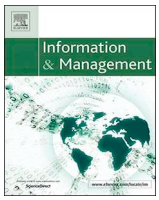
Information & Management 58 (2021) 103284

Contents lists available at ScienceDirect

Information & Management

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



The effect of Fair information practices and data collection methods on privacy-related behaviors: A study of Mobile apps

Christian Fernando Libaque-Sáenz[a], Siew Fan Wong[b], Younghoon Chang[c,*], Edgardo R. Bravo[a]

[a] Engineering Department, Universidad del Pacifico, Av. Salaverry # 2020, Jesus Maria, Lima, Peru
[b] Department of Computing and Information Systems, Sunway University, 5, Jalan Universiti, Bandar Sunway, 47500, Selangor, Malaysia
[c] School of Management and Economics, Beijing Institute of Technology, 5 South Zhongguancun Street, Haidian District, Beijing, 100081, PR China

ARTICLE INFO

Keywords:
Fair information practices
Control-risk
Information privacy
Privacy concerns
mobile apps
Data collection methods

ABSTRACT

To capitalize on valuable consumer and transactional data on mobile apps, companies should employ ethical decisions and strategies that can reduce privacy concerns, because such concerns present critical challenges for corporate social responsibility. In this study, we tested the effect of intervention strategies, Fair Information Practices, and the data collection method on privacy-related decisions. The results show that both intervention strategies have a significant effect on perceived data control and perceived risks and in turn on behavioral intention. Our findings have novel theoretical and managerial implications to those who want to promote ethical business practices in the mobile apps industry.

1. Introduction

The increasing affordability and features of mobile devices and mobile apps have enabled companies to collect huge amounts of user data [1–3]. In particular, cookies and GPS, along with consumers' transactional data, allow companies to track user preference, and provide accurate location-based prediction and recommendations [4]. When processed effectively and innovatively, consumer data supply actionable real-time information to improve operations, facilitate innovation, optimize resource allocation, reduce costs, and enhance decision-making [4,5]. The recent big data analytics capabilities and tools further accentuate potential benefits companies could gain from having access to a large amount of consumer data [4].

While companies could capitalize on consumer data to improve market advantage, privacy concerns stand as the biggest roadblock to monetizing these data [3,6]. The concerns also present critical challenges for ethical business practices [3,6]. Specifically, consumers are concerned about how their personal data will be processed, stored, shared, and used [7]. They are also worried about the vulnerabilities of mobile technologies that lead to potential data leakages, hacking, and data thefts [7]. All these concerns may stop consumers from using mobile apps. As the success of mobile apps depends on the usage rate [8,9], a low adoption rate is a loss to companies considering that the size of the mobile apps market is one of the biggest within the IT sector. Its total market revenue for 2016 was 76.5 billion dollars, and the figure is expected to grow to 101 billion dollars in 2020 [10]. Therefore, companies ought to strategize on how to reduce consumers' privacy concerns, so as to increase the consumption rate and present a better corporate image [11]. In this paper, we tested the effect of two company intervention strategies, Fair Information Practices (FIPs) and the data collection method, on privacy-related decisions linked to the use of mobile apps. These intervention strategies are framed using the control-risk literature, which gives our research model a strong theoretical foundation [12,13].

We contended that using FIPs to instill consumer confidence toward a company's data management practices is a good strategy. The privacy literature posits that FIPs have a regulatory endorsement effect, which conveys the perception of "fairness" [14,15]. Companies could utilize the power of FIPs to shape positive perception toward their data management practices. Existing FIP studies have examined various aspects including origin [16], challenges in the implementation process [12,17,18], companies' compliance [12,16–21], perceptions [6,22,23], and enforcement [24–27]. From a further inspection of Appendix A, which covers studies on FIPs or closely related variables, most of them focused on fixed platforms or general scenarios, while only five focused on mobile technologies. Following are the few studies on fixed platforms or general scenarios that used experimental research. Culnan and Armstrong [14] conducted a preexperimental study with secondary data. However, data were captured from secondary sources, there was no control group, and the research items were proxy measures of

* Corresponding author.
E-mail addresses: cf.libaques@up.edu.pe (C.F. Libaque-Sáenz), siewfanw@sunway.edu.my (S.F. Wong), younghoonchang@bit.edu.cn (Y. Chang), er.bravoo@up.edu.pe (E.R. Bravo).

https://doi.org/10.1016/j.im.2020.103284
Received 16 February 2018; Received in revised form 13 February 2020; Accepted 16 February 2020
Available online 17 February 2020
0378-7206/

privacy concerns and other related variables. Therefore, the results should be interpreted with caution. Nemati and Van Dyke [27] conducted a quasi-experimental research using *t*-test and ANOVA techniques. However, the results showed a nonsignificant effect of FIPs on trust and risk perception (the study did not include behavioral intention). Liu, Marchewka, Lu and Yu [28] conducted an experimental study on the effect of FIPs on trust and behavioral intention. However, they only included two scenarios: FIPs and non-FIPs (they did not study interaction with other factors). To fully understand the power of FIPs, it is necessary to assess their effectiveness in various situations. Other studies that focused on fixed platforms are either descriptive in nature [12,16,18–20] or do not consider all the aspects of FIPs. For example, Awad and Krishnan [29], Bellman et al. [24], Chellappa and Pavlou [30], Li, Sarathy and Xu [31], Milne and Boza [23], Milne and Rohm [32], and Xu et al. [25] focused on some aspects of FIPs but considered neither all the FIPs dimensions nor their interaction with other interventions. In addition, all these studies are nonexperimental research, and thus do not allow testing of causality.

As for the studies that focused on mobile platforms, Karyda, Gritzalis, Park, and Kokolakis [17] conducted a descriptive study on the obstacles of implementing FIPs. In the case of Libaque-Saenz, Chang, Kim, Park and Rho [6] and Libaque-Sáenz, Wong, Chang, Ha, and Park [22], although these studies focused on the mobile sector, the scope was the secondary use of personal information by network operators (i.e., a situation faced by users when their data have been already collected), and not user interaction with mobile devices before their data are collected. Prior literature contends that the data collection stage is more sensitive for users than the postrelease process itself [33]. In addition, none of these studies used an experimental design to assess causality. Finally, although Xu, Gupta, Rosson, and Carroll [7] focused on mobile apps and used an experimental design, they neither included all the FIPs principles (only choice) nor focused on behavioral intention (their focus was privacy concerns). They did not include another internal factor; rather, they focused on external factors, namely, government intervention and industry regulation. Thus, there is still a gap in the literature to fully understand the effectiveness of FIPs in various contexts.

In short, existing studies have not investigated the effect of all FIPs dimensions on consumers' privacy-related decisions within the mobile apps context. Mobile apps or mobile platforms in general differ from fixed platforms, because the former are characterized by portability, mobility, and permanent availability features [34]. Hence, these platforms can be used anywhere and at any time. In contrast, fixed platforms are usually used in predetermined environments, such as in an office or at home [35]. In addition, mobile apps run on mobile devices (e.g., mobile phones), which are regarded as personal and individual items because users always carry them and rarely share them with others [36]. However, fixed platforms can be used by many people, such as family members and office workers [37]. Furthermore, the location-awareness features of mobile Internet can be used to determine users' physical locations [38], unlike fixed Internet, which does not expose where consumers are located. To better support these differences, we developed an additional survey to determine user perceptions about which device (fixed or mobile) is storing more of their personal information. First, an extensive list of items (pieces of data) was developed based on the General Data Protection Regulation (GDPR) and prior research [39–41]. These items were reviewed by three researchers to assess the clarity and appropriateness of the questions. Finally, we gathered 150 responses through Mechanical Turk, which is the same platform we used to collect data to assess our research model, as it is discussed in the Methodology section. Appendix B shows the source of each of the questions of this survey, while Fig. 1 shows clearly that user perception of the amount of personal information stored by mobile devices is far larger than the amount of data collected by fixed platforms. In fact, according to Ghose [40], smartphones are storing information about who we are, where we are from, where we go, where we have been, our location, what we need, what we have bought, and what our interests are. In addition, the IT Security Survey 2019 revealed that though most of the fixed computers have an installed antivirus, there are about 37.8 % of mobile phones without any antivirus solution [42]. These features of mobile platforms (an active collection of personal information and lack of antivirus programs) may raise greater user perception of risks compared to fixed platforms, and thus additional analysis is required. We argue that the effect of FIPs still remains an accepted "black box" because it "assumes the status of a taken-for-granted truth where its label replaces its contents" [16].

As well as FIPs, we argue that companies could also intervene by adjusting their data collection methods. Data collection activities have raised concerns about data control and the associated potential risks [23,43,44]. Aggressive data collection may give the impression of privacy invasion and affect consumers' decision to use an app. For example, quitters of Facebook are motivated by privacy concerns when they commit "virtual identity suicide" [45]. They are worried about Facebook making their location available, which may reveal patterns of their day-to-day activities and place them at risk [46]. At the same time, they feel they are losing control over personal data because their friends may post information about them without restrictions [47]. Prior research on data collection methods has focused on theoretical discussions [48], their effect on the use of u-commerce [49], and perceptions of personalization [50,51]. However, the interaction of these methods with FIPs remains unexplored. Our study will provide empirical evidence to explain the role of data collection methods in creating consumers' willingness to participate in privacy-related behaviors when using mobile apps and their interaction with FIPs.

