Journal of Global Information Management
Volume 31 • Issue 1

Inattention and Forewarning on Individuals' Smart Apps Permissions-Consenting Behavior

Solomon Negash, Kennesaw State University, USA
Peter Meso, Florida Gulf Coast University, USA
Philip Musa, The University of Alabama at Birmingham, USA*

ABSTRACT

In the era of bring-your-own-device and general data protection regulation, corporate network managers have limited control over the non-corporate-owned devices connected onto their corporation's network. However, they are principally responsible for the consequent liabilities that may accrue from breaches of individual consumers' privacy traceable to the network. Hence, this study revisits the notion of information-privacy at the point of contact between an individual end user and the smart-apps that the end user employs. The authors examine the impacts of inattention on consumers' behavioral reactions to perceived smart-app privacy concerns. The authors find that inattention's effects on consumers' behavioral reactions, especially pertaining to re-examination and modification of an app's default permissions settings, is significant. Forewarning has significant impacts on mitigating inattention and altering consumers' behavioral reactions pertaining to re-examination and modification of an app's default permissions settings. Implications of these findings on corporate privacy management are discussed.

KEYWORDS

App Permissions, Forewarning, Inattention, Information Privacy Concerns (IPC), Smart-Apps

INTRODUCTION

The era of smart applications (hereafter referred to as smart-apps) and the Internet of Things (IoT) brings with it tensions among communications and economic considerations and personal information privacy concerns (Rath & Kumar, 2021; Fox et al., 2021; Acquisti et al., 2015; Dinev, 2014; Teubner & Flath, 2019; FTC, 2014; Carpenter et al., 2019; Chan & Saqib, 2021). Fundamental to these tensions is, first, the mechanisms and methods used to harvest personal data. Second, how much of one's personal information is too-much when disclosed, shared, collected, or mined in the economic and communications transactions. As Teubner and Flath (2019) point out, 'the boundaries between

DOI: 10.4018/JGIM.328519 *Corresponding Author

This article published as an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/) which permits unrestricted use, distribution, and production in any medium, provided the author of the original work and original publication source are properly credited.

the private and economic spheres have started to erode' (pp. 213). Software applications designed to function on mobile phones, tablets, wearables, and IoT user-interfaces incrementally mandate the exchange of personal information. Thus, serving as fodder for the community-building and/or trust-enhancement initiatives that leverage the success of their economic models (Einav et al., 2015; Proserpio et al., 2016; Stutzman & Kramer-Duffield, 2010). These software applications are collectively termed smart-apps. Smart-apps have shifted the way personal information is collected and used by companies, hence, raising critical information privacy concerns (Dinev & Hart, 2006; Krasnova et al., 2012; Goldfard & Tucker, 2012; Lutz et al., 2018).

One consequence of this is that the related issues of privacy-consent mechanisms employed within smart-apps and consequent impacts on end-users' information privacy are increasingly becoming contentious in present day information society. Advances in the architecture, structure, and complexity of smart-apps as well as enhancements in the scope, breadth, and ubiquity-of-usages has significantly changed. Hence the need to examine whether consumers are harmed or better served by current privacy-consenting mechanisms inherent in these apps. This notwithstanding, it is worth noting that Bring Your Own Device (BYOD) is changing control of organizational computing. The mobile generation relies heavily on BYOD and more employees in international organizations are using their personal smartphones for work purposes (Ameen et al., 2021). The 186 billion BYOD market in 2019 (Onanuga, 2020) is projected to grow to 367 billion in 2022 (Georgiev, 2021) and 430 billion in 2025 (Onanuga, 2020). BYOD is adopted by 69% of organizations (BYOD, 2020). BYOD market analysis indicates that 95% of organizations allow personal devices in some way in the workplace, 78% of organizations in the US had BYOD activities since 2018, 67% of employees use personal devices at work, BYOD generates $350 of value each year per employee, a BYOD-carrying employee works an extra two hours, and 87% of businesses are dependent on their employee's ability to access mobile business apps from their smartphone (Georgiev, 2021).

While BYOD have contributed to productivity gains in many organizations, they have also been a source or security vulnerabilities that worry the very same organizations. Some of the security risks and potential exposures attributed to BYOD include malformed content such as videos and image files that BYOD devices may have downloaded from external sources and systems outside of the control of a firm's cybersecurity installations; systems software and platforms that may still possess 'holes' owing to laxity by various BYOD owners to patch their devices and or ensure that the versions of software applications installed on their devices are the most current; Theft and/or loss of sensitive and proprietary corporate data owing to stolen or lost BYOD devices; unauthorized access and or intrusion into corporate networks via on-the-road employees connecting to third party networks, such as at airports or hotels, that may not be as thorough in their cybersecurity defense and intrusion detection mechanisms as the employee's employer may be (Virgillito, 2020; von Ogden, 2023). For example, a security research firm "discovered a vulnerability in network routers used by hotels across 29 countries. The flaw allowed hackers to monitor and tamper with traffic from Wi-Fi networks and even access management systems" (Virgillito, 2020). On the other hand, General Data Protection Regulation (GDPR) is being adopted beyond the 28 Schengen countries. A look at the 90 countries listed by the Digital Innovation Index (2020) show majority of these countries have implemented personal information protection policies and regulations.

Therefore, this study seeks to revisit the notion of information-privacy at the point of contact between an individual end-user and the smart-apps. Our study examines the impacts of inattention on end-users' permissions consenting behavior. It then examines effects of forewarning on end-user's permissions consenting behavior. A survey-based simulated pre-test, treatment, post-test study is conducted to determine the impact of inattention and forewarning on end-user's permissions consenting behavior. It uses the pre-treatment data to assess impacts of inattention. Forewarning is implemented as the treatment. We then contrast pre-treatment and post treatment data to assess if forewarning results in observable changes in end-users' permissions consenting behavior. The paper then discusses the implications of its findings on corporate privacy management within the present-day BYOD and

GDPR era. We look at the dilemma corporate network managers have with limited control over the non-corporate-owned devices connected onto their corporation's network, and yet remain principally responsible for the consequent liabilities that may accrue from breaches of individual consumers' privacy traceable to the network.

For purposes of this study, we define smart-apps as software applications that have advanced auto-data-capture and/or auto-sensing capabilities. Features such as geolocation (e.g., GPS), accelerometer (e.g., technologies that sense movements or vibrations), environmental sensing (e.g., cameras, microphones), and bio sensing (e.g., technologies that sense body temperature, heart rate, perspiration, etc.).

THEORETICAL BACKGROUND

Privacy Review

The individuals' Information Privacy Concerns (IPC) model proposed by Smith et al. (1996) was ground-breaking in that it provided a framework for understanding individual's information privacy concerns. It defined and conceptualized IPC as a formative construct made up of four factors, namely, data-collection, unauthorized-secondary-use, improper-access, and errors-in-the data. When the Internet became prevalent, leading to an exponential increase in digital data-collection and access, Malhotra et al. (2004) extended the conceptualization of the IPC model. Malhotra et al. (2004) included control and awareness as additional formative factors and renamed the model IUPC (Internet Users Privacy Concerns). They also identified two precedent constructs impacted by IUPC, namely, trusting beliefs and risk beliefs.

Over the same time span, several researchers have provided comprehensive reviews of the literature on consumer's information privacy concerns including Hong and Thong (2013); Bélanger and Crossler (2011); Li (2011); Smith et al. (2011); Dinev and Hart (2004); Malhotra et al. (2004); and, Smith et al. (1996). Some of these extensive review studies resulted in the proposal of new or extended IPC models. Smith et al. (2011), for example, upon extensively reviewing published research on information privacy, integrated the dominant privacy perspectives into a comprehensive model that they termed the Antecedents-Privacy Concerns-Outcomes (APCO) Model. Hong and Thong (2013) also conducted an extensive review of the literature and proposed therefrom that IUPC is a second order formative construct made up of awareness plus two first order factors, termed information-management and interaction-management, respectively. Interaction-management aggregates three of the factors initially identified by Smith et al (1996) and Malhotra et al (2001), namely, data-collection, unauthorized-secondary-use, and control. Information management comprises errors-in-data and improper-access. In this regard, it remains in keeping with earlier conceptualizations of IPC.

Privacy Risk and Privacy Calculus

The APCO model, however, deviates somewhat from prior conceptualizations of IPC as it introduces the concept of the privacy-calculus. APCO 'posits that individuals' responses to external stimuli result in a deliberate privacy calculus that leads to fully informed privacy related behaviors (Choi et al., 2018, pp. 127-128). APCO acknowledges that there can be antecedents to IPC, and that such antecedent factors tend to vary from one decision-making context to another. In this regard, privacy concerns can be perceived as being transaction-specific in nature (Ackerman & Mainwaring, 2005). They are influenced by the context in which a user is placed, the perceived costs associated with privacy loss, and the perceived beneficial outcomes that a user derives from the transaction (Dinev et al., 2015). For example, Jiang et al. (2013) found that the two-way digital communications where the other party participated anonymously, such anonymity increased an individual's concerns about personal information privacy. It also decreased the individual's evaluation of the social rewards accruing from the digital communications. Further, privacy concerns may also be informed by the

task that a user may be performing, and possibly the device or software application that the user may be employing (Dinev et al., 2015; Hui et al., 2007; Xu et al., 2010; Xu et al., 2012). Consequently, an individual's assessment of his/her privacy concerns will vary based on the antecedents-privacy nexus defined by the context.

