev and Hart (2006)	**APC1**	0.948	145.499***
	APC2	0.931	103.472***
	APC3	0.944	138.780***
	APC4	0.942	112.944***
Privacy protection subjective norm; adapted from Davis and Tuttle (2013), Venkatesh and Davis (2000), Venkatesh et al. (2003)	**PSN1**	0.919	94.988***
	PSN2	0.914	73.290***
	PSN3	0.915	82.128***
	PSN4	0.901	80.589***
App subjective norm; adapted from Davis and Tuttle (2013), Venkatesh and Davis (2000), Venkatesh et al. (2003)	**ASN1**	0.896	87.278***
	ASN2	0.912	79.100***
	ASN3	0.929	121.888***
	ASN4	0.910	81.736***
Positive affect; adapted from	**PA1**	0.908	99.514***

Terpstra et al. (2014); Yang and Kahlor (2012)	**PA2**	0.923	87.201***
	PA3	0.836	55.240***
	PA4	0.886	73.625***
	PA5	0.919	108.649***
Negative affect; adapted from Terpstra et al. (2014); Yang and Kahlor (2012)	**NA1**	0.803	5.218***
	NA2	0.916	5.880***
	NA3	0.859	5.633***
	NA4	0.851	5.810***
	NA5	0.954	5.571***
Job satisfaction; Posey et al. (2015) adapted from Cammann et al. (1983)	**Marker1**	0.960	19.010***
	Marker2	0.860	11.935***
	Marker3	0.965	17.092***

*p < 0.05, **p < 0.01, ***p < 0.001, (n/s) = not significant.

Table B.2. Cross Loadings

Items	SProc	HProc	Suff	IGC	PAI	APC	PSN	ASN	PA	NA	Marker
SProc1	0.873	0.196	0.063	0.326	-0.214	0.112	0.192	0.106	0.211	-0.037	0.068
SProc2	0.776	0.145	0.034	0.217	-0.188	0.110	0.174	0.170	0.259	-0.050	0.102
SProc3	0.726	0.245	0.024	0.140	-0.168	0.133	0.267	0.238	0.230	-0.019	0.093
SProc4	0.739	0.227	0.028	0.286	-0.171	0.134	0.229	0.087	0.161	-0.052	0.048
SProc5	0.871	0.165	0.051	0.253	-0.242	0.121	0.175	0.095	0.229	-0.042	0.070
SProc6	0.763	0.395	0.099	0.248	-0.166	0.103	0.248	0.138	0.198	-0.042	0.081
HProc1	0.162	0.816	0.089	0.122	0.235	0.044	0.068	0.092	0.089	-0.091	0.033
HProc2	0.294	0.815	0.106	0.154	0.133	0.126	0.133	0.131	0.108	-0.081	0.035
HProc3	0.188	0.661	0.118	0.213	0.189	0.038	0.112	0.089	0.066	-0.054	0.046
HProc4	0.214	0.773	0.097	0.104	0.156	0.054	0.133	0.202	0.060	-0.049	0.054
HProc5	0.103	0.743	0.116	0.069	0.225	-0.019	0.024	0.185	0.122	-0.039	0.013
HProc6	0.183	0.595	0.124	0.100	0.184	0.001	0.076	0.135	0.195	-0.081	0.059
HProc7	0.295	0.645	0.005	0.077	0.028	0.124	0.187	0.166	0.126	-0.003	0.031
Suff1	0.047	0.097	0.920	0.458	0.132	-0.305	-0.102	-0.004	0.366	-0.412	0.119
Suff2	0.088	0.139	0.939	0.473	0.127	-0.247	-0.026	0.021	0.331	-0.380	0.111
Suff3	0.076	0.133	0.925	0.477	0.145	-0.259	-0.020	0.037	0.345	-0.397	0.130
Suff4	0.009	0.061	0.902	0.432	0.114	-0.269	-0.076	0.018	0.298	-0.372	0.091
Suff5	0.075	0.127	0.912	0.481	0.142	-0.245	-0.050	0.006	0.343	-0.367	0.102
Suff6	0.012	0.117	0.897	0.433	0.147	-0.261	-0.067	0.010	0.308	-0.373	0.065
Suff7	0.060	0.111	0.937	0.472	0.110	-0.290	-0.061	0.007	0.343	-0.384	0.119
IGC1	0.223	0.128	0.499	0.814	0.039	-0.079	0.027	0.004	0.256	-0.255	0.122
IGC2	0.290	0.150	0.443	0.897	0.083	-0.045	0.116	0.041	0.250	-0.206	0.107
IGC3	0.278	0.149	0.366	0.847	0.044	-0.008	0.171	0.064	0.186	-0.148	0.115
PAI1	-0.215	0.220	0.063	0.039	0.852	-0.070	0.001	0.013	-0.016	-0.047	-0.029
PAI2	-0.218	0.169	0.148	0.080	0.901	-0.155	-0.016	0.052	0.053	-0.112	-0.015
PAI3	-0.223	0.218	0.172	0.071	0.923	-0.122	-0.011	0.028	0.043	-0.120	0.006
PAI4	-0.212	0.187	0.135	0.049	0.914	-0.104	-0.006	0.034	0.041	-0.087	0.025
APC1	0.149	0.069	-0.249	-0.034	-0.116	0.948	0.291	0.117	-0.186	0.326	-0.050
APC2	0.122	0.079	-0.283	-0.079	-0.125	0.931	0.311	0.169	-0.203	0.343	-0.049
APC3	0.135	0.073	-0.273	-0.028	-0.106	0.944	0.332	0.140	-0.194	0.335	-0.063
APC4	0.153	0.077	-0.282	-0.046	-0.123	0.942	0.296	0.144	-0.223	0.361	-0.047
PSN1	0.256	0.134	-0.036	0.119	0.010	0.291	0.919	0.308	0.016	0.110	0.034
PSN2	0.235	0.145	-0.063	0.112	-0.014	0.317	0.914	0.357	0.028	0.142	0.015
PSN3	0.217	0.119	-0.043	0.116	-0.015	0.295	0.915	0.346	0.037	0.135	0.011
PSN4	0.270	0.143	-0.063	0.121	-0.014	0.287	0.901	0.326	0.080	0.109	0.062
ASN1	0.162	0.192	0.009	0.008	0.031	0.130	0.305	0.896	0.155	0.031	0.046