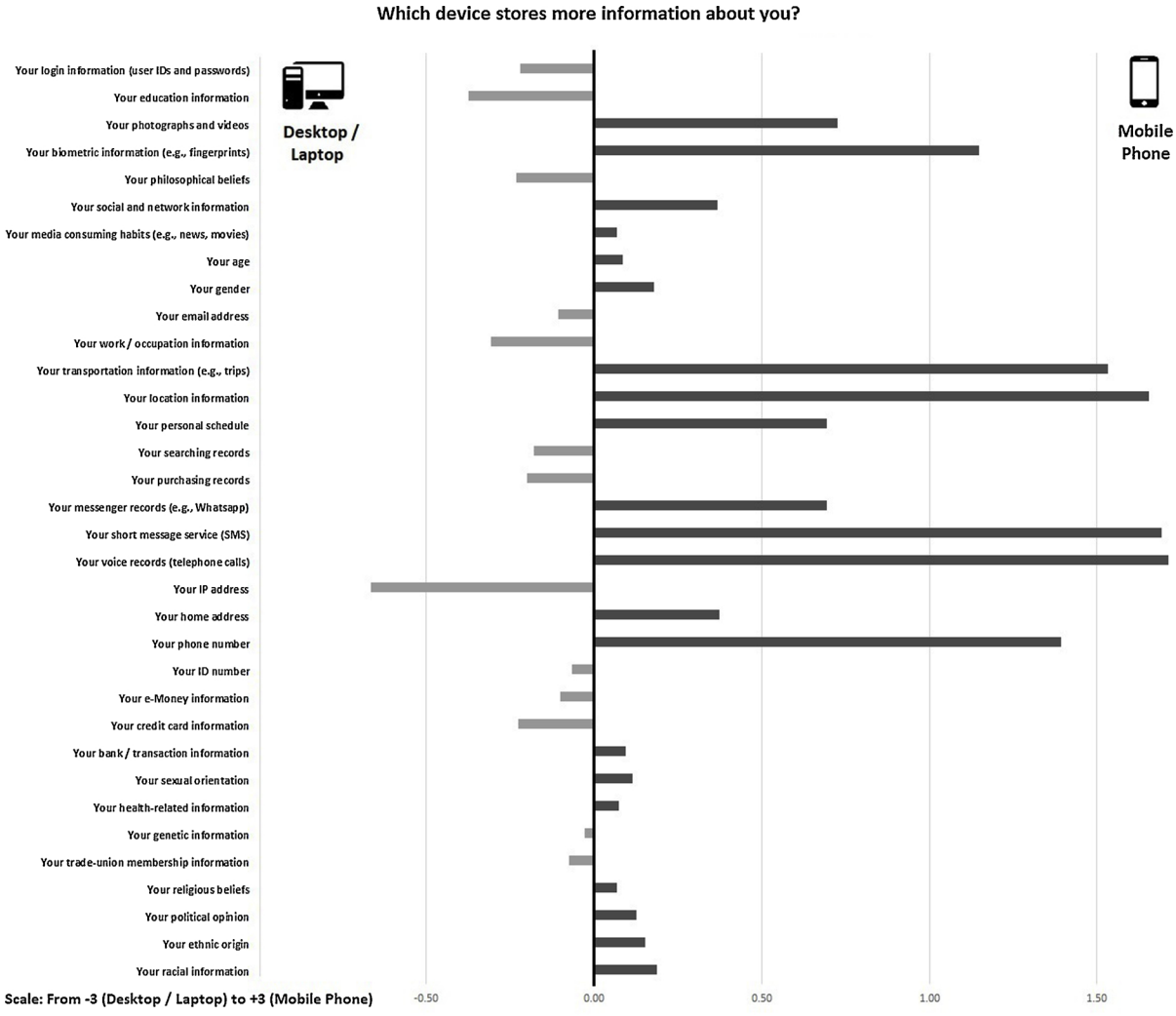
In summary, our study fills previously discussed research gaps by adding a theoretical explanation on the effect of FIPs on user privacy-related decisions. Specifically, we use an experimental design to support causality and include all dimensions of FIPs, and the interaction of FIPs with other important internal factors, such as data collection methods, to understand the power of this intervention on user privacy-related decisions. In addition, we focus on the mobile context that has not yet been fully studied.

The rest of the paper is organized as follows. The next section provides the literature review and develops the hypotheses. The subsequent two sections detail the research methodology and show the results of the study. We then present the discussion and implications as well as the limitations and future research. Finally, we provide a conclusion for the paper.

2. Literature review and hypothesis development

2.1. Fair information practices (FIPs) and other recent privacy policy developments

FIPs is a "set of internationally recognized practices for addressing the privacy of information about individuals" [52]. FIPs were originally proposed in a 1973 report of the US Secretary's Advisory Committee on Automated Personal Data Systems published in response to incensement at automated data collection of individuals' personal information. They were set out in their most effective form in 1980 by the Organization for Economic Co-operation and Development [52]. In the 1990s, the Federal Trade Commission issued amended FIP guidelines in response to the increasing use and processing of personal information by governments and companies in the US. FIPs establish that all companies collecting personal information should comply with four widely accepted FIP principles: notice, access, choice, and security [27,44]. Notice informs consumers that their personal data are being collected prior to data collection; access allows consumers to access and check the accuracy of their data and correct any errors; choice lets consumers decide, which elements of their personal data may be used; and security provides adequate means to keep consumers' personal data secure [44]. A fifth principle on enforcement was added in 2010 [53]. However,



Scale: From -3 to +3 (As respondents's perceptions that their desktops/laptops store more information than their mobile phones do rise higher, the closer to the left are their responses. In contrast, if they perceive that their mobile phones store more information than their desktops/laptops do, their responses are placed at the right part of the scale). Sample = 150 respondents

Fig. 1. Which device stores more information about you?.

FIPs still have limited law enforcement and restriction. In general, organizations can use FIPs to set their own internal privacy policy.

Today, FIPs have become the foundation of privacy policy in many countries [12,16]. They first served as the foundation that influenced the European Union (EU) to set their own first privacy regulation in the 1980s [53]. In May 2018, the EU took its privacy policy effort further by enacting the (GDPR) to ensure proper collection, storage, and use of personal information [54]. As one of the strictest personal data protection laws in the world so far, the GDPR gives clear guidelines to data collectors on the specific rights of data subjects [55]. The GDPR is applicable to both EU and non-EU based organizations that handle the data of EU citizens. The GDPR has four major impacts. First, the rights of EU citizens are enhanced. Data collectors must inform EU citizens about personal data collection, provide them with access, rectify, and erase this data upon their request. Citizens can also object to the secondary use of their personal data. Even big data analytics will likely require explicit consent from the data subjects. Data collectors must also obtain specific consent when they resell and reuse (even in the case of automatic decision-making) personal data [55]. Second, the GDPR redefines and broadens the scope of "Personal Data" to include all direct and indirect identifiers, behavioral, derived and self-identified data, biometrics, and genetic data, and cookies in the computer [56]. However, the GDPR allows special exemptions to governments and research institutes for special data collection and usage of data without complying with the detailed principles in the regulation. For instance, governments may collect personal information of those who might be connected to terrorist organizations without notice or choice [54,55]. Third, the GDPR strongly influences the organizational data processing task and its governance. Both domestic and foreign organizations that are handling the personal data of EU citizens must provide stringent data security and a 72-h data breach notification. Organizations that collect and use data have to make sure that process responsibility applies to both data controllers and data processors [56]. Moreover, the data controllers are legally bound to validate data processors' compliance, and chief data protection officers in the company will take responsibility for specific cases involving severe violation of the GDPR [56]. Fourth, the GDPR will charge high amounts of penalty for non-compliance. For instance, if an organization does not comply with the GDPR, the EU Data Privacy Authority will charge up to 4% of the company's annual revenue or 20 million euro [56].

While initial FIPs movement influenced the EU's regulation, it seems now that the EU's new GDPR strongly affects privacy law in the US, particularly at the individual state level [57]. In the US, two states have enacted personal data protection acts; the first is Vermont and the second is California. In May 2018, Vermont passed the first law on data brokerage, which covers all issues related to selling personal data. The

data brokers in the US collect large amount of personal information, such as marital status, debts, browsing histories, housing status, histories of online purchases, and education credentials. This information is sensitive to many data owners; at the same time, it is valuable to marketing companies.

Prior to March 2018, all 50 US states enacted data breach notification laws that require companies to notify the data subjects, if their personal information is compromised [57]. In addition, individual states have also passed various state-level acts to expand the definition of personal information, and specifically mandate that the data collectors or data brokers implement certain information security requirements on their own [57]. For example, on June 28, 2018, California passed the "California Consumer Privacy Act (CCPA) of 2018." Similarly, on June 2, 2018, Oregon amended its data breach notification law [57]; on April 11, 2018, Arizona amended its Data Breach Notification Law [57]; on September 1, 2018, Colorado passed the Consumer Data Protection Law [57]; on July 19, 2018, Nebraska passed the Nebraska Data Privacy and Security Law; and on July 1, 2018, South Dakota enacted the Data Breach Notification Law [57].

Among all the states, California has the most comprehensive measures to protect users' privacy [57,58]. Its Consumer Privacy Act of 2018 permits consumers to know what type of information any organization has stored about them. At the same time, consumers can ask any organization to remove their personal information. California is also the only state that has protected consumers' cloud data, emails, text messages, metadata, and other information [59].

Many US states have also started to study the EU's GDPR and California's CCPA to enhance their current policy [60]. For example, New York city and New York state government will set their privacy law in the near future [60]. Based on the National Conference of State Legislatures, currently at least 35 states have introduced or have considered having new or amended privacy and security laws in 2018 [60]. Previously, the US had less restriction on using consumer data for business purposes [55,57]. However, because of the strong influence from the EU's GDPR, and the strong economic connection among global companies, the US has begun to change its privacy law starting at the individual state level.

After the EU enacted the GDPR, many countries have also devised their own privacy policy. For example, in July 2018, Brazil passed the personal data protection act [61]. In August 2018, India and Australia introduced the first draft of a data protection act [62,63], and the United Kingdom introduced the new data protection act to plan for personal data protection after Brexit in March 2019 [64].

With the development of privacy policy laws and regulations in the US and other countries, all companies have to carefully handle consumers' personal information regardless of their location. Essentially, they must comply with the core principles of FIPs that are the foundation of all later privacy policies.

2.2. Control-risk framework

Our research is grounded in the control-risk literature – "the most useful framework for analyzing contemporary consumer privacy concerns" [12] – that incorporates the interplay between risk and control to explain behavior. It posits that perceptual control positively affects risk-taking behavior and negatively affects risk perception [43,65]. Perceptual control leads to optimistic bias about the outcome of a behavior [for a review, see 66]. As individuals are motivated to minimize negative outcomes [67], they will weigh the control they possess and the risks they face prior to taking any action. Those who feel in control, tend to have more positive expectation about the outcome, assess the risks as less serious, and take risks compared to individuals who feel a lack of control [33,66,68,69]. Essentially, perceptual control affects risk-taking behavior both directly and indirectly through risk perception (Fig. 2). This control-risk relationship is consistent with the propositions in the Theory of Reasoned Action and the Theory of Planned Behavior (TPB) [70], which posit that behavioral beliefs affect one's intention and actual behavior.

The control-risk, privacy and security literatures suggest that intervention can be used as an action or strategy to reduce risk or induce control as well as to address other concerns happening in a specific situation [71–73]. Midgley [15] defined intervention as a "purposeful action by a human agent to create change." Interventions have been used in prior risk-related studies in various domains, such as the medical/health education, disaster management, and security management fields [15,71–75]. Interventions have no fixed methods or techniques to reduce risk and induce control. It is a situational- and contextual-focused action related to risk observation [15,76]. In the Information Systems field, security and privacy literatures have used interventions to cope with computer system risks [71–73]. Therefore, we added intervention as an antecedent of the control-risk framework.

2.3. Privacy interventions

We tested two privacy interventions (FIPs and the data collection method) that are important to the mobile apps context. FIPs were initiated by the government and expected to be enforced by companies. Previous research has used survey methods to examine the effect of FIPs. For example, Culnan and Armstrong [14] suggested that FIPs are strong antecedents of trust in the information privacy context. Chang et al. [77] surveyed 363 online banking users and found that 4 elements of FIPs (access, notice, security, and enforcement) have significant impact on perceived effectiveness of privacy policy. Wu et al. [78] also used FIPs to examine the intervention effect on privacy concern and trust in the e-commerce context.

As for the data collection methods, previous research [26,79,80] contended that the practices of automatic data access and transmission employed by mobile apps and devices were aggressive, and thus likely to raise privacy concerns among users. Automatic data transmission communicates users' confidential information, such as real-time location, personal identity, and daily behavior [7]. It would be interesting to see how the enforcement of FIPs or the presence of automatic data collection (AUTO) methods and the lack thereof affects users' behavior.