Privacy risks have been shown to impact an individual's behavior pertaining to their personal information and the privacy of that information (Choi et al, 2018; Hui et al., 2007; Goldfarb & Tucker, 2012; Mitrou et al., 2014). An individual's perceived privacy risks can be expressed by the extent to which the individual believes that their privacy is open to exploitation (Xu et al., 2011; Carpenter et al., 2019; Future Sight, 2011). Prior research indicates that the higher one's perception of the privacy risks inherent in a transaction, the less the individual is willing to disclose personal information (Dienlin & Metzger, 2016; Sun et al., 2015; Xu et al., 2010, 2012), engage with an information technology application (Luo et al., 2010), or communicate via a digital medium with other parties (Posey & Ellis, 2007; Jiang et al., 2013). As such, perceived privacy risks factor into an individual's privacy calculus. We expect this to apply in the context of users' engagement with smart-apps. In this paper, we test and propose two variables, inattention and forewarning, found to impact smart-app permission granting behavior. We discuss the privacy concern variables in the literature and show empirical support for the impact of inattention on granting smart-app permissions. We also found that forewarning has a moderating effect on inattention and privacy concerns. The findings show inattention has impact on permission granting user behavior and forewarning as an effective strategy to help users make more informed decisions about granting permissions to smart apps.

Privacy concerns arise when users are worried about their personal information being collected, shared, or misused by smart apps. This can be especially concerning if the app is collecting sensitive information such as location data, financial information, or health data. Users may be hesitant to grant permissions if they do not trust the app developer or if they do not fully understand how their data will be used.

Inattention plays a role in user behavior when it comes to granting permissions. Users may not pay close attention to the permissions requested by the app, or they may not fully understand the implications of granting certain permissions. This can lead to users inadvertently granting permissions that they later regret. Forewarning can be an effective way to mitigate the effects of privacy concerns and inattention on user behavior. By providing clear and concise information about what data will be collected and how it will be used, app developers can help users make more informed decisions about granting permissions. Additionally, app developers can provide reminders and warnings throughout the app experience to ensure that users are aware of the data being collected and have the opportunity to revoke permissions if they so choose.

We employ this privacy risk lens in examining an individual's privacy calculus concerning their potential use of smart-apps. Our study stays consistent with extant research by defining privacy risk as threats to the loss of personal information or the loss of control over personal information (Choi et al., 2018; Dienlin & Metzger, 2016; Posey & Ellis, 2007). In the context of this study, privacy risk is operationalized as personal information risks associated with a user's interaction with, or usage of, a smart-app.

IPC and Smart-Apps Use

Smart-apps continue to experience meteoric diffusion within the information systems ecosystem. Increasing number of consumers embrace the convenience and pliability of nomadic computing, as well as the ever-growing range of computational capabilities and services embedded within these applications (Alani, 2017; Choi et al 2018; Mitrou et al., 2014; Brennan, 2016; Chike-Obiekwe et al., 2020). Empirical assessments of privacy or privacy calculus in the smart-apps domain are still sparse (Choi et al. 2018; Lin & Armstrong, 2019). But suggests that privacy remains an important concern among users of smart-apps (Brennan & Lovells, 2016; Future Sight, 2011). Most of prior published studies in this sub-domain focus on the dispositional privacy concerns of individuals as

they employ devices upon which smart-apps have been installed (Scutti, 2017; Mitrou et al., 2014; Krasnova et al., 2009). Others critically expose the emergent privacy risks associated with novel functions and features, uses of, or data-capture modalities inherent in emergent smart applications and IoT applications (Sutanto et al., 2013; Metzger, 2004; Prabhakar et al., 2003; Oliveira & Zaïane, 2002; Goldfarb & Tucker, 2012). These studies paradoxically report that despite privacy being a concern, individuals still engage with smart-apps without much cognitive forethought about the privacy-risks to which they may be exposing themselves. For example, a survey of over 4,000 android users, designed to assess 'users' interaction with the permissions required by different applications they installed, revealed apparent weakness in the awareness of Android users regarding the privacy of their data' (Alani, 2017, p. 130). Indeed, research on the use of social-media applications and other smart-communications applications suggests that many individuals freely engage in self-disclosure of personal private information in extents that significantly compromise their individual privacy (Campbell, 2019). Research in the interpersonal communication and electronic commerce domains also offers insight into the privacy-calculus evaluations (Karl & Peluchette, 2011; Xu et al., 2012; Choi et al., 2018).

We note that most published studies examining privacy or privacy calculus within the context of smart-apps generalize smart-apps as being integral types of Internet-enabled software. Internet-enabled software are broadly classified as business-to-consumer (B2), business-to-business (B2), or consumer-to-consumer (C2) software applications on the one hand (Scutti, 2017; Metzger, 2004; Luo et al., 2010; Angst & Agarwal, 2009) or social media and communications software on the other (Krasnova et al., 2009; Chen, 2013; Mitrou et al., 2014). The bundling of smart applications into these broader software-types may explain the predominant use of the dispositional-privacy lens in examining and assessing privacy concerns associated with these types of software applications. However, this obfuscates some fundamental architectural differences of smart-apps when contrasted to conventional media-and-communications software or e-commerce and m-commerce software. Smart-apps represent additional potential sources of privacy invasions. Unlike earlier generations of software applications, smart-apps are particularly intrusive in their design (Oliveira & Zaïane, 2002). Beyond the overt data-entry-based submission of, and transparent self-disclosure of, personal information manifest in conventional software applications, the architecture of smart-apps and IOT applications enables them to engage in both overt and covert data-capture. Privacy invasions may occur due to covert capture and disclosure of personal data as an individual use or engages with smart-apps. Such invasions may be accidental, or they may be deliberate and intentionally built into the way the smart-apps functions. It is likely that the end user may be unaware of the scope, extent, or mechanisms by which personal information is being captured and disclosed to other parties by smart-apps; or the nature and timings of such disclosures. A well-documented example of this is the 'super bright flashlight application' (Alani, 2017) that compelled end users who downloaded it to provide much more permissions to access user-data from a user's device than was needed to perform the primary functions for which it was designed. When such permissions were granted, covert methods were used to capture and disseminate the individuals' personal information to external parties. Alepis and Patsakis (2017) showcase how smart applications installed on devices using the Android operating system 'can still determine users' location efficiently without requiring any such permission …. from the user [and] can even return the results when … running in the background, so the user is unaware of any of its actions' (p. 278).

Because of this, an assessment of privacy concerns and privacy calculus within the context of smart-apps using a purely transactional lens or dispositional-privacy lens is, in our opinion, wanting. Such assessments fail to consider the covert and hyper-intrusive properties of smart-apps. One potential approach to addressing this gap is to employ a cognitive perspective to smart-apps use with respect to privacy concerns by examining end-users' permissions granting behavior, particularly when cognitively inattentive to the privacy implications of their choices.

RESEARCH QUESTIONS AND HYPOTHESIS

Prior studies point to the role and contributions of cognition in an individual's privacy calculus. For example, Choi et al. (2015) demonstrate that individuals typically struggle with information overload and limited cognitive resources when evaluating privacy risks against perceived benefits of using an information technology and are thereby vulnerable to heuristic and cognitive biases. They find that individuals are likely to take mental shortcuts (e.g., dispositions) to bypass the cognitive challenges they experience when performing privacy risk-reward or cost-benefit assessments.

Cognitive dispositions may also have a bearing on behavioral reactions concerning the effects of a privacy trade-off. For example, individuals have been shown to discount the risks associated with a particular action cognitively, such as the disclosure of personal information, where the risk was spread over time or when such the risk was inevitable (Smith et al., 2011). Consequently, 'emerging evidence hints at the role of privacy dispositions in shaping the intricate joint influence of perceived risk and benefit on privacy related behaviors (Choi et al. 2018, p. 126). It can also be argued that certain cognitive actions potentially may diminish or enhance an individual's sensitivity to privacy of personal information. We elect to focus on inattention as a factor, and forewarning as an action, that influence end-users' information privacy calculus as demonstrated by their permissions consenting behavior.

Smartphone have assisted a stream of new applications and turned out to be a symbol of our times. The absent-minded use of smartphones is linked to mind wandering and lack of attention; excessive smartphone use causes inattention among school children (Nayak & Padmashali, 2020). Inattention was found to predict lack of success among graduate students when seeking online information (Burek & Martinussen, 2021).

The theory of rational inattention assumes that agents cannot process all available information, hence the agent chooses what and how much information to absorb (Sims, 2003). Smartphones have made voluminous amount of information available at our finger tips, and yet we are able to digest little of it. After reviewing the recent literature on rational inattention Mackowiak et al. (2021) posit that the pieces of information we possess and act upon is largely determined by which information we choose to pay attention to.

Conscious experience is fluid; it rarely remains on one topic for an extended period without deviation (Smallwood & Schooler, 2015). The dynamic nature of consciousness is illustrated by the experience of mind wandering, in which attention switches from a current task to unrelated thoughts and feelings (Smallwood & Schooler, 2015). Personal data constitute the main source of revenue of several online companies (Marreiros et al., 2017) hence, targeted advertising senders prefers to target receivers' rational inattention and inability to independently acquire information as optimal disclosure strategy (Matveenko & Starkov, 2021).

In many cases, consumers may be inattentive about the digital transactions of their data; people's dormant privacy concerns may manifest only when consumers are asked to think about privacy (Marreiros et al., 2017). Highlighting online privacy policies affect consumers' privacy actions and attitudes. Participants adopt a more conservative stance on disclosing sensitive and identifiable information but do not change their attitudes and social actions towards privacy. Marreiros et al. (2017) posit that privacy behavior is not necessarily sensitive to exposure to objective threats or benefits of disclosing personal information and found that privacy concerns are dormant and manifest when users are asked to think about privacy.

Zheng et al. (2014) investigated the association of inattention with mobile phone use. Their population based cross-sectional study of 7102 adults found significant inattention among mobile users, the inattention was stronger among adults that use their mobile phones over 60 minutes per day. Failure to check for information is a typical form of inattention. A Swedish car crash study found distraction and inattention as threats to road safety. One third of the fatal road crashes among at-fault drives were due to inattention and a third of these were caused by pedestrian inattention.