ASN2	0.168	0.155	0.014	0.034	0.012	0.132	0.336	0.912	0.143	0.043	0.023
ASN3	0.155	0.195	0.008	0.061	0.045	0.154	0.356	0.929	0.140	0.009	0.057
ASN4	0.148	0.172	0.028	0.062	0.039	0.132	0.339	0.910	0.150	0.001	0.063
PA1	0.252	0.141	0.306	0.206	0.014	-0.183	0.055	0.156	0.908	-0.452	0.229
PA2	0.237	0.137	0.341	0.278	0.047	-0.203	0.037	0.118	0.923	-0.524	0.220
PA3	0.260	0.128	0.239	0.183	0.003	-0.154	0.050	0.223	0.836	-0.307	0.169
PA4	0.229	0.131	0.402	0.282	0.041	-0.217	0.018	0.091	0.886	-0.527	0.198
PA5	0.224	0.134	0.355	0.257	0.046	-0.204	0.038	0.124	0.919	-0.552	0.197
NA1	-0.001	-0.030	-0.332	-0.171	-0.100	0.378	0.174	0.016	-0.396	0.803	-0.086
NA2	-0.064	-0.045	-0.393	-0.224	-0.092	0.339	0.145	0.069	-0.490	0.916	-0.096
NA3	0.004	-0.018	-0.373	-0.206	-0.098	0.362	0.163	0.057	-0.479	0.859	-0.074
NA4	-0.036	-0.026	-0.366	-0.236	-0.083	0.332	0.131	0.062	-0.396	0.851	-0.098
NA5	-0.055	-0.117	-0.387	-0.208	-0.094	0.312	0.094	-0.021	-0.515	0.954	-0.100
Marker1	0.103	0.044	0.136	0.150	-0.013	-0.081	0.026	0.067	0.234	-0.117	0.960
Marker2	0.046	0.002	0.055	0.080	0.001	-0.024	0.062	0.067	0.165	-0.062	0.860
Marker3	0.097	0.074	0.106	0.121	0.004	-0.036	0.030	0.027	0.214	-0.098	0.965