2.4. Fair information practices (FIPs)

The first intervention we used is FIPs. The goal of these principles is to give consumers control over the disclosure and use of their personal data [14]. When an interaction is ruled by impersonal relationships [12], and when individuals lack full understanding about the technologies used for collecting and using their data [49] as in the use of mobile apps, establishing a fair social contract can instill willingness to disclose personal information for a second exchange transaction [81]. We argued that FIPs can serve as a useful strategy to create such a fair social contract when consumers use mobile apps, thus giving them the perception of control over their data. The access principle, for example, gives consumers control over the quality and accuracy of their data. Having data integrity raises one's perception of control [22,82]. The choice principle allows consumers to opt in or opt out of a mobile app service, which again places control in the hands of the customers [18].

While access and choice give self-control over personal data, the principles of notice and security underscore the concept of proxy control. Bandura [83] postulated that individuals' perceptions of proxy control may increase their overall perceptual control. In commercial transactions, not only are companies data holders, they are also agents of proxy control to protect consumers' personal data. As FIPs establish the rules of data usage [19], consumers may be motivated to exert control through the guidelines and feel empowered knowing companies' plans of data collection and use [26,84]. More importantly, consumers have to rely on companies to implement technologies (e.g., privacy-enhancement technologies) to secure their personal data [6,73].

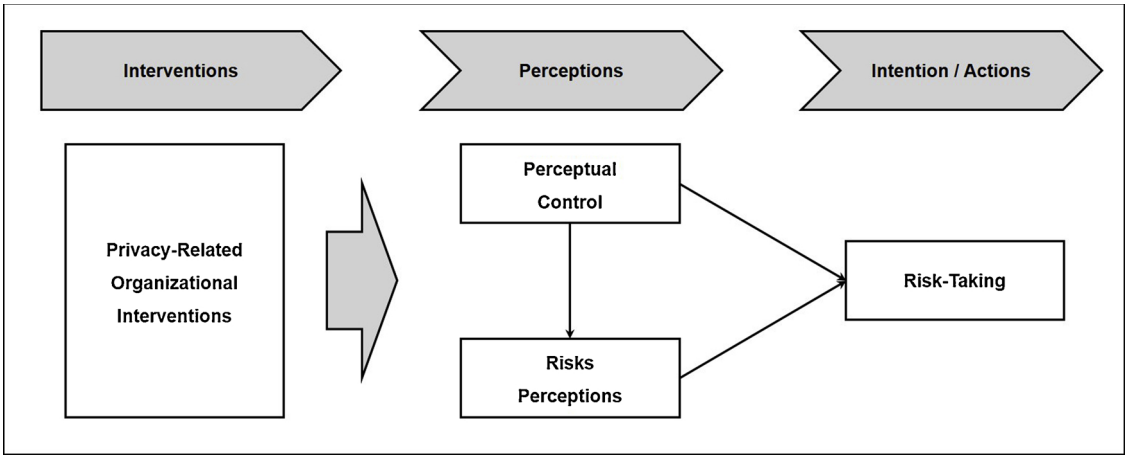


Fig. 2. Control risk framework.

FIPs can also influence consumers' perceived information risks (PIR). The primary purpose of FIPs is to give assurance of security and the proper use of personal information [14]. By informing consumers about their data-handling processes, companies inspire higher perception of procedural fairness and confidence that they will comply with FIPs [25,77]. This will reduce the perception of information risks. In a study of online banking, Chang, Wong, Libaque-Saenz and Lee [77] found that privacy policy negatively influences PIR. On the basis of the arguments presented above, we hypothesized that the presence of FIPs has a direct positive effect on consumers' perceived data control (PDC) and a direct negative effect on consumers' PIR.

Hypothesis 1: Consumers who are explicitly informed that FIPs will be employed in their use of a mobile app will have higher PDC, as compared to consumers who are not explicitly informed about it.

Hypothesis 2: Consumers who are explicitly informed that FIPs will be employed in their use of a mobile app will have lower PIR as compared to consumers who are not explicitly informed about it.

2.5. Data collection method

The second intervention that we are using is the data collection method. Technologies enable the identification of consumer preferences and their locations, to provide personalized offers and services [49]. However, aggressive data collection practices that involve automatic access to consumers' whereabouts, their identity, and daily behaviors [7] are clearly intrusive and have raised concerns on companies' surveillance practices. Nonetheless, companies such as Google and Apple have used apps to collect user location information, to build massive databases for commercial purposes without the consent of device owners [79].

We used the line between customization and personalization [48] to classify the data collection method into nonautomatic (i.e., non-aggressive) and automatic (aggressive) collection. In customization, users must explicitly specify their preferences by selecting the option that best matches their interests (e.g., by entering a zip code to receive local news), whereas personalization employs techniques that automatically collect data and draw user behavioral patterns [48]. Consequently, the concept of customization is used to represent non-AUTO methods, while personalization represents AUTO methods. AUTO subjects consumers to continuous surveillance and tracking to gather huge amount of personal information [7]. This process heightens perceived risks associated with intrusion and privacy violations, and lowers perceived control over personal data [13,26]. Furthermore, to consumers' dismay, AUTO and the associated data analysis techniques employed to automatically draw user behavioral patterns may not always match their needs [48], which again accentuates the lack of control they have over their data. In comparison, nonAUTO places the decision to specify preferences in the hands of the consumers [48], thus giving the impression of lesser risk and higher level of PDC. Accordingly, we proposed:

Hypothesis 3: The AUTO method leads to lower PDC compared to the non-AUTO method.

Hypothesis 4: The AUTO method leads to higher PIR compared to the non-AUTO method.

2.6. Perceived data control, perceived risks, and behavioral intention

"Control" lies at the core of information privacy, [26,65] as individuals want to "determine for themselves when, how, and to what extent information about them is communicated to others [and is being used]" [85, p. 7]. The ease with which digital data are duplicated, disseminated, and used raises the perception of loss of control over personal information [14,86]. There are two types of control: self-control, exerted by the individual; and proxy control, exerted by powerful others, which is used to gain control in situations where the individual lacks power to achieve desired outcomes [26,87].

Privacy literature has operationalized control through PDC, which is defined as consumers' perception of their ability to manage the collection and use of their personal information [25,85]. For mobile app users, the perception of data control is especially salient because many mobile apps can automatically track user location and collect user information [79,88]. Some even require access to certain information such as photo gallery before the users can use the application. These requirements suggest users may have lower control over their personal data, if they choose to use the mobile apps. As consumers lose control over their data, they are likely to perceive higher level of risks because they are worried about potential privacy violations and data leaks [13,43]. Therefore, the higher the level of PDC, the lower the PIR [89,90]. In fact, to gain data control and reduce risks, many users welcome self-protecting options, such as the use of opt-out options or the refusal of information sharing with third parties, to build boundaries in the use of their personal data [91,92]. Thus, we proposed,

Hypothesis 5: PDC negatively affects PIR.

PDC also has a positive effect on behavioral intention [33]. We defined behavioral intention as consumers' willingness to adopt mobile apps. The success of a mobile app depends solely on user adoption and continued use of the app [8,9]. The more users adopt an app, the higher is its success rate. When consumers feel they are in control of their data and perceive others as having limited access to their private information [13,43], they are more likely to use the mobile apps.

Hypothesis 6: PDC positively affects intention.

PIR is defined as "the expectation of losses associated with the disclosure of personal information" [25]. The features of mobile apps raise users' perceptions of information risks. For example, Google and

Apple apps were accused of regularly transmitting users' locations back to the respective companies [79]. Security breaches may also place user information at risk if misappropriated. A good example is the case of KT in South Korea, where the personal information of 12 million customers was stolen after its website was compromised by hackers [93].

Prior studies show that perceived risk is an important antecedent to intention. For example, Janssen and Helbig [94] conducted a study on intention to purchase from B2C e-commerce online stores, and found that risk beliefs have both a direct and an indirect significant effect on purchase intention. In studying intentions to use online banking, Lee [95] found that different types of risks, such as performance, social, time, financial, and security risks, significantly affect behavioral intention. Additionally, both Li, Sarathy and Xu [31] and Malhotra, Kim and Agarwal [65] conducted research on the intention to disclose personal information through the Internet, and found support for a significant effect of risk perceptions on behavioral intention. Pavlou [96] and Van Slyke, Shim, Johnson and Jiang [97] studied the antecedents to intention to transact on the Internet. Both studies found that risk belief has a significant effect on privacy-related behavioral intention. Therefore, we hypothesized,

Hypothesis 7: PIR negatively affect intention.

2.7. Moderation effect of interventions

We investigate the moderation effect of the two intervention methods, FIPs, and AUTO methods, on consumers' perception of data control and information risks. FIPs and AUTO methods have opposite characteristics and serve different purposes. On the one hand, FIPs were developed to monitor how companies handle consumers' personal data to protect consumer privacy [52]. On the other hand, AUTO methods are adopted by companies to collect and maximize the utility of consumer data [25]. Specifically, these methods are designed to collect sensitive information that gives companies more detailed information and knowledge about consumer behavior, and their consumption patterns. Therefore, while FIPs aim to strengthen consumer information privacy, AUTO methods may infringe it.

Erdogan [98] postulated that fairness perception may be influenced by contextual factors. In our research, the data collection variable differentiates two contexts: one with the AUTO method that may be perceived as more intrusive, and one with the non-AUTO method, which may be seen as less intrusive. Therefore, we hypothesize an interaction effect between FIPs and data collection methods on PDC and PIR. FIPs are supposed to provide consumers with control over the collection of their personal information and lower the risks of sharing their information. We argue that non-AUTO scenarios will further accentuate these effects because consumers consciously enter their information. Indeed, consumers must select the products and services that best match their interests, and to obtain discounts they have to enter their location as well [13,48]. It means that in these scenarios consumers can, to a certain extent, predefine what personal information is collected by companies, providing them with control over data collection, and reducing the risks associated with sensitive information that consumers may not want to share with companies. In contrast, in AUTO scenarios, consumers' expectation toward their data control and information risks are low because consumers already agreed to companies' AUTO in exchange for personalized services [48,74]. Vaidyanathan and Aggarwal [99] postulated that controllability may affect individuals' perception of fairness. It is, thus, expected that fairness perception in AUTO scenarios will be lower than that in non-AUTO scenarios, because in the former scenarios consumer controllability of data collection is lower than in the latter. This situation may further increase consumer perceptions of risks, because companies may be gathering information that consumers may not want to be tracked. In other words, while the presence of FIPs will also increase PDC and decrease PIR in AUTO scenarios, the effect will not be as high as in non-AUTO scenarios. Comparatively, the difference in PDC and PIR between the presence and the absence of FIPs is greater in the non-AUTO context than in the AUTO context.

Hypothesis 8: The difference between consumers' PDC when they are explicitly told that FIPs will be employed for collecting and using their personal data, and when they are not explicitly told about FIPs is greater in non-AUTO than in AUTO scenarios.

Hypothesis 9: The difference between consumers' PIR when they are explicitly told that FIPs will be employed for collecting and using their personal data, and when they are not explicitly told about FIPs is greater in non-AUTO than in AUTO scenarios.