To this end, we posit that cognition may have a bearing on an individual's privacy dispositions and or behaviors. Specifically, we operationalize and examine effects of contemplative cognition on individual's information privacy beliefs and behaviors. We define contemplative cognition as the attentive concentration on, and consideration of, events happening in the present (Grossenbacher & Quaglia, 2017). The contemplative cognition 'integrates three attention-related processes entailed by a variety of contemplative practices: intended attention, attention to intention, and awareness of transient information' (Grossenbacher & Quaglia, 2017, p. 1580).

We define inattention as failure to check for information (Sundfor et al., 2019), the deviation of attention and experience of mind wandering (Smallwood & Schooler, 2015) from the event at present.

Forewarning facilitates attitude change (Apsler & Sears, 1968) and enhanced resistance to persuasion on individuals with high levels of prior bias (Neimeyer et al., 1991). Providing participants with a forewarning about a scam attempt reduced susceptibility (Scheibe et al., 2014). A field experiment on the impact of forewarning on people who were victimized by telemarketing fraud found that forewarning reduced the impact from the same scam, but the forewarning benefits on a new scam loses effect overtime (Scheibe et al., 2014).

Assisting people remember forewarning through a direct central route increased the participants' ability to detect advertisers' manipulative intent. (Daiku, 2020). Younger and older adults are targeted by fraudulent email phishing scams at the same rate, however, older adults are more likely to mislabel a legitimate email as fraudulent, fraud prevention and educational initiatives can help reduce these frauds (O'Connor et al., 2021). Forewarning reduces fraud susceptibility in vulnerable consumers (Scheibe et al., 2014). Sundfør et al. (2019) identified awareness education (or forewarning) as one of the approaches for reducing inattention.

Consequently, the two research questions this paper seeks to address are:

RQ1: Does inattention impact (i.e. mitigate) an individual's privacy calculus within the context of smart-apps installation? Is there a relationship between inattention and end user's permissions-settings / permissions consenting behavior when installing new smart-apps?

RQ2: Does forewarning impact an individual's privacy calculus (and by so doing moderate the effects of inattention on permissions consenting behavior) within the context of smart-apps installation? Is there a relationship between forewarning and deliberative (purposeful) alteration of default permissions-settings within smart-apps?

Our basic hypothesis is that, at the point of installing a smart app, end-users generally do not pay much attention to the default permissions that are established in the app. If asked to self-report their perceptions on smart-app permissions, terms and conditions of use, end-users are likely to indicate that they accept the default settings without much of a review – a measure of end-users' inattention (indifference) to the app's privacy permissions settings. In this study, we operationalize inattention by examining end-users' pre-test permissions consenting dispositions and the relationship of these dispositions to reported future use intention. Therefore, we posit the following two hypotheses with respect to inattention:

Hypothesis 1a: Inattention to privacy risks inherent on smart-apps has a significant impact on individuals' - privacy-related app permissions behavior.

Hypothesis 1b: Inattention has a significant impact on individuals' reported future use of smart-apps.

We operationalize forewarning as a treatment where we prime end-users to pay attention to privacy concerns thereby reassessing their privacy calculus pertaining to smart-apps. We use the antecedent constructs of the conventional IPC model, namely concerns about collection of personal data, unauthorized access to personal data, secondary use of personal data, errors in personal data, control over collection, and awareness about collection (Smith et al, 1996; Hong and Thong 2003) as

the elements of the treatment. We then use a post-test to examine the effects of the treatment on end-users' permissions consenting behavior. We anticipate a shift in their permission-granting disposition if indeed forewarning as a treatment has an impact on the end-user. Consequently, we hypothesize that:

Hypothesis 2a: Forewarning of end-users about permissions sought by a smart app (and associated information privacy implications) leads to a significant change in their behavior pertaining to granting/modifying privacy-related app-permissions. After forewarning, we anticipate end-users are significantly more attentive to the privacy-related app permissions sought by a smart app (and their associated information privacy implications) at the point of installation.

Hypothesis 2b: Forewarning of end users about permissions sought by a smart app and information privacy implications of such permissions leads to a significant change in their behavior pertaining to future use of smart-apps.

RESEARCH DESIGN AND METHODOLOGY

Survey-Based Instrumentation

This study employed a positivistic survey-based design consistent with most IPC studies (Hong & Thong, 2013; Bélanger & Crossler, 2011; Li, 2011; Smith, Dinev, & Xu, 2011; Dinev & Hart, 2004; Malhotra et al., 2004; Smith et al., 1996). However, the survey instrument was structured into three parts (see Appendix A). The first part contained a set of pre-treatment questions pertaining to the four measurement constructs: trusting beliefs, risk beliefs, use of social media apps, and granting of privacy-related app-permissions. Permissions-granting behavior and future use of smart-apps were the key dependent constructs. Trusting Beliefs and Risk Beliefs were implemented as control variables. Their purpose was to establish that the respondents in the sample reacted to the IPC model's constructs in line with prior published studies. Thereby validating the veracity, validity and dependability of the survey instrument.

The second part of the survey consisted of the treatment items. These items served the purpose of sensitizing the respondent to IPC concerns inherent in smart-apps and included the conventional IPC antecedents: collection of data; unauthorized secondary use; improper access to data; errors in data; control over collection and awareness about collection.

The third part of the survey instrument repeated the constructs initially contained in the first part of the survey, but this time these constructs served as post-treatment measured for those constructs. The only exception is the construct involving smart-app use intentionality which was structured to elicit responses about a subject's future use of smart-apps.

By structuring the survey instrument in this format, we achieved a classic Campbell and Stanley (1963) pre-test, treatment, post-test design. In this design, respondents provided us with their initial dispositions to smart-apps permissions-granting and reactions to IPC dependent constructs; then were exposed to a inattention treatment; and then their post-treatment smart-apps permissions-granting dispositions and IPC dependent-construct responses.

Half of the demographic questions were interlaced within the first part – the pre-test part – of the survey instrument, and the other half within the third part — the post-test part. This design was selected because the pre-test, treatment, post-test design lends itself well to testing of our propositions.

Data Collection

The instrument was administered as a web-based questionnaire in the United States, United Kingdom, and India and drew 1,017 respondents – 393, 331, and 293, respectively. Of these, 927 responses were deemed complete and useable – 372, 295, and 260, respectively. Consequently, the combined response rate was 91%; response rate by country was 95%, 89%, and 89%, respectively. The country response rates were comparable to the combined response rate of 91% for the entire dataset.

Table 1. Response rate by geographic region

Country	Total Responses	Valid Responses	Response Rate
USA	393	372	95%
UK	331	295	89%
India	293	260	89%
Total	1017	927	91%

Demographic Characteristics of Respondents

The demographic parameters that were collected from respondents were age, gender, and usage frequency of social media apps. The descriptive statistics and frequency distribution of respondents are provided in Table 2. About 90% of the respondents reported using social media apps at least once per week, with the clear majority (54%) indicating that they use them several times a day. An analysis of the distribution of respondents by age indicates that 55% of the respondents were between the ages of 25 and 45, 21% were between ages 45 and 65, 15% were between 18 and 25, and only 8% were older than 65 years of age. This observation is an indication that the study was successful at targeting individuals within the working age-range. Contrary to popular belief, Choudrie et al. (2020) found that older adults are open to adopting, using, and diffusing new technologies and propose a model of smartphone acceptance; future studies should investigate IPC concerns specifically with older adults. With respect to gender, the respondent pool was relatively balanced, with 54% female and 46% male.

We also sought to understand a priori experience and cognizance of respondents concerning information privacy. Therefore, we used three additional items to capture respondents' ratings of (a) how frequently they misrepresented their personal information when using smart-apps, (b) the degree to which they had been victims of data breaches, and (c) the extent of media exposure to information about smart-apps within the preceding one year.

Table 2. Demographic characteristics of respondents

Construct	Frequency Distribution		
	Category	Frequency	Percent
Gender	Female	498	53.7
	Male	429	46.3
Age	18-24	139	15
	25-34	288	31.1
	35-44	228	24.6
	45-54	103	11.1
	55-64	94	10.1
	65 or above	75	8.1
Mobile Apps Use Frequency	1 = every other week	94	10.1
	2 = once a week	62	6.7
	3 = every other day	95	10.2
	4 = once per day	170	18.3
	5 = many times per day	506	54.6

Results of this analysis are presented in Table 3. Of all respondents, only 11% reported that for the year preceding their participation in this study, they had not heard or read anything about information privacy concerning social media applications. Only 8% of the respondents reported never having falsified information when using social media apps. Concerning prior victimhood pertaining to use of social media app, 70% of the respondents reported having been victims in the past, while 30% reported never having been victims of an improper invasion of privacy. These observations indicate that privacy was a concern for a majority (at least 70%) of the respondents. Further, most of the respondents were cognizant of the concept of privacy as shown by their self-report where 89% had exposure to social media privacy and 92% engaged in some form of privacy-enhancing behavior by obfuscating or misrepresenting their personal information when using certain social media applications.

ANALYSIS OF DATA

The data collected from the respondents was analysed using SPSS (version 25). The four constructs used in this study were (a) privacy-related app-permissions, (b) intention to use social media, (c) trusting beliefs, and (d) risk beliefs. The first two constructs were used to assess change in individuals' privacy calculus when using smart-apps. The latter two were used as control variables to ascertain that the sample we used in this study was representative of, or consistent with, samples used in prior published IPC studies with respect to their reactions to the IPC model). Each construct had three measurement items. The measurement items were assessed to determine if subjects responded to the awareness-inattention treatment and whether the treatment influenced their post-treatment responses. Construct validation checks were performed with results, presented in Appendix B, revealing no concerns.