Table B.3. Measurement Model Statistics and AVEs

Latent construct	C.R.	C.A.	AVE	SProc	HProc	Suff	IGC	PAI	APC	PSN	ASN	PA	NA	Mark
SProc	0.910	0.881	0.630	**0.794**										
HProc	0.885	0.847	0.527	0.292	**0.726**									
Suff	0.974	0.970	0.844	0.064	0.129	**0.919**								
IGC	0.889	0.813	0.728	0.311	0.168	0.505	**0.853**							
PAI	0.943	0.920	0.807	-0.242	0.222	0.144	0.066	**0.898**						
APC	0.969	0.957	0.886	0.149	0.079	-0.288	-0.049	-0.125	**0.941**					
PSN	0.952	0.933	0.832	0.270	0.149	-0.057	0.129	-0.009	0.326	**0.912**				
ASN	0.952	0.933	0.832	0.173	0.197	0.016	0.045	0.035	0.150	0.366	**0.912**			
PA	0.953	0.937	0.801	0.270	0.150	0.365	0.268	0.033	-0.214	0.045	0.161	**0.895**		
NA	0.944	0.936	0.772	-0.051	-0.080	-0.417	-0.233	-0.102	0.363	0.135	0.023	-0.525	**0.878**	
Marker	0.950	0.928	0.864	0.097	0.054	0.117	0.134	-0.004	-0.055	0.035	0.052	0.227	-0.106	**0.930**

Note: Bolded, underlined values represent the square root of the AVEs

Table B.4. Collinearity Statistics

Latent construct	Items	VIF	Latent construct	Items	VIF
Systematic processing; adapted from Davis and Tuttle (2013)	SProc1	3.158	Information gathering capacity; adapted from Zhang et al. (2013)	IGC1	1.747
	SProc2	1.982		IGC2	2.161
	SProc3	1.654		IGC3	1.710
	SProc4	1.703	Android privacy concerns; adapted from Dinev and Hart (2006)	APC1	5.479
	SProc5	3.258		APC2	4.626
	SProc6	1.723		APC3	5.338
Heuristic processing; developed for the current study	HProc1	2.402		APC4	4.822
	HProc2	2.252	Personal app interest; adapted from Dinev and Hart (2006)	PAI1	2.150
	HProc3	1.452		PAI2	3.348
	HProc4	1.941		PAI3	3.989
	HProc5	1.879		PAI4	3.721
	HProc6	1.356	Positive affect; adapted from Terpstra et al. (2014); Yang and Kahlor (2012)	PA1	3.700
	HProc7	1.350		PA2	4.783
Information sufficiency; adapted from Trumbo (2002)	Suff1	5.021		PA3	2.358
	Suff2	5.659		PA4	3.619
	Suff3	4.788		PA5	4.777
	Suff4	5.855	Negative affect; adapted	NA1	2.647

	Suff5	4.293	from Terpstra et al. (2014); Yang and Kahlor (2012)	NA2	3.759
	Suff6	5.289		NA3	3.718
	Suff7	6.083		NA4	2.996
Privacy protection subjective norm; adapted from Davis and Tuttle (2013), Venkatesh and Davis (2000), Venkatesh et al. (2003)	PSN1	3.660		NA5	3.501
	PSN2	3.571	Job satisfaction; Posey et al. (2015) adapted from Cammann et al. (1983)	Marker1	4.577
	PSN3	3.825		Marker2	2.886
	PSN4	2.939		Marker3	4.608
App subjective norm; adapted from Davis and Tuttle (2013), Venkatesh and Davis (2000), Venkatesh et al. (2003)	ASN1	2.899			
	ASN2	3.555			
	ASN3	4.078			
	ASN4	3.572			

References for Appendices

Bagozzi, R. P. (2011). Measurement and meaning in information systems and organizational research: Methodological and philosophical foundations. *MIS Quarterly*, *35*(2), 261-292.

Cammann, C., Fichman, M., Jenkins, D., & Klesh, J. R. (1983). Assessing the attitudes and perceptions of organizational members. In E. Lawler, P. Mirvis & C. Cammann (Eds.), *Assessing organizational change: A guide to methods, measures, and practices* (pp. 71-138). New York: Wiley.