Research on procedural justice suggests that perceptions of aggressiveness may be reduced by procedural fairness [100]. Accordingly, in the presence of FIPs, the effects of AUTO methods are expected to be lower than in scenarios without FIPs. Although AUTO methods are expected to reduce consumer perception of control, the presence of FIPs may weaken this perception by providing consumers with knowledge about how their data will be treated (i.e., procedural fairness). Indeed, this knowledge provides consumers with the opportunity to exert control if companies do not comply with FIPs principles. Likewise, it is expected that AUTO methods have a positive effect on perceptual risk. However, considering that FIPs aim to assure security and the proper use of personal information [14], the presence of FIPs may reduce this effect by increasing consumer perception that companies will use appropriate mechanisms to protect their information and avoid misusing it. We hypothesize:

Hypothesis 10: The difference between consumers' PDC when AUTO methods are used and when non-AUTO methods are used, is greater in scenarios without FIPs than in scenarios with the presence of FIPs.

Hypothesis 11: The difference between consumers' PIR when AUTO methods are used and when non-AUTO methods are used, is greater in scenarios without FIPs than in scenarios with the presence of FIPs.

2.8. Mediation effect

The research model implies that the effect of privacy interventions on behavioral intention is fully mediated by behavioral beliefs. We tested these mediations.

Fig. 3 shows our research model.

3. Research methodology

We adopted an experimental design for this research. The presence or absence of FIPs and the data collection method were manipulated using a 2 (FIPs versus NO-FIPs) X 2 (AUTO versus non-AUTO) between-subject factorial design (Fig. 4). We used a scenario-based methodology because scenarios are descriptions of possible future situations and the methodology supports causality [101]. Prior research based on experimental design have used this methodology to manipulate similar interventions in similar situations [26,49]. We created four scenarios (Appendix C) that corresponded to each of the manipulations.

The scenario describes a mobile app called "E-Discounts" that provides paperless promotion and discount information on products and services, such as books, cosmetics, restaurants, and cinemas. This app can store records of the discounts and promotions used. Considering that each coupon has a unique code and refers to a specific product or service, the app may create a list of past shopping records associated with a user.

As for FIPs intervention, it was operationalized by explicitly telling the subjects that the app has a set of "privacy clauses" that allows them to: 1) give or withhold their consent for the collection and use of their personal data; 2) access their past shopping records and correct them in the event of any mistake; 3) revise the app's practices in the use of their personal information; and 4) use data encryption to keep personal information safe from security breaches. This clause corresponds to the four dimensions of FIPs. In the case of NO-FIPs, information on the privacy clause was removed from the description of the scenario.

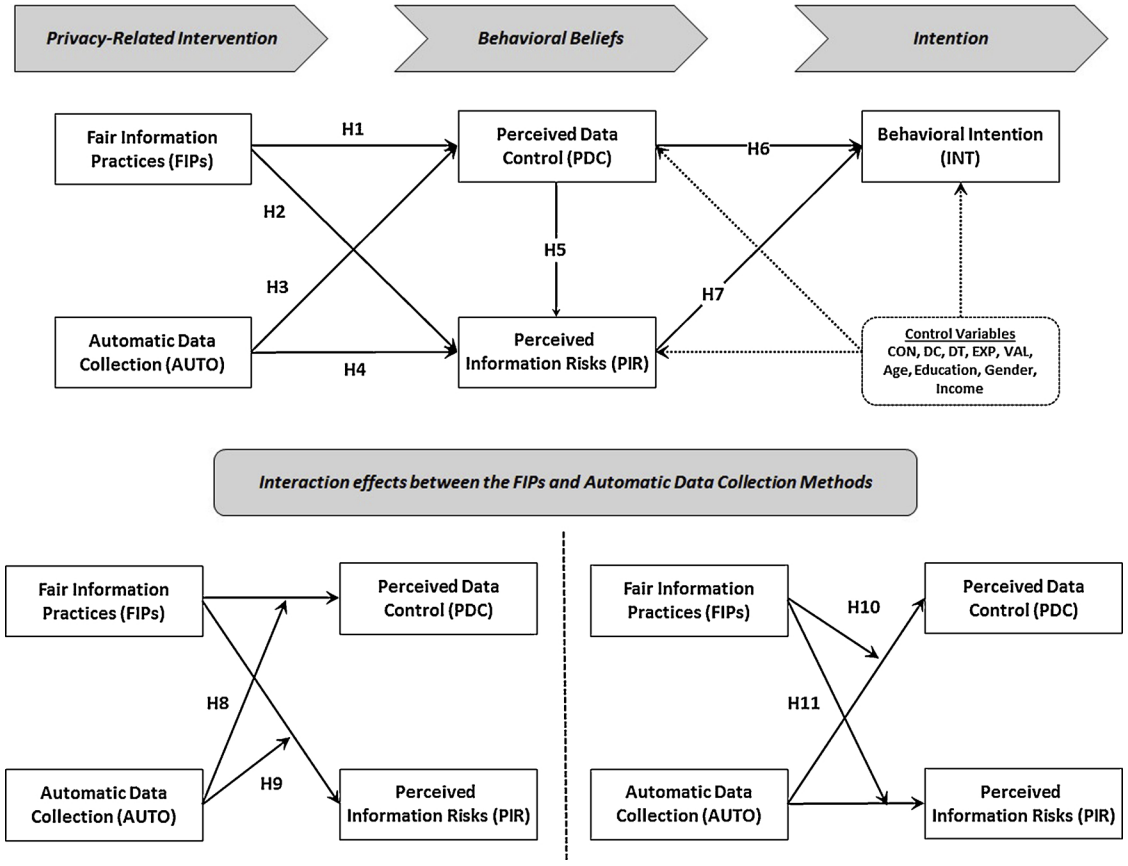


Fig. 3. Research model.

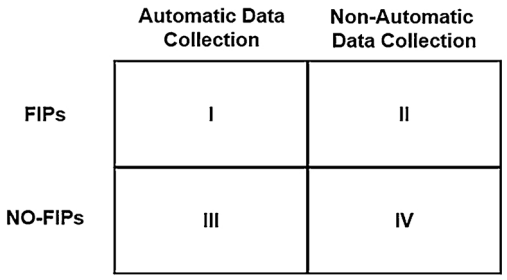


Fig. 4. Experimental design.

In the case of data collection methods, this app is a location-based service (LBS), and thus, it needs to know user location to provide discounts and promotions. Also, an LBS needs to be personalized to match user preferences about products and services. We built two options for the way this app could know both user location and preferences. In the first option, we explained to the respondents that this app will be connected to the database of their mobile telephone service provider, and therefore, is capable of automatically tracking their location even when they are not using the app. In addition, the app will be able to track user' search habits in the app itself as well as in other platforms, such as Google, Amazon, and eBay, to automatically suggest coupons based on their location and preferences. This option was labeled as AUTO (aggressive).

As for the second option, the respondents were informed that the app has no capability to automatically track user location or user search habits. Instead, users will be asked to provide a "preference list" of the products and services that best match their interests as well as entering the zip code of the area where they are located, to access information on promotions and discounts. Accordingly, this second option was labeled as non-AUTO (nonaggressive).

3.1. Subject and procedures

We used Amazon Mechanical Turk[1] to collect data from consumers in the USA. We asked potential respondents to assist a company in evaluating an app that would soon be launched on the market. They were informed that their participation was voluntary and their answers would remain anonymous. We followed three methods used in the literature [102] to detect careless responses: 1) two attention check items that have only one correct response embedded in the question (Appendix D), 2) reverse-coded items (Appendix D), and 3) a statement informing the participants that a statistical method is in place to detect random responses.

For each valid and completed response, we gave a monetary incentive of US$1.40. Such compensation is comparable to payments for similar tasks on this website. In addition, to ensure that the scenarios were randomly displayed to the respondents, we built four questionnaires in Google Drive representing each of the four scenarios (each questionnaire with its own *url*[2]). We used a *php*[3] file that generated a random number from 1 to 4 and associated this number (1–4) to the *url* of a specific questionnaire. Then, we uploaded this file to a website hosted on the Internet. When a respondent accessed the website, the *php* file was executed generating a random number that redirected the respondent to the *url* of the associated scenario.

After excluding careless responses, a total of 258 valid responses were used for analysis (66, 65, 61, and 66 for scenarios I, II, II, and IV, respectively). There was no significant difference among the number of participants in the four scenarios ($X_1^2 = 0.143$, $p = 0.706$). Table 1

Table 1
Demographics.

Participants (N = 258)		Frequency	Percent
Gender	Female	107	41.47
	Male	151	58.53
Age	20-30 years	86	33.33
	31-40 years	100	38.76
	41-50 years	43	16.67
	51 and over	29	11.24
Education	Incomplete school studies	3	1.16
	High school graduate	40	15.50
	Some college, no degree	85	32.95
	Bachelor or professional degree	112	43.41
	Master's degree	16	6.20
	Doctorate degree	2	0.78
Income	US$ 19,999 or below	60	23.26
	US$ 20,000 - US$ 29,999	46	17.83
	US$ 30,000 - US$ 39,999	42	16.28
	US$ 40,000 - US$ 49,999	35	13.57
	US$ 50,000 - US$ 59,999	23	8.91
	US$ 60,000 - US$ 69,999	24	9.30
	US$ 70,000 - US$ 79,999	9	3.49
	US$ 80,000 - US$ 89,999	3	1.16
	US$ 90,000 or above	16	6.20
Internet experience	3 years - Less than 6 years	1	0.39
	6 years - Less than 9 years	16	6.20
	9 years - Less than 12 years	26	10.08
	12 years - Less than 15 years	57	22.09
	15 years or more	158	61.24
e-Commerce experience	Less than 12 months	22	8.53
	12 months - 24 months	16	6.20
	24 months - 36 months	8	3.10
	More than 3 years	212	82.17
Mobile device experience	Less than 12 months	13	5.04
	12 months - 24 months	11	4.26
	24 months - 36 months	18	6.98
	More than 3 years	216	83.72
m-Commerce experience	Less than 12 months	65	25.19
	12 months - 24 months	46	17.83
	24 months - 36 months	53	20.54
	More than 3 years	94	36.43

presents the demographics of the subjects. More than 70 % of the participants are less than 40 years old, representing a younger generation that is more likely to adopt new technology and services [103]. This is evident from their fairly extensive experience in using the Internet, mobile devices, e-commerce, and m-commerce.

The experimental procedures consisted of two phases. In the first phase, each subject was asked to read the scenario they were presented with. In the second phase, the subjects were asked to complete a questionnaire that measured their PDC, perceived risks, and intention to subscribe to the service provided by the company (i.e., the registration stage). Data control, for instance, could be assessed both at the time of initial registration and subsequent use of the app. Even though data control assessment may be most important at the usage stage, individuals tend to focus on the most proximate level of control they have, that is, the registration stage [33]. Accordingly, Brandimarte, Acquisti, and Loewenstein [33] claimed that people who feel in control at the registration stage, may underestimate the level of risk that arises from the actual use of the data. Therefore, we focused on the registration stage to shed light on the effect of FIPs.

Finally, each subject was also asked to provide demographic information and answer questions related to manipulation check, attention check, control variables, and marker variable. We conducted two pilot tests to refine treatment scenarios and to validate the measures.