Given that the survey instrument was designed to collect a pre-treatment and a post-treatment score from each respondent on each of the four measurement variables, the statistical technique that we

Table 3. Respondents' reported dispositions to information privacy

Construct	Frequency Distribution		
	Category	Frequency	Percent
Exposure to Media about Information Privacy	1 = very much	231	24.9
	2 = much	185	20
	3 = some	286	30.9
	4 = not much	125	13.5
	5 = not at all	100	10.8
Prior Victimhood to Information Privacy Invasion	1 = Very frequently	90	9.7
	2 = frequent	111	12
	3 = a few times	214	23.1
	4 = very few times	229	24.7
	5 = Never	283	30.5
Misrepresentation of Personal Information	never falsified information	78	8.4
	under 25% of the time	83	9
	26% to 50% of the time	145	15.6
	51% to 75% of the time	145	15.6
	over 75% of the time	476	51.3

selected to use for data analysis is the paired samples comparison of means. Therefore, when analysing the study's set of hypotheses (H1a and H1b), we examined the mean difference in the respondents' responses relating to smart-app privacy-permissions. However, for the use construct, we aggregated the three pre-treatment items relating to use to obtain a homogeneous value and repeated the same for the three post-treatment items to obtain a homogeneous value for the future-use construct. We then assessed the difference in means of the use and future-use constructs. Results of this analysis are provided in section 6.

Because we collected data from three different regions of the world, prior to analysis, we sought to confirm if indeed the samples across the three countries could be combined into a single homogeneous sample. We also sought to examine if there were differences in responses based on the gender and on the age of a respondent. Hence, we conducted a MANOVA to examine the influences of the three categorical variables — country, gender, and age, on the respondents' reactions to the dependent variable items within the survey. Table 4 provides the results of this analysis.

By assessing the p-values for the Pillai's Trace and Wilks' Lambda scores for each of the three variables to see if any of them was less than 0.01, we found that responses to the survey were significantly statistically different by country, but not by gender or by age. Based on this, we treated the data collected as three separate samples – based on country. Hence, the hypothesis-testing is done independently for each country-group. We then contrast the observed results across the three groups to generalize our findings.

RESULTS FROM HYPOTHESIS TESTING

Assessment of Inattention (Operationalized as Duration) on Privacy-Permissions Dispositions and App-Future-Use Dispositions (H1)

Hypothesis H1a was tested by analyzing the causal effects of the duration that respondents took to complete the survey instrument on the respondents' reported post-test permissions-setting and

Table 4. Multivariate tests on effects of grouping variables on dependent variable

Effect		Value	F	Hypothesis df	Error df	Sig.	Partial ETA Squared	Observed Power
COUNTRY	Pillai's Trace	0.137	2.675	48.000	1740.000	0.000	0.069	1.000
	Wilks' Lambda	0.867	2.678[b]	48.000	1738.000	0.000	0.069	1.000
AGE	Pillai's Trace	0.166	1.245	120.000	4365.000	0.038	0.033	1.000
	Wilks' Lambda	0.844	1.253	120.000	4275.773	0.034	0.033	1.000
GENDER	Pillai's Trace	0.023	.864[b]	24.000	869.000	0.654	0.023	0.744
	Wilks' Lambda	0.977	.864[b]	24.000	869.000	0.654	0.023	0.744
COUNTRY * AGE	Pillai's Trace	0.273	1.026	240.000	8780.000	0.381	0.027	1.000
	Wilks' Lambda	0.757	1.026	240.000	8075.694	0.381	0.027	1.000
COUNTRY * GENDER	Pillai's Trace	0.048	0.884	48.000	1740.000	0.697	0.024	0.945
	Wilks' Lambda	0.953	.884[b]	48.000	1738.000	0.698	0.024	0.945
AGE * GENDER	Pillai's Trace	0.114	0.847	120.000	4365.000	0.884	0.023	0.999
	Wilks' Lambda	0.891	0.847	120.000	4275.773	0.883	0.023	0.999
COUNTRY * AGE * GENDER	Pillai's Trace	0.224	0.934	216.000	7893.000	0.746	0.025	1.000
	Wilks' Lambda	0.796	0.933	216.000	7370.624	0.750	0.025	1.000

future use dispositions. We use duration as a surrogate for inattention. The longer a subject takes to complete the survey, controlling for outliers, the greater the attention that individual is presumed to have paid to the task (which in this case is re assessment of their privacy calculus following exposure to potential information privacy concerns within the context of smart-app usage). Results obtained, are presented in table 5.

Analysis of the study's data (Table 5a) indicated that the total time that an individual spent on the information privacy questionnaire had an effect on the degree to which the individual adjusted his/her responses pertaining to privacy-related permissions granting behavior. However, it did not impact the extent to which an individual adjusted his/her judgements pertaining to continued use of smart applications. From a hypothesis perspective, H1a is supported but H1b is not. This is an interesting finding and we return to it in the discussion section of this paper.

We tested impacts of duration on the two control variables, trusting beliefs and risk beliefs, respectively. Prior individual privacy concerns and privacy calculus studies have established that individuals' attitudinal beliefs about privacy are relatively permanent and do not change from one encounter to another information (Hong and Thong, 2013; Choi et al, 2018; Goldfarb & Tucker, 2012; Mitrou et al., 2014). Therefore, we anticipated that the respondents would not register a change in their risk-beliefs or trusting beliefs post treatment. That is what we find in this study.

Analysis of the data collected in this study (Table 5b) indicated that there is no significant relationship between the duration of attention and trusting beliefs and risk beliefs. This indicates the degree of change in an individual's privacy dispositions, attitudinal beliefs about risk and trust of smart applications, is not affected by degree of attention or inattention to privacy-permissions and or potential information privacy concerns when installing a new smart-app. Indeed, the amount of time that an individual spent completing the survey (i.e. attention/ inattention to the study's treatment) did not have a direct bearing on the degree or extent to which they adjusted their responses.

Impact of Forewarning on Privacy-Enhancing Behavior (H2)

Hypothesis H2b was tested by analyzing the difference in means for the measurement items related to review of privacy-related app-permissions review (three measurements). The results of this analysis are presented in Tables 6a, 6b, and 6c. Pre-treatment responses, across all three samples showed a general disregard for privacy-related apps permissions. When their pre-treatment scores are contrasted to their post-treatment scores, it is evident that respondents in all three samples indicated a statistically significant change in their behavior pertaining to the review of privacy-related app-permissions. Consequently, hypothesis H2a is supported.

Table 5a. Impact of duration on permissions and app-usage dispositional measures

Construct	Measure	Impact of Duration (in Seconds) on Post-Test App-Privacy-Permissions-Dispositions and App-Usage in the Context of Social Media App Context					
		UK		India		USA	
		Regression Coefficient (B)	P-Value (2-tailed)	Regression Coefficient (B)	P-Value (2-tailed)	Regression Coefficient (B)	P-Value (2-tailed)
Review & Modification of Privacy Related App Permissions	Permissions 1	0.00011	0.183	-0.0005	**0.0002**	-0.00012	0.277
	Permissions 2	0.00032	**0.000**	0.0003	**0.0005**	0.00054	**0.000**
	Permissions 3	0.000104	**0.0997**	0.0003	**0.0007**	0.00056	**0.000**
Use of Social Media Apps	Aggregated Use	0.00015	0.339	0.0004	**0.0610**	0.00024	0.254

Table 5b. Impact of duration on privacy attitudinal beliefs measures

Construct	Measure	Impact of Duration (in Seconds) on Change in Respondents' Trusting and Risk Beliefs Concerning Information Privacy the Context of Social Media App Context					
		UK		India		USA	
		Regression Coefficient (B)	P-Value (2-tailed)	Regression Coefficient (B)	P-Value (2-tailed)	Regression Coefficient (B)	P-Value (2-tailed)
Trusting Beliefs	Trust 1	-0.000033	0.378	-0.00005	0.496	0.000075	0.252
	Trust 2	0.000058	0.159	-0.0001	0.149	-0.000005	0.935
	Trust 3	-0.00003	0.413	-0.00004	0.570	-0.00001	0.913
Risk Beliefs	Risk 1	-0.00002	0.664	0.00008	0.389	-0.00003	0.610
	Risk 2	-0.00003	0.455	0.00012	0.203	0.000087	0.153
	Risk 3	0.000068	0.142	0.00011	0.212	-0.000017	0.778

Table 6a. Paired samples statistics for UK: privacy calculus

Construct	Item	Measure	Mean (N=295)	Std. Dev.	Std. Error of Mean	Paired Differences					t-Value	P-Value (2-Tailed)
						Mean Difference (Pre-Post)	Std. Dev.	Std. Error of Mean	95% Confidence Interval of the Difference			
									Lower	Upper		
Review & Modification of Privacy Related App Permissions	Permissions 1	Pre	2.83	1.249	0.073	-0.132	1.584	0.092	-0.314	0.049	-1.433	0.153
		Post	2.97	1.091	0.063							
	Permissions 2	Pre	2.8	1.254	0.073	-0.698	1.31	0.076	-0.848	-0.548	-9.159	0
		Post	3.5	1.059	0.062							
	Permissions 3	Pre	3.44	1.132	0.066	-0.369	1.156	0.067	-0.502	-0.237	-5.491	0
		Post	3.81	0.962	0.056							
Use of Social media App	Aggregated Use	Pre	11.21	3.682	0.214	0.261	2.908	0.169			1.541	0.124
	Aggregated Future Use	Post	10.95	3.185	0.185							