Cenfetelli, R. T., & Bassellier, G. (2009). Interpretation of formative measurement in information systems research. *MIS Quarterly*, *33*(4), 689-707.

Davis, F. B. (1964). *Educational Measurements and their Interpretation*. Belmont, CA: Wadsworth Publishing Company.

Davis, J. M., & Tuttle, B. M. (2013). A heuristic-systematic model of end-user information processing when encountering IS exceptions. *Information & Management*, *50*(2), 125-133.

Diamantopoulos, A., & Siguaw, J. A. (2006). Formative versus reflective indicators in organizational measure development: A comparison and empirical illustration. *British Journal of Management*, *17*(4), 263-282.

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, *17*(1), 61-80.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, *18*(1), 39-50.

Gefen, D., & Straub, D. W. (2005). A practical guide to factorial validity using PLS-Graph: Tutorial and annotated example. *Communications of the Association for Information Systems*, *16*(5), 91-109.

Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., & Tatham, R. L. (2006). *Multivariate Data Analysis*. Upper Saddle River, NJ: Pearson Prentice Hall

Larose, D. T., & Larose, C. D. (2015). *Data mining and predictive analytics* (2nd ed.). Hoboken, NJ: Wiley.

Lindell, M. K., & Whitney, D. J. (2001). Accounting for common method variance in cross-sectional research designs. *Journal of Applied Psychology*, *86*(1), 114.

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*(2), 123-146.

MacKenzie, S. B., & Podsakoff, P. M. (2012). Common method bias in marketing: Causes, mechanisms, and procedural remedies. *Journal of Retailing*, *88*(4), 542-555.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, *15*(4), 336-355.

Pavlou, P., Liang, H., & Xue, Y. (2007). Understanding and mitigating uncertainty in online exchange relationships: A principal-agent perspective. *MIS Quarterly*, *31*(1), 105-136.

Peng, D. X., & Lai, F. (2012). Using partial least squares in operations management research: A practical guideline and summary of past research. *Journal of Operations Management*, *30*(6), 467-480.

Peterson, R. A. (1994). A meta-analysis of Cronbach's coefficient alpha. *Journal of Consumer Research*, *21*(2), 381-391.

Petter, S., Straub, D. W., & Rai, A. (2007). Specifying formative constructs in information systems research. *MIS Quarterly*, *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. *Journal of Applied Psychology*, *88*(5), 879-903.

Posey, C., Roberts, T. L., & Lowry, P. B. (2015). The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems*, *32*(4), 179-214.

Rönkkö, M., & Ylitalo, J. (2011, December 4-7). *PLS marker variable approach to diagnosing and controlling for method variance*. Paper presented at the Thirty-Second International Conference on Information Systems, Shanghai, PRC.

Staples, D. S., Hulland, J. S., & Higgins, C. A. (1999). A self-efficacy theory explanation for the management of remote workers in virtual organizations. *Organization Science*, *10*(6), 758-776.

Straub, D., Boudreau, M.-C., & Gefen, D. (2004). Validation guidelines for IS positivist research. The *Communications of the Association for Information Systems*, *13*(1), 380-426.

Straub, D. W. (1989). Validating instruments in MIS research. *MIS Quarterly*, *13*(2), 147-169.

Terpstra, T., Zaalberg, R., Boer, J., & Botzen, W. (2014). You have been framed! How antecedents of information need mediate the effects of risk communication messages. *Risk Analysis*, *34*(8), 1506-1520.

Trumbo, C. W. (2002). Information processing and risk perception: An adaptation of the heuristic-systematic model. *Journal of Communication*, *52*(2), 367-382.

Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management Science*, *46*(2), 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*(3), 425-478.

Yang, Z. J., & Kahlor, L. (2012). What, me worry? The role of affect in information seeking and avoidance. *Science Communication*, *35*(2), 189-212.

Zhang, L., Pavur, R., York, P., & Amos, C. (2013). Testing a model of users' web risk information seeking intention. *Informing Science: The International Journal of an Emerging Transdiscipline*, *16*(1), 1-18.