3.2. Measurement items

All measurement items were adapted from the literature to fit our research. Hair, Ringle, and Sarstedt [104] postulated that "one should not use dummy (i.e., categorical and dichotomous) variables in reflective measurement models." They suggest the use of formative models when using categorical variables because this type of modeling "requires an interpretation similar to that of regression analyses with dummy variables" [104]. Therefore, the FIPs and data collection variables that were dichotomous were modeled using formative measures. All other constructs were modeled as reflective measures. Appendix D shows the measurement items, while Table 2 shows the sources of the measurement items.

Table 2
Measurement Items.

Construct	Items	Scale	Likert	Adapted from
Behavioral Intention (INT)	3	bipolar	7-point	Sheng et al. [49]
Perceived data control (PDC)	5	unipolar	5-point	Xu, Teo, et al. [26]
Perceived information risks (PIR)	4	bipolar	7-point	Xu et al. [25]
Privacy concerns (CON)	3	bipolar	5-point	Joinson et al. [105]
Desire for control (DC)	2	bipolar	7-point	Xu, Teo, et al. [26]
Disposition to trust (DT)	3	bipolar	7-point	Xu, Teo, et al. [26]
Previous experience (EXP)	1	unipolar	5-point	Xu, Teo, et al. [26]
Value for personalization (VAL)	1	bipolar	7-point	Chellappa and Sin [106]
Marker variable (MV)	2	bipolar	7-point	Xu, Teo, et al. [26]

3.3. Control variables

Control variables are mainly used to explain factors other than the core theoretical constructs used in the study, which could help to explain the variance in the main constructs or dependent variables [107]. In this study, we collected data on personal characteristics and situational clues and used them as control variables (Appendix D). Age, gender, and education have been included as covariates in prior privacy studies [26]. Income was added because wealthier consumers may have more to lose financially, if privacy violations occur [29]. As for situational clues, we included privacy concerns, disposition to trust, desire for control, value for personalization, and previous experience with privacy invasion [29,41,43,106,108]. Many studies have examined these situational clues, and found that they exerted various effects on control, risk, and intention. In this study, we controlled these situational clues to minimize covariate effects from them.

4. Results

4.1. Manipulation and control checks

We took several steps to verify the salience of our manipulations. First, the conditions on the existence or absence of FIPs, and the use of automatic and non-AUTO were checked using yes/no questions to confirm that the respondents understood the scenarios (Appendix D). Second, the manipulation check for FIPs asked whether the respondents believed their personal information would be used fairly (1 = completely false; 7 = completely true) (Appendix D). The t-test result shows the participants in the FIPs group perceived that their personal data would be used more fairly than the participants in the NO-FIPs group (mean difference = 2.261, S.D. = 0.193, t = 11.724, and p = 0.000).

In addition, chi-square tests were conducted to examine the demographic differences among the treatments. The results show there were no significant differences among the treatments in age (Fisher's exact *p*-value = 0.660), gender ($X_3^2 = 5.780$, p = 0.123), education (Fisher's exact *p*-value = 0.919), income (Fisher's exact *p*-value = 0.657), Internet experience (Fisher's exact *p*-value = 0.706), e-commerce experience (Fisher's exact *p*-value = 0.391), mobile device experience (Fisher's exact *p*-value = 0.526), and m-commerce experience ($X_9^2 = 5.746$, p = 0.765).

We also tested the differences in the control variables. The ANOVA

tests show that there were no significant differences between treatments in previous experience ($F_{3,254} = 0.421$, $p = 0.738$) and privacy concerns ($F_{3,254} = 1.171$, $p = 0.321$). Welch ANOVA tests also show that the four treatments did not differ significantly in the value of personalization ($F_{3,139.376} = 2.014$, $p = 0.115$) and disposition to trust ($F_{3,140.660} = 2.231$, $p = 0.087$). Desire for control was severely non-normal with a kurtosis value greater than +3, so a nonparametric Kruskal-Wallis test was performed. The result shows that there were no significant differences between the four treatments ($X_3^2 = 5.057$, $p = 0.168$). Overall, all the tests confirmed that our manipulations were successful.

4.2. PLS analysis

We used SmartPLS 3.0 software [109] to validate the measurement model, and to evaluate the hypothesized path in the research model. Partial Least Square (PLS) is a powerful second-generation multivariate technique that employs a component-based approach to produce the estimates [110]. It assesses both the measurement and structural models simultaneously in an optimal fashion, while placing minimum restrictions on measurement scales, sample size, and residual distributions [110,111]. More importantly, PLS is robust in theory testing and in managing complex models [110]. We specifically chose PLS because of the exploratory nature of our study, which is in the early stage of theory development, and the use of formative items to measure FIPs and AUTO (dichotomous variables) [104].

4.3. Tests for multicollinearity and common method Bias

To check for potential multicollinearity, we analyzed the variance inflation factor (VIF). A VIF value less than or equal to 5 suggests the absence of multicollinearity [112]. We regressed behavioral intention on all other variables. The highest VIF value was 3.585 for PIR, indicating that our model does not present the evidence of multicollinearity.

Furthermore, we assessed the threat of common method bias (CMB) using the marker variable approach suggested by Lindell and Whitney [113]Lindell and Whitney [81] and Harman's single-factor [114]. For the marker variable approach, we used fashion leadership as the marker variable to compute the CMB-adjusted correlated matrix [115]. The result shows that the correlation coefficients between the marker variable and the theoretical constructs were close to zero ($r = 0.057$, n.s. for perceived fairness; $r = 0.007$, n.s. for PIR; $r = 0.031$, n.s. for PDC; and $r = 0.046$, n.s. for behavioral intention), which indicates that CMB was unlikely to be a significant issue. For Harman's test, we entered all measurement items into a single exploratory factor analysis in SPSS and analyzed the unrotated solution. The results show that the first extracted factor accounted for 36 % of the variance in the data, which was much lower than the threshold of 50 %. This result again suggests that CMB was not a significant issue.

4.4. Measurement model assessment

To validate the measurement model, we first examined item reliability and convergent validity using Cronbach's alpha, composite reliability, and average variance extracted (AVE). Table 3 shows that the values for composite reliability and Cronbach's alpha were above the recommended 0.7 level [116], and the AVEs were above 0.5 for all constructs [117]. Also, Appendix E shows that the factor loadings exceeded 0.7, suggesting that the variance shared between an item and its construct was greater than error variance [111].

We then assessed the discriminant validity. From Table 4, the square roots of all AVEs were much larger than the cross-correlations. Also, each item loaded most strongly on its corresponding construct (Appendix E). As the cross-loadings derived from PLS will inevitably be higher than those derived from exploratory factor analysis, Gefen and Straub [118] suggested the cross-loading difference (i.e., the difference between the loading of each item on its corresponding latent variable and the loading of the item on every other variable) should be higher than the recommended value of 0.1. Appendix E shows that all our cross-loading differences met this requirement. In addition, we assessed the heterotrait-monotrait ratio (HTMT). According to current literature, HTMT values supporting discriminant validity should be lower than 0.85 if constructs are conceptually different, while the threshold is set to 0.90 if the constructs are conceptually similar [119–121]. Table 5 shows that all HTMT values are under 0.85, except those for PDC and PIR, which is 0.87. This value, though, is under 0.90 because these variables are conceptually related. Together, these tests suggest that our measurement model demonstrated adequate item reliability, convergent reliability, and discriminant validity.

Table 3
Internal consistency.

Construct	AVE	Composite Reliability	Cronbach's Alpha
Behavioral intention (INT)	0.975	0.991	0.987
Perceived data control (PDC)	0.860	0.969	0.959
Perceived information risks (PIR)	0.886	0.969	0.957
Privacy concerns (CON)	0.730	0.890	0.816
Desire for control (DC)	0.876	0.934	0.868
Disposition to trust (DT)	0.911	0.968	0.951
Marker variable (MV)	0.934	0.966	0.930

4.5. Structural model assessment

To assess the structural model, we analyzed the R^2 values and the path coefficients. Table 6 presents the results for three models. Model 1 is the full model including the control variables; Model 2 presents the effect of our theoretical constructs, excluding the control variables; and Model 3 shows the effect of the control variables only which served as the baseline model to examine the impact of the theoretical constructs.

In Model 1, the presence of FIPs had a significant positive effect on PDC (H1). However, FIPs intervention had no effect on PIR (H2). As for AUTO, this intervention had a significant negative effect on PDC (H3), and a significant positive effect on PIR (H4). Moreover, PDC had a significant negative effect on PIR (H5), and a positive effect on behavioral intention (H6). Finally, PIR had a significant negative effect on behavioral intention (H7). It is important to notice from the results of Model 2 that the significance of these paths is the same even when we did not control the covariates.

We compared the R^2 values between Model 1 and Model 3 to determine the effect size of the theoretical model. Model 1 explained 52.51 % (61.41 %-8.90 %) more variance than Model 3 for PDC. The R^2 differences were 57.98 % (73.78 %-15.80 %) for PIR and 56.37 % (68.77 %-12.40 %) for behavioral intention. Cohen [122] was used to calculate the effect size (f^2) of the theoretical constructs.[1] Effect size with f^2 values of 0.02, 0.15, and 0.35 are considered small, medium, and large, respectively [122]. The inclusion of the theoretical constructs had an effect size of $f^2 = 1.36$ for PDC, $f^2 = 2.21$ for PIR, and $f^2 = 1.80$ for behavioral intention, all far above the cut-off of 0.35 for a large effect size.

We also compared the R^2 values between Model 1 and Model 2 to determine the effect size of the control variables. The differences in R^2 were 5.61 % (61.41 %-55.80 %) with $f^2 = 0.145$ for PDC, 3.38 % (73.78 %-70.40 %) with $f^2 = 0.129$ for PIR, and 2.27 % (68.77 %-66.50 %) with $f^2 = 0.073$ for behavioral intention. All effect sizes were close to the cut-off of 0.15, suggesting moderate effects. In other words, our

[1] Cohen's formula to calculate effect size: $f^2 = (R^2_{included} - R^2_{excluded})/(1 - R^2_{included})$

Table 4
Correlation among constructs.

Construct	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1. INT	**0.987**														
2. PDC	0.775	**0.927**													
3. PIR	−0.786	−0.833	**0.941**												
4. CON	−0.218	−0.234	0.315	**0.855**											
5. DC	−0.069	−0.124	0.162	0.221	**0.936**										
6. DT	0.202	0.121	−0.168	−0.190	0.029	**0.954**									
7. EXP	−0.123	−0.097	0.199	0.351	0.196	0.054	**1.000**								
8. VAL	0.289	0.189	−0.244	−0.320	−0.019	0.238	−0.125	**1.000**							
9. Age	−0.015	−0.058	0.028	0.039	0.165	0.134	0.102	−0.078	**1.000**						
10. Education	−0.073	−0.093	0.131	0.118	0.002	0.054	0.186	−0.163	0.002	**1.000**					
11. Gender	−0.003	0.021	−0.041	−0.040	−0.165	−0.118	−0.017	0.001	−0.219	−0.043	**1.000**				
12. Income	0.029	−0.056	0.019	−0.029	0.007	0.068	0.142	0.050	0.103	0.399	0.016	**1.000**			
13. FIPs	0.504	0.695	−0.573	−0.043	0.031	−0.007	−0.007	0.067	−0.017	−0.033	−0.089	−0.034	**1.000**		
14. AUTO	−0.314	−0.256	0.312	0.081	0.113	−0.148	0.025	−0.025	0.033	0.007	−0.037	−0.054	0.024	**1.000**	
15. FIPs x AUTO	−0.133	−0.102	0.117	0.074	0.073	−0.067	0.066	−0.120	0.117	0.015	−0.115	−0.008	−0.001	0.001	**1.000**

INT = behavioral intention, PDC = perceived data control, PIR = perceived information risks, CON = privacy concerns, DC = desire for control, DT = disposition to trust, EXP = previous experience, VAL = value for personalization, FIPs = fair information practices, AUTO = automatic data collection.
Numbers on the diagonal are the square root of AVE values.