Table 6b. Paired samples statistics for India: Privacy calculus

Construct	Item	Measure	Mean (N=295)	Std. Dev.	Std. Error of Mean	Paired Differences					t-Value	P-Value (2-Tailed)
						Mean Difference (Pre-Post)	Std. Dev.	Std. Error of Mean	95% Confidence Interval of the Difference			
									Lower	Upper		
Review & Modification of Privacy Related App Permissions	Permissions 1	Pre	3.77	1.085	0.067	0.623	1.617	0.1	0.426	0.821	6.214	0
		Post	3.14	1.201	0.074							
	Permissions 2	Pre	3.76	1.079	0.067	-0.223	1.141	0.071	-0.362	-0.084	-3.153	0.002
		Post	3.98	0.948	0.059							
	Permissions 3	Pre	3.79	0.949	0.059	-0.188	1.122	0.07	-0.325	-0.052	-2.71	0.007
		Post	3.98	0.93	0.058							
Use of Social media App	Aggregated Use	Pre	11.865	3.244	0.201	-0.381	3.279	0.203			-1.872	0.062
	Aggregated Future Use	Post	12.246	2.34	0.145							

Table 6c. Paired samples statistics for USA: Privacy enhancing behaviors

Construct	Item	Measure	Mean (N=295)	Std. Dev.	Std. Error of Mean	Paired Differences					t-Value	P-Value (2-Tailed)
						Mean Diff. (Pre-Post)	Std. Dev.	Std Error of Mean	95% Confidence Interval of the Difference			
									Lower	Upper		
Review & Modification of Privacy Related App Permissions	Permissions 1	Pre	3.27	1.24	0.064	0.228	1.656	0.086	0.06	0.397	2.661	0.008
		Post	3.05	1.104	0.057							
	Permissions 2	Pre	3.19	1.243	0.064	-0.535	1.07	0.055	-0.644	-0.426	-9.645	0
		Post	3.73	0.955	0.049							
	Permissions 3	Pre	3.37	1.139	0.059	-0.503	1.085	0.056	-0.613	-0.392	-8.933	0
		Post	3.88	0.912	0.047							
Use of Social media App	Aggregated Use	Pre	11.097	3.822	0.198	-0.233	3.22	0.167			-1.399	0.163
	Aggregated Future Use	Post	11.33	2.909	0.151							

Hypothesis H2b was also tested by analyzing the difference in means for the measurement items related to use of smart-apps (three measurements). Concerning use of smart-apps, respondents in the UK, India, and USA reflected mixed results, with statistically significant change being reflected in the aggregated usage measurement. Respondents in the UK demonstrate a marginal drop in their intention to continue using smart-apps in the future. However, those in the USA and India indicate a marginal uptake. Therefore, hypothesis H2b is not supported.

The analysis of the measurement items pertaining to the control constructs, trusting beliefs and risk beliefs (Tables 7a, 7b, and 7c), indicate that changes in these two measures were not statistically significant even after the treatment. While changes in the respondents' risk-belief and trusting beliefs appear to move in the hypothesized direction, they were not strong enough to register statistical significance.

Table 7a. Paired samples statistics for UK: Consumer attitudinal beliefs towards information privacy

Construct	Item	Measure	Mean (N=295)	Standard Deviation	Standard Error of Mean	Paired Differences					t-Value	P-Value (2-Tailed)
						Mean Difference (Pre-Post)	Standard Deviation	Standard Error of Mean	95% Confidence Interval of the Difference			
									Lower	Upper		
Trusting Beliefs	Trust 1	Pre	2.98	1.105	0.064	0.003	0.735	0.043	-0.081	0.088	0.079	0.937
		Post	2.98	1.066	0.062							
	Trust 2	Pre	2.89	1.139	0.066	-0.041	0.79	0.046	-0.131	0.05	-0.884	0.377
		Post	2.94	1.081	0.063							
	Trust 3	Pre	3.08	1.092	0.064	0.024	0.749	0.044	-0.062	0.11	0.544	0.587
		Post	3.06	1.032	0.06							
Risk Beliefs	Risk 1	Pre	3.63	0.956	0.056	0.058	0.918	0.053	-0.048	0.163	1.078	0.282
		Post	3.57	0.892	0.052							
	Risk 2	Pre	3.53	0.989	0.058	-0.044	0.966	0.056	-0.155	0.067	-0.783	0.434
		Post	3.57	0.919	0.053							
	Risk 3	Pre	3.52	0.958	0.056	-0.085	0.89	0.052	-0.187	0.017	-1.635	0.103
		Post	3.61	0.919	0.054							

Table 7b. Paired samples statistics for India: Consumer attitudinal beliefs towards information privacy

Construct	Item	Measure	Mean (N=260)	Standard Deviation	Standard Error of Mean	Paired Differences					t-Value	P-Value (2-Tailed)
						Mean Difference (Pre-Post)	Standard Deviation	Standard Error of Mean	95% Confidence Interval of the Difference			
									Lower	Upper		
Trusting Beliefs	Trust 1	Pre	3.77	1.002	0.062	0.073	0.962	0.06	-0.044	0.191	1.225	0.222
		Post	3.7	0.996	0.062							
	Trust 2	Pre	3.9	0.943	0.058	0.119	0.985	0.061	-0.001	0.24	1.952	0.052
		Post	3.78	0.936	0.058							
	Trust 3	Pre	3.77	1.018	0.063	0.035	1.011	0.063	-0.089	0.158	0.552	0.581
		Post	3.73	0.956	0.059							
Risk Beliefs	Risk 1	Pre	3.6	1.098	0.068	-0.077	1.16	0.072	-0.219	0.065	-1.069	0.286
		Post	3.68	1.029	0.064							
	Risk 2	Pre	3.48	1.11	0.069	-0.112	1.172	0.073	-0.255	0.032	-1.535	0.126
		Post	3.59	1.088	0.067							
	Risk 3	Pre	3.43	1.043	0.065	-0.115	1.112	0.069	-0.251	0.02	-1.672	0.096
		Post	3.55	1.091	0.068							

Table 7c. Paired samples statistics for USA: Consumer attitudinal beliefs towards information privacy

Construct	Item	Measure	Mean (N=372)	Standard Deviation	Standard Error of Mean	Paired Differences					t-Value	P-Value (2-Tailed)
						Mean Difference (Pre-Post)	Standard Deviation	Standard Error of Mean	95% Confidence Interval of the Difference			
									Lower	Upper		
Trusting Beliefs	Trust 1	Pre	2.98	1.189	0.062	-0.054	0.986	0.051	-0.154	0.047	-1.051	0.294
		Post	3.03	1.131	0.059							
	Trust 2	Pre	2.95	1.183	0.061	-0.005	0.853	0.044	-0.092	0.082	-0.122	0.903
		Post	2.96	1.153	0.06							
	Trust 3	Pre	3.1	1.11	0.058	0.022	0.846	0.044	-0.065	0.108	0.49	0.624
		Post	3.08	1.097	0.057							
Risk Beliefs	Risk 1	Pre	3.78	0.977	0.051	0.065	0.944	0.049	-0.032	0.161	1.318	0.188
		Post	3.72	0.998	0.052							
	Risk 2	Pre	3.62	1.003	0.052	-0.038	0.901	0.047	-0.13	0.054	-0.805	0.421
		Post	3.66	0.995	0.052							
	Risk 3	Pre	3.73	0.945	0.049	0.003	0.883	0.046	-0.087	0.093	0.059	0.953
		Post	3.73	0.954	0.049							

DISCUSSION

In this study, we sought to examine the effects of inattention and forewarning on an individual's privacy dispositions. We also sought to examine if inattention and forewarning impact an individual's decisions about using smart-apps and examined the individual's behavior pertaining to information-privacy-related app-permissions.

The findings of this study indicate that an individual's privacy dispositions are usually well established and unchanging across different contexts. This finding is in congruence with past findings

in the information privacy domain (Hong & Thong, 2013; Dinev et al., 2015) that have contributed to the definition of what is commonly referred to as the information-privacy paradox.

The study also finds that contemplation on privacy-related aspects of smart-apps, wrought about via forewarnings and the extent of attention paid to those forewarnings, does lead to a significant alteration in an individual's behaviors pertaining to permissions setting within smart-apps. What is interesting, however, is that an individual's judgements about use or continued use of smart-apps is not impacted by their contemplation of the privacy related aspects of the smart-apps. This finding indicates that practice of app builders to obfuscate privacy-policies and privacy-related permissions into hard-to-understand user-agreements or hard-to-access app-settings may be misinformed.

The study indicates that users seem to rely on their dispositional privacy which, as established in prior research, is unchanging when determining whether or not to use smart-apps. Hence, providers of smart-apps need not fear about losing potential consumers by making an app's privacy policies much more transparent to prospective and current customers.

However, designing smart-apps' user-interfaces, permissions-request interfaces, and privacy-related policy statements to be more transparent, understandable, and accessible by end users may endear the app to a wider market of consumers. For one, it will make for better judgements by end users about what privacy-related permissions to grant the app and which ones to withhold. This allows the app provider to obtain a more accurate sensing of consumer sentiments and preferences pertaining to their privacy, thereby providing higher-quality customization and or apps that better align with consumer preferences. This, in turn, enhances consumers' trust, which leads to greater loyalty or more transparency (e.g., greater self-disclosure, less provision of false information, etc.) from the end users as they transact with the smart-app.

In this regard, the results also provide insights into the management of smart-app use, at the individual-consumer level, within a corporation. That forewarning, and attention thereto, causes individuals to re-examine the permissions settings in a smart-app indicates that it could be a viable and effective strategy for user-driven smart-apps permissions management. Network managers could use this strategy to compel individual consumers to actively and consciously interrogate whether the current app-permission settings on the individual's personal computing device leverage the privacy of the individual's personal information as the individual attempts to connect the device onto a company's computer network or attempts to use the device to access corporate data and services.