Table 5
Heterotrait-monotrait ratio (HTMT).

Construct	1	2	3	4	5	6	7	8
1. INT	—							
2. PDC	0.795	—						
3. PIR	0.809	0.868	—					
4. CON	0.243	0.263	0.356	—				
5. DC	0.067	0.127	0.169	0.265	—			
6. DT	0.205	0.124	0.173	0.216	0.036	—		
7. EXP	0.124	0.100	0.204	0.386	0.217	0.056	—	
8. VAL	0.291	0.193	0.250	0.356	0.036	0.244	0.125	—

theoretical constructs were substantive enough to explain a large proportion of the variance in the proposed research model. The only hypothesis that was not supported was the direct effect of FIPs on PIR (H2).

Finally, we included Fig. 5 that graphically shows the results of the full model compared with the results of the theoretical model to summarize our findings.

4.6. Overall model fit assessment

To assess the overall goodness of fit of our research model, we used the consistent PLS algorithm to examine the following parameters: the standardized root mean squared residual (SRMR), the Normed Fit Index (NFI), unweighted least squares discrepancy (d_{ULS}), and geodesic discrepancy (d_G), as suggested by Henseler, Hubona, and Ray [123]. In the case of SRMR, values under 0.08 are considered a good fit [123]. In terms of NFI, to support an adequate fit, this parameter should be higher than 0.90 [123]. As for d_{ULS} and d_G, these parameters should be lower than the 95 % bootstrapped quantile [123]. Our research model meets the above criteria as follows: SRMR = 0.021 (< 0.08), NFI = 0.956 (> 0.90), d_{ULS} = 0.046 (HI95 % = 0.052), and d_G = 0.256 (HI95 % = 0.687). In other words, there is evidence that there is a good fit between our proposed research model and the data.

4.7. Moderation test

First, we assessed the moderation effect of AUTO on the effect of FIPs on PDC (H8), and the moderation effect of FIPs on the interaction between AUTO and PDC (H10). The coefficient path of the interaction term between FIPs and AUTO on PDC was significant (β=-0.10, $p < 0.05$), supporting the existence of both moderation effects (H8 and H10). In addition, the effect size of the interaction term was 0.023,

Table 6
Structural model results.

Effect	1. Full Model	2. Theoretical	3. Control
Perceived Data Control			
Fair information practices	0.70***	0.70***	
Automatic data collection	−0.24***	−0.27***	
Privacy concerns	−0.12*		−0.17*
Desire for control	−0.08*		−0.09
Disposition to trust	0.06		0.08
Previous experience	−0.01		0.01
Value for personalization	0.08		0.11
Age	0.00		−0.04
Education	0.06		−0.04
Gender	−0.02		0.00
Income	−0.05		−0.05
R^2	**61.41**	**55.80**	**8.90**
Perceived Information Risks			
Perceived data control	−0.70***	−0.78***	
Fair information practices	−0.09	−0.03	
Automatic data collection	0.11**	0.11**	
Privacy concerns	0.07		0.19**
Desire for control	0.03		0.10
Disposition to trust	−0.05		−0.12
Previous experience	0.09**		0.09
Value for personalization	−0.05		−0.13*
Age	−0.04		0.00
Education	−0.03		0.08
Gender	0.04		−0.03
Income	−0.04		0.00
R^2	**73.78**	**70.40**	**15.80**
Behavioral Intention			
Perceived data control	0.40***	0.39***	
Perceived information risks	−0.44***	−0.46***	
Privacy concerns	0.06		−0.09
Desire for control	0.04		−0.05
Disposition to trust	0.06		0.14*
Previous experience	−0.03		−0.06
Value for personalization	0.11**		0.21**
Age	0.01		0.00
Education	−0.01		−0.04
Gender	0.01		0.00
Income	0.05		0.03
R^2	**68.77**	**66.50**	**12.40**

*p < 0.05, **p < 0.01, ***p < 0.001.

which was considered to be between small and medium effect according to [122]. Table 7 shows the mean and standard deviation for PDC across the four scenarios created by the interaction between FIPs and AUTO.

Fig. 6 further confirms the presence of the interaction effect. FIPs

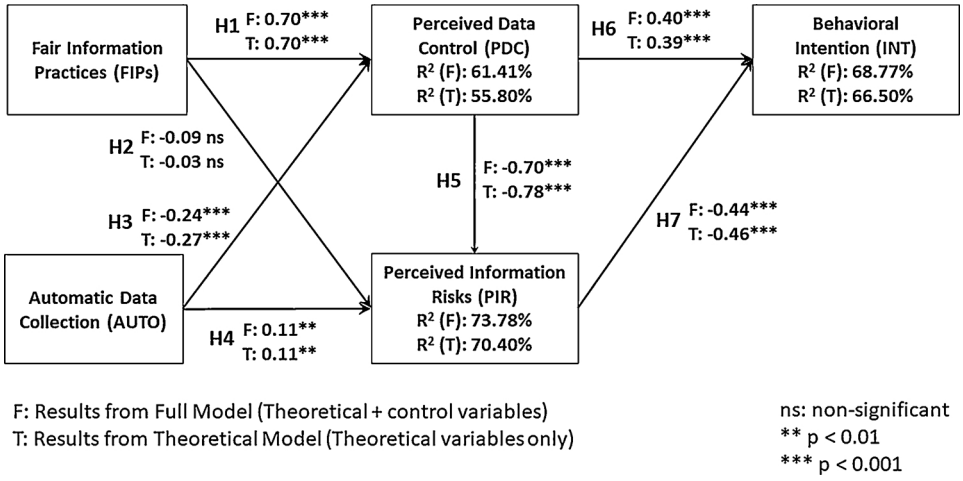


Fig. 5. SEM assessment.

Table 7
Means and standard deviations for PDC (FIPs and AUTO).

Between-Subjects Factors		PDC		
FIPs	AUTO	Number of Participants	Mean	Standard Deviation
Yes	Yes	66	2.85	0.81
	No	65	3.68	0.80
No	Yes	61	1.52	0.60
	No	66	1.90	0.70

PDC = perceived data control, FIPs = fair information practices, AUTO = automatic data collection.

triggered higher perceptions of data control in both AUTO (mean difference = 1.33, p = 0.001) and non-AUTO (mean difference = 1.78, p < 0.001). Also, the difference in PDC between FIPs and NO-FIPs was greater in the non-AUTO context (1.78) than in the AUTO context (1.33), which suggested that the automatic collection of personal data triggers higher perception of loss of control. With FIPs, consumers' perceptions of data control were significantly larger when their information was not collected automatically, than when it was collected automatically (mean difference = 0.83, p < 0.001). Even in the absence of FIPs, this difference remained significant (mean difference = 0.38, p < 0.05). Finally, the difference in PDC between the automatic and non-AUTO contexts was greater when FIPs were used (0.83) than in scenarios without FIPs (0.38), which suggested that fairness in information practices weakens the negative effect of AUTO practices. Overall, there was support for H8 and H10.

In the case of the moderation effect of AUTO on the effect of FIPs on PIR (H9), and the moderation effect of the FIPs on the impact of AUTO on PIR (H9), the coefficient path of the interaction term between the FIPs and AUTO on PIR was found to be nonsignificant (β = 0.038, p = 0.270). Therefore, these moderation effects (H9 and H11) were not supported.

4.8. Mediation test

Considering that H2 was not supported, the above results suggest that FIPs exert an indirect effect on PIR rather than a direct effect. Accordingly, we conducted an additional test to assess the mediation effect of PDC on the relationship between FIPs and PIR. We followed the guidelines proposed by Zhao, Lynch Jr, and Chen [124] by setting the software, in 5000 bootstrap samples, at the 95 % level of confidence. Table 8 shows that the indirect effect of FIPs on PIR was significant, while the direct effect remained nonsignificant. These results support the existence of a full mediation.

In addition, our research model proposes that privacy interventions influence consumer beliefs, which in turn impact on behavioral intention. In other words, consumer beliefs mediate the effect of interventions on intention, which is consistent with the TPB [70]. To assess this

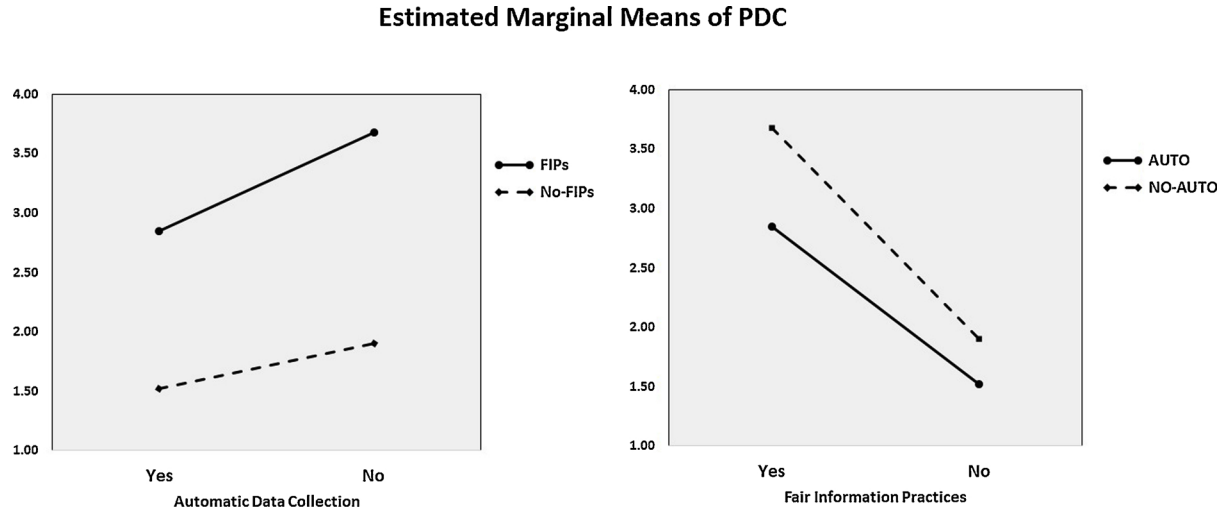


Fig. 6. Interaction effects.

Table 8
Mediation analysis.

Relationship	Direct effect	Indirect effect
FIPs → PIR	−0.033[ns]	−0.548***
FIPs → INT	−0.034[ns]	0.306***
AUTO → INT	−0.070[ns]	−0.163***

[ns] = nonsignificant, ***p < 0.001.

mediation effect, we included a direct path between FIPs and intention and between AUTO and intention. Table 8 shows that direct effects of FIPs and AUTO on intention were both nonsignificant, whereas the indirect effects of these interventions on intention were significant, supporting a mediation effect of consumer beliefs on the relationship between the interventions and behavioral intention.

5. Discussion and implications

Our study has several key findings that contribute novelty to the privacy literature. First, by finding the significant impact of FIPs and data collection methods on PDC and perceived risks and in turn behavioral intention, we show how the intervention strategies effectively influence privacy intention. In developing and validating the substantive model, our study contributes new findings to the privacy literature, and reaffirms control risk as a useful framework to analyze contemporary consumer privacy concerns. Furthermore, we extend current understanding of privacy to the mobile technology context – an imminent trend that is full of challenges especially with advancement of hacking techniques [125].

Second, despite being in effect for years, FIPs remain a black box. Our study empirically found that this set of institutional guidelines exerts an influence on consumers' privacy assessment in their intention to adopt mobile apps. Moreover, our findings reveal what is inside this black box by showing that FIPs provide consumers with control, and it is this control that impacts on their perception of risk and risk-taking behaviors. This result suggests that technology adoption research ought to consider the power of institutional guidelines when introducing new technology, especially mobile apps. Our finding is also novel in unveiling the effect of institutional guidelines on information privacy decisions.

Third, the significant direct effect and moderating effect of the data collection method elucidates the powerful role of the data collection method in determining privacy decisions, and ultimately the intention to use mobile apps. In particular, AUTO is considered aggressive, and tends to increase perceived risk and lower PDC. The difference in PDC between situations with the presence and absence of FIPs is also larger in nonautomatic than in AUTO. Our findings provide theoretical and empirical insights into the dynamics of consumer data collection methods. It draws attention to the fact that while FIPs are effective in increasing PDC, companies need to adopt a more informative technique to increase this perception. A more informative technique also reduces consumers' information risk perception.

Fourth, our mediation analysis found that behavioral beliefs are significant mediators between company intervention strategies and behavioral intention, suggesting that intervention strategies may regulate privacy behavioral beliefs and, in turn, use intention.

5.1. Implications for practice

Our findings provide important practical implications for companies. First, because FIPs are effective in increasing PDC, companies should clearly communicate to consumers their commitment to FIPs. In particular, companies should highlight the principles of access and choice that give consumers the power to manage their personal data. They should also underscore the principle of notice that equips consumers with knowledge of their data usage. When consumers are officially informed how their information will be collected and used, and when they have the choice to opt in or opt out, they feel in control of their information and see less risk. Therefore, to increase consumer confidence, companies should include consumer notification and permission seeking, as part of their standard operating procedures. The practice is useful as the potential value companies might gain from the large volume of personal information captured, and the subsequent understanding achieved through consumer analytics far outweighs minor consumer nuisance of screen pop-ups. The practice is also useful in promoting companies' image in abiding by ethical standards.

Second, companies should strategize the best approach to manage the tradeoff between consumer data collection method and privacy concerns. AUTO, while highly valuable, may deter consumers from using the apps. However, companies may try a counter-approach that can increase consumers' willingness to use mobile apps. For example, they can provide consumers with more benefits that will overshadow the privacy risks in sharing personal data. The literature posits that consumers use a risk-benefit calculus when formulating their privacy concerns and intention to share personal information [23,43]. When the benefits outweigh the costs, consumers may assume risky behaviors of sharing personal data, such as participating in "second exchange" transactions, in return for high quality and personalized services [126].

Third, in the mobile-apps market, consumers' intention to use an application is influenced by their perception of data control and information risks. Companies could deploy a control-risk balancing technique that reduces consumers' perceived risks and increases their PDC. For example, developers and content providers could provide clear options that allow consumers to exercise personal data control within the apps.

5.2. Limitations and suggestions for future research

Despite the empirical support for our research model, our study has limitations, which call for additional research. First, our categorization of automatic and non-AUTO methods represents only one of the factors that may interact with FIPs to affect PDC and behavioral intention. As justice perception literature postulates that the perception of fairness may be influenced by contextual factors [98], future research could examine additional variables, such as the presence or absence of enforcement and the degree of information sensitivity. Furthermore, we only categorized the FIPs intervention into two types: the presence and absence of FIPs. Likewise, data collection methods were classified into two types: automatic (i.e., aggressive) and nonautomatic (i.e., nonaggressive). Future research could gain deeper insights by further dividing the FIPs intervention into different levels of compliance with each of its dimensions, while data collection methods could be further divided into different levels of intrusiveness.

Another limitation is the use of scenarios, to operationalize the presence or absence of FIPs and the data collection method. Some may argue a scenario does not mirror the real life context, especially when the target is complex human decision-making related to privacy. However, the literature contends that scenario design does provide useful insights into similar phenomena [49]. Moreover, we limited the number of variables to those that are most realistic when one uses mobile apps.

Also, we have not considered perceived usefulness of a mobile app, which might have influenced users' decision to adopt an app. The literature [127–129] suggests that users may choose to use an app when the perceived usefulness outweighs the privacy risk, which reduces the effect of privacy concerns. Future research could include both perceived usefulness and privacy concerns in the study, to examine a potential tradeoff between the variables.

Furthermore, our sample was based in the United States. Care should be taken with generalization, because privacy-related situations are culture-dependent [24]. Future work could replicate our study in

other contexts and evaluate the potential moderation effect of cultural factors.

Our study focused only on mobile apps. Future research could compare and contrast our findings with those from services such as social network sites, e-banking, and e-commerce. Prior research has found that different services may invoke different levels of concerns about privacy [25]. Future research could also address the effectiveness of the FIPs implementation method. The negative side of FIPs also opens new opportunities for future research. For example, future study may extend the literature on the control paradox, which claims that the same control that leads consumers to disclose more information may expose them to higher levels of privacy violations [33]. Finally, the potential moderation effect of the covariates included in this study may call for further attention.

6. Conclusion

The success of mobile apps depends on the usage rate. However, privacy concern often stands as the roadblock that may hinder consumers' adoption of these apps. In this study, we tested the effect of two company intervention strategies, FIPs and the data collection method, on privacy-related decisions. We found that the intervention strategies are effective in influencing privacy-related decisions. This finding suggests companies could deploy our validated intervention strategies to increase the use of their mobile apps while abiding by ethical standards.

6.1. Endnote

1 Amazon Mechanical Turk is a web-based environment where employers (called the requesters) post outsourced tasks for an anonymous network of laborers (called the workers), who receive compensation for their contribution [130]. The responses are anonymous [130–132]. Prior research has reported that this tool is effective, and has produced similar results to those obtained using samples from USA students and USA consumer panels [130].

[2] Uniform Resource Locator (url) refers to a web resource that specifies its location on the Internet and a mechanism for retrieving it.

[3] Hypertext processor (php) is a language designed for web development that uses a general-purpose programming language.

6.2. Compliance with ethical standards

Ethical approval: All procedures performed in studies involving human participants were in accordance with the ethical standards of the institutional and/or national research committee, and with the 1964 Helsinki declaration and its later amendments or comparable ethical standards. Informed consent: Informed consent was obtained from all individual participants included in the study.

CRediT authorship contribution statement

Christian Fernando Libaque-Sáenz: Conceptualization, Investigation, Methodology, Writing - original draft. **Siew Fan Wong:** Writing - review & editing, Funding acquisition. **Younghoon Chang:** Project administration, Visualization, Formal analysis. **Edgardo R. Bravo:** Supervision.

Acknowledgment

This study was funded by the Malaysian Ministry of Education, Fundamental Research Grant Scheme (FRGS) (Grant Number FRGS/1/2014/SS05/SYUC/02/1).

Appendix A. Literature Review

Authors (Year)	Research Question	Context	Dependent Variable	Independent Variables/ Concepts in the case of descriptive design	Research Design (Data Analysis Technique)	Main Findings
Awad and Krishnan [29]	Does information transparency affect willingness to be profiled online for personalized offerings?	Fixed (Website)	Willing to be profiled online for personalized services/ advertisement	Importance of information transparency, privacy concern, importance of privacy policies, previous privacy invasion	Nonexperimental correlation (Structural equation modeling)	Consumers who value information transparency are less likely to participate in personalization.
Bellman, Johnson, Kobrin and Lohse [24]	Are cultural values, Internet experience, or desire for government intervention associated with different forms of Internet privacy regulation?	Fixed (Website)	Privacy concerns	Cultural values, government involvement in regulation, Internet experience	Non experimental correlation (MANCOVA)	Differences in Internet privacy concerns across countries may be explained by differences in cultural values and Internet experience ("enforcement" dimension of Fair Information Practices [FIPs]).
Bonner and Chiasson [16]	What are FIPs and how did they achieve their status?	General (Unspecified)	None	Fair information practices principles, actant	Nonexperimental descriptive (None)	FIPs were the result of a complex interaction among various social, political, and technical elements, while their worldwide acceptance was due to enlistment, convenience, and expediency factors.
Chellappa and Pavlou [30]	1) Which are the antecedents to perceived security in e-commerce? 2) Is perceived security an antecedent to trust?	Fixed (Website)	Trust in e-commerce transactions	Encryption, protection, verification, authentication, perceived security, financial liability	Nonexperimental correlation (Lineal regression)	Perceived security (encryption, protection, and authentication) is a stronger antecedent to trust than are reputation and financial liability.
Culnan [20]	1) How many Web sites have posted privacy disclosures? 2) To what extent do these privacy disclosures reflect fair information practices?	Fixed (Website)	None	Fair information practices, types of personal information	Nonexperimental descriptive (None)	Although the majority of websites disclose a privacy policy, only 14 % of these policies present clear and comprehensive statements.
Culnan and Armstrong [14]	Are consumers willing to disclose personal information and be profiled for marketing when organizations use FIPs?	Fixed (Website)	Willingness to be profiled	Privacy concerns, prior experience	Preexperimental (Lineal Discriminant Analysis)	When customers are told that FIPs are used, privacy concerns do not distinguish between those who are willing to be profiled from those who are unwilling to participate.