One way of attaining this may be through an interactive panel that reveals to a consumer all the permissions settings for each smart-app hosted on his/her device and explains to the individual the inherent information privacy-loss or information privacy-damage that the consumer may suffer owing to each permission setting. The consumer then has the choice of altering the permission-setting or accepting it as is. In this way, responsibility to an individual's information privacy is ceded from the corporation to the consumer. Network managers may still have the power to override certain app-permission settings, should they deem those as compromising other aspects of the organization's information security or the privacy of other individuals' personal information. In this way, companies can mitigate exposures to privacy loss as well as other data-security breaches, when they allow individuals to connect non-corporate-owned devices to the company's networks.

The results also present innovative questions that warrant investigation in future studies. First, the support for forewarning and duration of attention thereto on the study's outcomes, especially on individuals' behavioral reactions to privacy-permissions-settings within smart apps, suggests that the use of elaborate training regimens, be they long-term or short-tern in duration, may not necessarily be the most cost-effective strategy or policy consideration for leveraging individuals' self-driven information-privacy management. This study shows that merely getting individuals to consciously consider privacy alters their privacy enhancing behavior. Consequently, these findings suggest that embedding even short-bursts or micro-instances of cognitive-contemplation within smart-app-enabled or smart-app supported business-processes may be just as effective a strategy for leveraging user-driven information privacy maximization, as formal training. We note, however, that the scope of

this study did not allow us to test this proposition. Therefore, we see this as one question that future work in this area could address.

Second, the lack of support for effects of inattention and/or forewarning on trusting beliefs and risk beliefs raises several interesting issues that are worth investigating in future research. This is magnified because high-impact IT-enabled privacy management solutions are in dire need. Understanding of how to effectively manage privacy in today's highly-interconnected computational eco-systems remains a critical issue of concern among IT scholars. Future research should focus on confirming if these are indeed nonissues or whether mechanisms exist that can alter or shape individuals' trusting and risk beliefs, since these may be fundamental to how individuals perceive and treat privacy-issues, both within corporate-work settings and private/personal settings.

LIMITATIONS

We acknowledge that this study is not all-encompassing and we thus document some of its limitations. The first is that we employ self-reported data and assume that this data realistically measure the constructs we use in this study. The design and context of the study made it difficult to assess each construct with real measurement data. Constructs such as trust and risk beliefs are hard to assess using direct measurement. If we were to use a direct measurement approach, it would take a very long time to collect data for constructs such as terms of use, like changes made to app-permissions. It would also necessitate that we construct a real-life treatment-app, thereby introducing additional complexities of controlling for an untold number of extenuating circumstances and other potential factors that have a bearing on a user's decision to change the default settings of the treatment-app. As we were not able to use actual or direct-measurement data, a future study designed to capture such data would be welcome.

This study is also limited to a single data collection context and used social media as the exemplar of smart-app technology. Therefore, the findings we obtain need validation by replicating this study in other contexts and potentially using other types of smart-app technologies as exemplars. We also recognize that while we collected data from three countries—USA, UK and India—these are countries that rank relatively highly in information technology competence and the intensity of diffusion of their digital societies. Therefore, as future studies seek to validate our findings, it would be good to see replications of this study in economies that do not rank highly in information technology competence or maturity of digital societies.

Despite these limitations, we see the results as providing room for the incorporation and empirical evaluation of additional constructs into the model. This allows assessing their justifications and relevance to information privacy and smart-app contexts, such as IoT, artificial intelligence, and Big data. The research illuminates the interplay and the influences of forewarning and individuals' attitudinal beliefs as well as behavioral reactions of individuals with respect to information privacy in the era of smart-apps. In so doing, it adds richness to our current understanding of information privacy at the individual level and potential strategies for leveraging and managing such privacy effectively.

CONCLUSION

This study examined the notion of information-privacy at the point of contact between an individual consumer and the smart-apps the end user employs. We assessed the impacts of inattention and forewarning on consumers' trust and perceived risks inherent in smart-apps. We also evaluated consumers' behavioral reactions to the perceived smart-app privacy concerns. The study's results revealed that while forewarning does not alter individuals' attitudinal beliefs, its effects on consumers' behavioral reactions, especially pertaining to a re-examination and revision of an app's default permissions settings, is significant.

Indeed, this study contributes to the efforts aimed at leveraging the management of information privacy, especially as it pertains to individuals' personal data. For one, it provides some credence to the notion that designing smart-apps' user-interfaces, permissions-request interfaces, and privacy-related policy statements to be more transparent, understandable, and accessible by end users. This may endear smart-apps to a wider market of consumers. Further, while consumers may be set in their trusting and risk beliefs pertaining to smart-apps, transparent interfaces and micro-processes that allow then to transparently contemplate impacts of app-settings on the privacy of their personal information may be sufficient in getting the consumers to optimize those settings for maximal personal information privacy.

DISCLOSURE STATEMENT

No potential conflict of interest was reported by any of the coauthors.

REFERENCES

Ackerman, M., & Mainwaring, S. (2005). Privacy issues and human-computer interaction. *Computer*, *27*(5), 19–26.

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, *347*(6221), 509–514. doi:10.1126/science.aaa1465 PMID:25635091

Alani, M. (2017). Android users privacy awareness survey. *International Journal of Interactive Mobile Technologies*, *11*(3), 130–144. doi:10.3991/ijim.v11i3.6605

Alepis, E., & Patsakis, C. (2017). There's Wally! Location tracking in Android without permissions. In *Proceedings of the 3rd International Conference on Information Systems Security and Privacy (ICISSP 2017),* (pp. 278-284). ScitePress.. . doi:10.5220/0006125502780284

Ameen, N., Tarhini, A., Shah, M. H., Madichie, N., Paul, J., & Choudrie, J. (2021). Keeping customers' data secure: A cross-cultural study of cybersecurity compliance among the Gen-Mobile workforce. *Computers in Human Behavior*, *114*, 106531. doi:10.1016/j.chb.2020.106531

Angst, C., & Agarwal, R. (2009). Adoption of electronic health records in the presence of privacy concerns: The elaboration likelihood model and individual persuasion. *Management Information Systems Quarterly*, *33*(2), 339–370. doi:10.2307/20650295

Apsler, R., & Sears, D. O. (1968). Warning, personal involvement, and attitude change. *Journal of Personality and Social Psychology, 9*(2p1), 162.

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. *Management Information Systems Quarterly*, *35*(4), 1017–1042. Retrieved January 12, 2021, from. doi:10.2307/41409971

Brennan, M., & Lovells, H. (2016). Mobile app privacy considerations. *Lexis Practice Advisor Journal*. https://www.lexisnexis.com/lexis-practice-advisor/the-journal/b/lpa/archive/2016/11/08/mobile-app-privacy-considerations.aspxCarpenter.

Burek, B., & Martinussen, R. (2021). The Relationship between Behavioral Inattention, Meta-Attention, and Graduate Students' Online Information Seeking. *Mind, Brain and Education : the Official Journal of the International Mind, Brain, and Education Society*, *15*(1), 111–121. doi:10.1111/mbe.12270

Chan, E. Y., & Saqib, N. U. (2021). Privacy concerns can explain unwillingness to download and use contact tracing apps when COVID-19 concerns are high. *Computers in Human Behavior*, *119*, 106718. doi:10.1016/j.chb.2021.106718 PMID:33526957

Chen, R. (2013). Living a private life in public social networks: An exploration of member self-disclosure. *Decision Support Systems*, *55*(3), 661–668. doi:10.1016/j.dss.2012.12.003

Chike-Obuekwe, C., Choudrie, J., Nwanekezie, D., Sundaram, D., & Peko, G. (2020, January). Investigating the Use, Adoption and Diffusion of Online Social Network Adoption (Facebook vs Twitter), within the Older Adult Population (50+) in Hertfordshire UK. In *Proceedings of the 53rd Hawaii International Conference on System Sciences.* doi:10.24251/HICSS.2020.546

Choi, B., Wu, Y., Yu, J., & Land, L. (2018). Love at first sight: The interplay between privacy dispositions and privacy calculus in online social connectivity management. *Journal of the Association for Information Systems*, *19*(3), 124–151. doi:10.17705/1jais.00487

Choi, B. C., Jiang, Z., Xiao, B., & Kim, S. (2015). Embarrassing exposures in online social networks: An integrated perspective of privacy invasion and relationship bonding. *Information Systems Research*, *26*(4), 675–694. doi:10.1287/isre.2015.0602

Choudrie, J., Pheeraphuttranghkoon, S., & Davari, S. (2020). The digital divide and older adult population adoption, use and diffusion of mobile phones: A quantitative study. *Information Systems Frontiers*, *22*(3), 673–695. doi:10.1007/s10796-018-9875-2

Daiku, Y., Kugihara, N., Teraguchi, T., & Watamura, E. (2020). Effective forewarning requires central route processing: Theoretical improvements on the counter argumentation hypothesis and practical implications for scam prevention. *PLoS One*, *15*(3), e0229833. doi:10.1371/journal.pone.0229833 PMID:32134968

Dienlin, T., & Metzger, M. J. (2016). An extended privacy calculus model for SNSs: Analyzing self-disclosure and self-withdrawal in a representative US sample. *Journal of Computer-Mediated Communication*, *21*(5), 368–383. doi:10.1111/jcc4.12163

Dinev, T. (2014). Why would we care about privacy? *European Journal of Information Systems*, *23*(2), 97–102. doi:10.1057/ejis.2014.1

Dinev, T., & Hart, P. (2004). Internet privacy concerns and their antecedents: Measurement validity and a regression model. *Behaviour & Information Technology*, *23*(6), 413–422. doi:10.1080/01449290410001715723

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, *17*(1), 61–80. doi:10.1287/isre.1060.0080

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. . 10.1287/isre.2015.0600

Einav, L., Farronato, C., & Levin, J. (2015). Peer-to-peer markets. *Annual Review of Economics*, *8*(1), 615–635. doi:10.1146/annurev-economics-080315-015334

Fox, G., Clohessy, T., van der Werff, L., Rosati, P., & Lynn, T. (2021). Exploring the competing influences of privacy concerns and positive beliefs on citizen acceptance of contact tracing mobile applications. *Computers in Human Behavior*, *121*, 106806. doi:10.1016/j.chb.2021.106806

FTC. (2014, February 19). *Spring privacy series: Mobile device tracking. Federal Trade Commission: Protecting America's consumers*. FTC. https://www.ftc.gov/news-events/events-calendar/2014/02/spring-privacy-series-mobile-device-tracking

Future Sight. (2011). *User perspectives on mobile privacy: Summary of research findings*. Future Sight. https://www.gsma.com/publicpolicy/wp-content/uploads/2012/03/futuresightuserperspectivesonuserprivacy.pdf 10.1257/aer.102.3.349

Goldfarb, B. A., & Tucker, C. (2012). Shifts in privacy concerns. *American Economic Review, 102*(3), 349-353. <ALIGNMENT.qj></ALIGNMENT>10.1257/aer.102.3.349

Georgiev, G. (2021). *43+ Stunning BYOD Stats and Facts to Know in 2021*. Tech Jury. https://techjury.net/blog/byod/#gref

Grossenbacher, P. G., & Quaglia, J. T. (2017). Contemplative cognition: A more integrative framework for advancing mindfulness and meditation research. *Mindfulness*, *8*(6), 1580–1593. doi:10.1007/s12671-017-0730-1

Hong, W., & Thong, J. (2013). Internet privacy concerns: An integrated conceptualization and four empirical studies. *Management Information Systems Quarterly*, *37*(1), 275–298. doi:10.25300/MISQ/2013/37.1.12

Hui, K. L., Teo, H. H., & Lee, S.-Y. T. (2007). The value of privacy assurance: An exploratory field experiment. *Management Information Systems Quarterly*, *31*(1), 19–33. doi:10.2307/25148779

Jiang, Z., Heng, C. S., & Choi, B. C. (2013). Privacy concerns and privacy-protective behavior in synchronous online social interactions. *Information Systems Research*, *24*(3), 579–595. doi:10.1287/isre.1120.0441

Krasnova, H., Günther, O., Spiekermann, S., & Koroleva, K. (2009). Privacy concerns and identity in online social networks. *Identity in the Information Society*, *2*(1), 39–63. doi:10.1007/s12394-009-0019-1

Luo, X., Li, H., Zhang, J., & Shim, J. P. (2010). Examining multi-dimensional trust and multifaceted risk in initial acceptance of emerging technologies: An empirical study of mobile banking services. *Decision Support Systems*, *49*(2), 222–234. doi:10.1016/j.dss.2010.02.008

Lutz, C., Hoffmann, C. P., Bucher, E., & Fieseler, C. (2018). The role of privacy concerns in the sharing economy. *Information Communication and Society*, *21*(10), 1472–1492. Retrieved March 26, 2022, from. doi:10.1080/1369118X.2017.1339726

Mackowiak, B., Matejka, F., & Wiederholt, M. (2021). *Rational inattention: A review*. 10.2866/417246

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. doi:10.1287/isre.1040.0032

Marreiros, H., Tonin, M., Vlassopoulos, M., & Schraefel, M. C. (2017). "Now that you mention it": A survey experiment on information, inattention and online privacy. *Journal of Economic Behavior & Organization*, *140*, 1–17. doi:10.1016/j.jebo.2017.03.024

Matveenko, A., & Starkov, E. (2021). *Sparking Curiosity or Tipping the Scales? Targeted Advertising to Rationally Inattentive Consumers.* Academic Press.

Metzger, M. J. (2004). Privacy, trust, and disclosure: Exploring barriers to electronic commerce. *Journal of Computer-Mediated Communication*, *9*(4). Advance online publication. doi:10.1111/j.1083-6101.2004.tb00292.x

Mitrou, L., Kandias, M., Stavrou, V., & Gritzalis, D. (2014). Social media profiling: A Panopticon or Omniopticon tool? In *Proceedings of the 6th Conference of the Surveillance Studies Network* (pp. 1-15). Academic Press.

Nayak, R. D., & Padmashali, A. Prevalence of Inattention among School Children with Excessive Smart Phone Use. *International Journal of Humanities and Social Science Invention*. www.ijhssi.org

Neimeyer, G. J., MacNair, R., Metzler, A. E., & Courchaine, K. (1991). Changing personal beliefs: Effects of forewarning, argument quality, prior bias, and personal exploration. *Journal of Social and Clinical Psychology*, *10*(1), 1–20. doi:10.1521/jscp.1991.10.1.1

O'Connor, A. M., Judges, R. A., Lee, K., & Evans, A. D. (2021). Can adults discriminate between fraudulent and legitimate e-mails? Examining the role of age and prior fraud experience. *Journal of Elder Abuse & Neglect*, *33*(3), 1–25. doi:10.1080/08946566.2021.1934767 PMID:34134594

Oliveira, S., & Zaïane, O. (2002). Privacy preserving frequent itemset mining. In *Proceedings of the IEEE ICDM Workshop on Privacy, Security, and Data Mining* (pp. 43-54). IEEE.

Onanuga, A. (2020). *BYOD Adoption: What are the concerns, how can they be mitigated and what does the future hold?* Retrieved from https://www.linkedin.com/pulse/byod-adoption-what-concerns-how-can-mitigated-does-future-onanuga

Posey, C., & Ellis, S. (2007). Understanding self-disclosure in electronic communities: An exploratory model of privacy risk beliefs, reciprocity, and trust. *AMICS 2007 Proceedings*, 1-11.

Prabhakar, S., Pankanti, S., & Jain, A. (2003). Biometric recognition: Security and privacy concerns. *IEEE Security and Privacy*, *99*(2), 33–42. doi:10.1109/MSECP.2003.1193209

Proserpio, D., Xu, W., & Zervas, G. (2016). You get what you give: Theory and evidence of reciprocity in the sharing economy. *Quantitative Marketing and Economics Conference Proceedings*, 1-46. doi:10.2139/ssrn.3203144

Rath, D. K., & Kumar, A. (2021). *Information privacy concern at individual, group, organization and societal level-a literature review*. Vilakshan-XIMB Journal of Management. doi:10.1108/XJM-08-2020-0096

Scheibe, S., Notthoff, N., Menkin, J., Ross, L., Shadel, D., Deevy, M., & Carstensen, L. L. (2014). Forewarning reduces fraud susceptibility in vulnerable consumers. *Basic and Applied Social Psychology*, *36*(3), 272–279. doi:10.1080/01973533.2014.903844 PMID:25328263

Scutti, S. (2017, March 22). *The psychology of privacy in the era of the Internet of Things*. Retrieved from https://www.cnn.com/2017/03/22/health/psychology-privacy-wikileaks-internet-of-things/index.html

Smallwood, J., & Schooler, J. W. (2015). The science of mind wandering: Empirically navigating the stream of consciousness. *Annual Review of Psychology*, *66*(1), 487–518. doi:10.1146/annurev-psych-010814-015331 PMID:25293689

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *Management Information Systems Quarterly*, *35*(4), 989–1016. doi:10.2307/41409970

Smith, H. J., Milberg, H. S., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *Management Information Systems Quarterly*, *20*(2), 167–196. Retrieved May 8, 2021, from. doi:10.2307/249477

Stutzman, F., & Kramer-Duffield, J. (2010). Friends only: Examining a privacy-enhancing behavior in Facebook. *CHI Proceedings*, 1553-1562. doi:10.1145/1753326.1753559

Sun, Y., Wang, N., Shen, X.-L., & Zhang, J. X. (2015). Location information disclosure in location-based social network services: Privacy calculus, benefit structure, and gender differences. *Computers in Human Behavior*, *52*, 278–292. doi:10.1016/j.chb.2015.06.006

Sundfør, H. B., Sagberg, F., & Høye, A. (2019). Inattention and distraction in fatal road crashes–Results from in-depth crash investigations in Norway. *Accident; Analysis and Prevention*, *125*, 152–157. doi:10.1016/j.aap.2019.02.004 PMID:30763812

Sutanto, J., Palm, E., Tan, C., & Phang, C. (2013). Addressing the personalization–privacy paradox: An empirical assessment from a field experiment on smartphone users. *Management Information Systems Quarterly*, *37*(4), 1141–1164. doi:10.25300/MISQ/2013/37.4.07

Teubner, T., & Flath, C. (2019). Privacy in the sharing economy. *Journal of the Association for Information Systems*, *20*(3), 213–242. doi:10.17705/1jais.00534

Xu, H., Dinev, T., Smith, J., & Hart, P. (2011). Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems*, *12*(12), 798–824. doi:10.17705/1jais.00281

Xu, H., Teo, H. H., Tan, B. C. Y., & Agarwal, R. (2010). The role of push-pull technology in privacy calculus: The case of location-based services. *Journal of Management Information Systems*, *26*(3), 135–174. doi:10.2753/MIS0742-1222260305

Xu, H., Teo, H. H., Tan, B. C. Y., & Agarwal, R. (2012). Effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: A study of location-based services. *Information Systems Research, 23*(4), 1342-1363. 10.1287/isre.1120.0416

Young, D. K., Barrett, P., & McLeod, A. J. (2019). Refining technology threat avoidance theory. *Communications of the Association for Information Systems, 44*. 10.17705/1CAIS.04422

Zheng, F., Gao, P., He, M., Li, M., Wang, C., Zeng, Q., Zhou, Z., Yu, Z., & Zhang, L. (2014). Association between mobile phone use and inattention in 7102 Chinese adolescents: A population-based cross-sectional study. *BMC Public Health*, *14*(1), 1–7. doi:10.1186/1471-2458-14-1022 PMID:25273315

APPENDIX A

Survey Instrument

Table 8. Demographics variables

COUNTRY	Please indicate your country/region: - Other (Please specify) - Text
GENDER	Please indicate your gender:
AGE	Please indicate your age group:

Table 9. Pre-treatment survey items

Please indicate your agreement/disagreement level about the following statements by selecting from the 5-point Strongly Disagree to Strongly Agree scale.	
PRMS1a	I read the apps Terms and Permissions whenever I am downloading social media apps.
PRMS2a	I review the apps Terms and Permissions whenever I am updating social media apps.
PRMS3a	I change the apps default permissions, where necessary, whenever I am downloading social media apps.
RISK1a	In general, it would be risky to give information about me to social media apps.
RISK2a	There would be high potential for loss associated with giving information about me to social media apps.
RISK3a	There would be too much uncertainty associated with giving information about me to social media apps.
TRUS1a	Social media apps, in general, would be trustworthy in handling information about me.
TRUS2a	Social media apps would keep my best interests in mind when dealing with information about me.
TRUS3a	Social media apps would fulfill their promises related to information about me.
USE1	Actual use of social media apps (e.g. Facebook, Twitter, Instagram): - I use social media apps frequently.
USE2	Actual use of social media apps (e.g. Facebook, Twitter, Instagram): - I use social media apps regularly.
USE3	Actual use of social media apps (e.g. Facebook, Twitter, Instagram): - I use social media apps routinely.
PPE -MISR	Some social media apps (e.g. Facebook, Twitter, Instagram) ask for you to register with the site by providing your information. When asked for such information, what percent of the time do you falsify the information?
PPE-VICT	How frequently have you personally been the victim of what you felt was an improper invasion of privacy? (1=Very frequently and 5=Never)
PPE-MEDI	How much have you heard or read during the last year about the use and potential misuse of the information collected from Apps? (1 = very much; 5 = not at all)

Table 10. Post treatment survey items

Please indicate your agreement/disagreement level about the following statements by selecting from the 5-point Strongly Disagree to Strongly Agree scale.	
PRMS1b	In the future, I intend to read the apps Terms and Permissions whenever I am downloading social media apps.
PRMS2b	In the future, I intend to review the apps Terms and Permissions whenever I am updating social media apps.
PRMS3b	In the future, I intend to change the apps default permissions, where necessary, whenever I am downloading social media apps.
RISK1b	In general, it would be risky to give information about me to social media apps.
RISK2b	There would be high potential for loss associated with giving information about me to social media apps.

continued on following page

Table 10. Continued

RISK3b	There would be too much uncertainty associated with giving information about me to social media apps.
TRUS1b	Social media apps, in general, would be trustworthy in handling information about me.
TRUS2b	Social media apps would keep my best interests in mind when dealing with information about me.
TRUS3b	Social media apps would fulfill their promises related to information about me.
FUSE1	I plan to continue using social media apps in the future.
FUSE2	I intend to continue using social media apps in the future.
FUSE3	I expect to continue using social media apps in the future.

APPENDIX B

Construct Validity of Survey Instruments

Table 11. Items used on the survey instrument to induce/conjure treatment effect

Please indicate the degree to which you agree or disagree with the following statements by selecting from the 5-point Strongly Disagree to Strongly Agree scale.	
item 1	It bothers me that social media apps may be collecting some information about me that is unknown to me.
item 2	It bothers me that collection of information about me by social media apps is perpetual (never-ending).
item 3	I am concerned that collection of information about me by social media apps is pervasive.
item 4	I am concerned about the multifaceted (multi-dimensional) ways in which social media apps can collect information about me.
item 5	I am concerned that social media apps would enable data brokers to aggregate information about me.
item 6	I am concerned that social media apps would enable advertisers to send me unsolicited intrusive promotions based on information about me.
item 7	I am concerned that social media apps would enable service providers (e.g. Insurance companies) to deny me certain services based on the information about me.
item 8	I am concerned that social media apps would share information about me with other companies without my authorization.
item 9	I am concerned that social media apps do not allow me to personally correct the errors in information about me.
item 10	I am concerned social media apps have never-ending access to features on my device including contact list, location, and camera.
item 11	I am concerned social media apps have pervasive access to features on my device including contact list, location, and camera.
item 12	I am concerned about the non-transparent ways in which social media apps access the features on my device including contact list, location, and camera.
item 13	I am concerned about the multifaceted ways in which social media apps access the features such as contact list, location, media, camera, microphone etc.
item 14	It bothers me that access to features such as contact list, location, media, camera, microphone etc. by social media apps is not transparent.
item 15	It bothers me that the way others see me is no longer based on my own discretion, my own will, or my own choice because of social media apps.
item 16	It bothers me that I no longer have control over how others perceive me because of social media apps.
item 17	It bothers me that control over my autonomy and self-determination is diminishing because of social media apps.
item 18	I am concerned when control over my anonymity is lost or unwillingly reduced as a result of using social media apps.
item 19	I am concerned that social media apps monitor my every activity, task, or location.

continued on following page

Table 11. Continued

item 20	I am concerned that social media apps keep an eye on my every activity, task, or location.
item 21	I am concerned when control over my reputation is lost or unwillingly reduced as a result of information about me contained in social media apps.
item 22	It usually bothers me when social media apps seek for my consent by using hard-to-understand language.
item 23	It usually bothers me when social media apps hide consent statements inside large documents such as Terms and Conditions.
item 24	It usually bothers me when social media apps deny downloading when I opt to alter how the app should collect, use, and share information about me.
item 25	It usually bothers me when I am not aware of whether social media apps could potentially access or collect other types of information about me in the future.

Table 12. Construct Validity of Survey Instruments

Dimension / Construct	UK			USA			India		
	Cronbach's Alpha	Composite Reliability	AVE	Cronbach's Alpha	Composite Reliability	AVE	Cronbach's Alpha	Composite Reliability	AVE
Collection	0.814	0.89	0.729	0.833	0.9	0.75	0.83	0.898	0.746
Secondary Use	0.927	0.954	0.873	0.892	0.933	0.823	0.872	0.921	0.796
Errors In Data	0.909	0.943	0.846	0.903	0.939	0.838	0.862	0.916	0.784
Unauthorized Access	0.909	0.943	0.847	0.897	0.936	0.829	0.894	0.934	0.826
Control	0.888	0.93	0.817	0.88	0.926	0.807	0.846	0.907	0.765
Awareness	0.87	0.92	0.794	0.885	0.929	0.813	0.84	0.904	0.758
Information Management	0.927	0.943	0.732	0.928	0.943	0.735	0.897	0.921	0.661
Interaction Management	0.941	0.951	0.683	0.941	0.95	0.679	0.91	0.926	0.581
Information Privacy Concerns	0.964	0.967	0.664	0.962	0.966	0.652	0.943	0.95	0.559
Trusting Beliefs	0.927	0.953	0.871	0.931	0.956	0.877	0.865	0.914	0.78
Risk Beliefs	0.846	0.906	0.763	0.858	0.914	0.779	0.892	0.933	0.822
Permissions Behavior	0.817	0.89	0.73	0.773	0.834	0.628	0.845	0.859	0.673
Use	0.885	0.923	0.8	0.909	0.797	0.58	0.919	0.931	0.819
Future Continued Use	0.952	0.914	0.783	0.944	0.963	0.898	0.851	0.908	0.768

Table 13. Demographic variables

COUNTRY	Please indicate your country/region: - Other (Please specify) - Text
GENDER	Please indicate your gender:
AGE	Please indicate your age group:

Solomon Negash is a Professor of Information Systems at Kennesaw State University. He has over 2900 citations at Google Scholar index and serves as editor-in-chief of the African Journal of Information Systems. His publications have appeared in journals including IM, ITD, JGIM, CACM, and CAIS. He championed and served as founding international coordinator of the Information Systems PhD program at Addis Ababa University IT Doctoral program in Ethiopia. He has served as member and chair of a doctoral committee at three institutions. He is a certified Project Management Professional (PMP) with 20 years each in industry and academia.

Peter Meso is a Professor of Information Systems and Business Analytics at the Lutgert College of Business, Florida Gulf Coast University. His current research interests are in the behavioral and managerial interactions of people and information technology particularly as they relate to the design and development of information systems; IS data management and strategy; and, information analytics. He has over 70 publications in scholarly outlets such as the Information Systems Research journal, Journal of the AIS, European Journal of Information Systems, Information Systems Journal, Requirements Engineering, Journal of the American Society for Information Sciences and Technology, various IEEE Transactions, Journal of Global Information Management, Information Technology for Development and various conference proceedings. Dr. Meso holds a Ph.D. in Management Information Systems from Kent State University and a Master of Business Administration Degree from the United States International University – Africa.

Philip F. Musa is a Professor of Information Systems and Management at The Univ. of Alabama at Birmingham. His research tends to be on the intersections of Information Technology in Developing Countries, Public Health, and Management. He has published in JGIM, EJIS, CAIS, EJISDC, ISJ, ITD, JPHMP, JOMS, CAIS, BMC Public Health, IJOQM, CACM, JISE, etc. He has also served as program manager, track/mini track chair of various IS conferences and published in proceedings of major IS conferences. He serves on Editorial Boards of some major IS and Healthcare Journals. Dr. Musa has served on PhD Dissertation committees as a member and as Chair. He has also served as External reviewer or opponent for PhD candidates at other universities such as University of the West Indies in Jamaica and Stockholm University/Royal Institute of Technology in Sweden.