Culnan and Bies [12]	1) Are privacy concerns shaped by perceived fairness of corporate information practices? 2) How to implement FIPs	Fixed (Website)	None	Willingness to disclose personal information, fair information practices implementation alternatives	Nonexperimental descriptive (None)	Justice theory explains the effect of FIPs on privacy concerns. Implement FIPs through regulation, industry self-regulation, and technological solutions.
Karyda, Gritzalis, Park and Kokolakis [17]	How can privacy protection through FIPs be accommodated in ubiquitous technologies?	Mobile (Ubiquitous technologies)	None	Obstacles to implementation of fair information practices	Nonexperimental descriptive (None)	Obstacles to the implementation of FIPs in ubiquitous technologies are due to technical and social issues, such as computing power limitations of small devices and asymmetry of power.
Li, Sarathy and Xu [31]	What is the impact of affective and cognitive reactions on personal information disclosure decision?	Fixed (Website)	Intention to give personal information	Risk belief, protection belief, relevance of information, awareness of privacy statement, privacy concerns, sensitivity of information, joy, and fear	Nonexperimental correlation (Structural equation modeling)	Initial emotions formed from an overall impression of a website act as initial hurdles to information disclosure. Once users enter the information exchange stage, fairness-based levers further adjust perceived privacy.
Libaque-Saenz, Wong, Chang, Ha and Park [22]	What is the impact of perceived information practices on individuals' perceptions of information risks?	Mobile (Network operator)	Perceived information risks to give consent to use personal information	Trust, privacy concerns, data control, policy awareness, and information protection	Nonexperimental correlation (Structural equation modeling)	Passive dimensions of information practices influence the active dimension of information practices, while the latter directly and indirectly affects individuals' perceptions of risks (through privacy concerns and trust).
Libaque-Saenz, Chang, Kim, Park and Rho [6]	What is the role of organizational information practices on users' intention to authorize the secondary use of their personal information?	Mobile (Network operator)	Intention to authorize personal data for secondary use	Perceived risk, perceived benefits, perceived data control, policy awareness, information protection, trust, and privacy concerns	Nonexperimental (Structural equation modeling)	Intention to authorize personal data for secondary use is driven by perceived risk, perceived benefits, and FIPs-related variables such as perceived policy awareness, perceived information protection, and perceived data control.
Liu, Marchewka, Lu and Yu [28]	What is the effect of perceived privacy (measured through information practices) on trust and behavioral intention?	Fixed (Website)	Behavioral intention (Repeat repurchase, visit again, recommend to others, and positive remarks)	Trust, privacy (Notice, access, choice, and security)	Experimental (Correlation)	Perceptions of privacy indirectly affect intention. This effect is explained by trust. When users are in a scenario based on FIPs, perceptions of privacy, trust, and their intentions are higher than in a non-FIP scenario.
Milne and Boza [23]	1) How concerned are individuals with organizations' information practices? 2) How much do they trust these information practices? 3) What are the antecedents and consequences of concerns and trust?	Fixed (Computer)	Computer usage, trust, and concerns	Perceived control, knowledge, attitude toward relationship marketing, and attitude toward direct marketing	Nonexperimental correlation (Lineal regression)	Improving trust and reducing concerns are different approaches to managing customer information. Improving trust is more effective than reducing privacy concerns.
Milne and Rohm [32]	1) How do customers' preferences about name removal vary depending on privacy, purchase experience, and channel? 2) Which alternative (opt-in or opt-out) may be more adequate for name removal?	Fixed (Email)	Respondents' desire to remove their names	Data collection awareness, name removal knowledge, purchase experience, demographics, and direct marketing channel	Nonexperimental correlation (Lineal regression)	When notice and choice exists, consumers are less inclined to remove their names for direct marketing. Channels for direct marketing and purchase experience affect customers' desires for name removal.
Nemati and Van Dyke [27]	1) What is the effect of reading privacy statements on individuals' trust and risk beliefs? 2) Does FIPs have any influence on individuals' trust and perception of risks?	Fixed (Website)	Trust and perceived risk	Fair information practices, reading privacy policy, and interaction of these two variables	Quasi-experimental (T-test, ANOVA)	Reading privacy statement may increase individuals' trust; however, these statements may increase risk perceptions. The effect of FIP components was found to be nonsignificant.
Pearson [18]	What are the privacy challenges faced by software engineers when they target the cloud?	Fixed (Cloud computing services)	None	Fair information practices, implementation options and guidelines	Nonexperimental descriptive (None)	FIPs could be implemented through Privacy Enhancing Technologies (PETs). The study also suggests some implementation guidelines.
Schwaig, Kane and Storey [19]	How well do the Fortune 500 firms comply with the FIP?	General (Unspecified)	None	Fair information practices compliance	Nonexperimental descriptive (None)	Most of the Fortune 500 firms comply with the notice component of FIPs but fail to address the other components (choice, security, and access).
Sheehan and Hoy [133]	Do FIPs address users' privacy concerns?	Fixed (Website)	Privacy concerns	Fair information practices principles	Nonexperimental correlation (Factor analysis)	FIPs can address most users' privacy concerns. However, relationship between entities and users, and the exchange of information for appropriate compensation may also influence this variable.
Smith, Milberg and Burke [134]	What is the nature of individuals' privacy concerns about	General (Unspecified)	None	Privacy concerns dimensions	Nonexperimental correlation (Factor analysis)	Privacy concerns are related to collection, errors, unauthorized secondary use, and improper

	organizational information practices?					access. The authors developed and validated a measurement instrument to address privacy concerns.
Xu, Dinev, Smith and Hart [135]	What is the link between individuals' privacy perceptions and institutional privacy assurances?	Fixed (Website)	Privacy concerns	Privacy risk, privacy control, effectiveness of privacy policy, effectiveness of industry self-regulation, and disposition to value privacy	Nonexperimental correlation (Structural equation modeling)	Individuals form their privacy concerns through a control-risk assessment, which is affected by their perceptions of the effectiveness of institutional privacy assurances.
Xu, Teo, Tan and Agarwal [26]	What is the effect of privacy assurances on privacy concerns?	Mobile (Apps)	Privacy concerns	Perceived data control, individual self-protection, industry self-regulation, and government legislation	Experimental (Structural equation modeling)	Perceived control is the key for managing consumers' privacy concerns. Consent and enforcement affect privacy concerns.

Appendix B. User perception of personal information collection by devices

Type of data	Source
Racial information	Article 9 GDPR
Ethnic origin	Article 9 GDPR
Political opinion	Article 9 GDPR
Religious beliefs	Article 9 GDPR
Trade-union membership information	Article 9 GDPR
Genetic information	Article 4 (13) GDPR
Health-related information	Article 4 (15) GDPR
Sexual orientation	Article 9 GDPR
Bank/transaction information	Financial data - Phelps et al. [41]
Credit card information	Financial data - Phelps et al. [41]
E-Money information	Financial data - Phelps et al. [41]
ID number	Ghose [40], Personal identifiers - Phelps et al. [41]
Phone number	Ghose [40], Personal identifiers - Phelps et al. [41]
Home address	Ghose [40], Personal identifiers - Phelps et al. [41]
IP address	Ghose [40], Personal identifiers - Phelps et al. [41]
Voice records (telephone calls)	Ghose [40], Personal identifiers - Phelps et al. [41]
Short message service (SMS)	Ghose [40], Personal identifiers - Phelps et al. [41]
Messenger records (e.g., Whatsapp)	Ghose [40], Personal identifiers - Phelps et al. [41]
Purchasing records	Ghose [40], Shopping habits - Phelps et al. [41]
Searching records	Ghose [40], Chen et al. [39]
Personal schedule	Ghose [40], Lifestyle characteristics - Phelps et al. [41]
Location information	Ghose [40]
Transportation information (e.g., trips)	Ghose [40], Lifestyle characteristics - Phelps et al. [41]
Work/occupation information	Demographics - Phelps et al. [41]
Email address	Personal identifiers - Phelps et al. [41]
Gender	Demographics - Phelps et al. [41]
Age	Demographics - Phelps et al. [41]
Media-consuming habits (e.g., news, movies, etc.)	Lifestyle characteristics - Phelps et al. [41]
Social and network information	Ghose [40], Chen et al. [39]
Philosophical beliefs	Article 9 GDPR
Biometric information (e.g., fingerprints)	Article 4 (14) GDPR
Photographs and videos	Recital 51 GDPR
Education information	Demographics - Phelps et al. [41]
Login information (user IDs and passwords)	Recital 56 GDPR, Chen et al. [39]

Note: Phelps et al. (2000) suggest five categories of data: demographics, lifestyle characteristics (including media habits), shopping habits, financial data, and personal identifiers.

Appendix C. Scenarios for the Study

Cover Story

Company X provides E-Discounts (paperless and wireless discounts) service as a platform between merchants and customers. This service is an optional channel to receive promotions and discounts about products or services. Products or services could be books, cosmetics, restaurants, cinemas, clothes, etc.

Suppose you are considering whether you will subscribe to E-Discounts service. First, you should learn the procedures for using this application (app), which is free.

Scenario I: Presence of FIPs and Automatic Data Collection

App Installation: You first need to install the E-Discounts app on your mobile phone.

Data Collection: This app is connected to your mobile telephone service provider database. Therefore, to profile your preferences, Company X can automatically access: (1) your whereabouts and (2) other information about you (e.g., search habits).

Options: This app will present a "Privacy Suit" that allows you to:

- give or withhold your consent to Company X to use specific personal data about you (e.g., name, occupation, gender, age, and e-mail) without affecting the use of this app.
- correct information about your past E-Discounts shopping records (you can correct mistakes, if any, in your records to keep an accurate profile).

- check Company X's practices for using your personal information (how long this information is stored, how this information is used, and with whom this information may be shared).
- use data encryption and secure your personal data (this technology is used to keep your personal data safe from potential security breaches).

Discounts: Company X can automatically access your whereabouts at any time, even if you are not using this app at that moment. When you move into the area of one of the merchants working with Company X, this company automatically provides you with E-Discounts for products or services based on your preferences profile. By showing these E-Discounts to the merchants, you can obtain cash discounts when buying a product or service.

Scenario II: Presence of FIPs and Non-Automatic Data Collection

App Installation: You first need to install the E-Discounts app on your mobile phone.

Data Collection: To profile your preferences for future discounts usage, you have to select a list of products and services ("preference list") that best matches your interests.

Options: This app will present a "Privacy Suit" that allows you to:

- give or withhold your consent to Company X to use specific personal data about you (e.g., name, occupation, gender, age, and e-mail) without affecting the use of this app.
- correct information about your past E-Discounts shopping records (you can correct mistakes, if any, in your records to keep an accurate profile).
- check Company X's practices for using your personal information (how long this information is stored, how this information is used, and with whom this information may be shared).
- use data encryption and secure your personal data (this technology is used to keep your personal data safe from potential security breaches).

Discounts: This app cannot automatically track your current whereabouts; therefore, to retrieve information about discounts of products and services you should enter the zip code of the zone where you are located. For example: If you are currently in a zone of Miami, FL, and want information about discounts for merchants located in this zone, you can choose the state "FL" from the menu, select the city of Miami, select the ZIP code of the zone, and then click on "search." A list of discounts based on your preferences (selected by yourself in your "preference list") will be displayed. By showing these E-Discounts to the merchants, you can obtain cash discounts when buying a product or service.

Scenario III: Absence of FIPs and Automatic Data Collection

App Installation: You first need to install the E-Discounts app on your mobile phone.

Data Collection: This app is connected to your mobile telephone service provider database. Therefore, to profile your preferences, Company X can automatically access: (1) your whereabouts and (2) other information about you (e.g., search habits).

Options: Upon installation, the following message will appear:

"I agree with the use of my personal information."

If you don't agree with this message, you will not be able to use this app. (Notice that beyond this message, no additional information about privacy policy will be displayed).

Discounts: Company X can automatically access your whereabouts at any time, even if you are not using this app at that moment. When you move into the area of one of the merchants working with Company X, this company automatically provides you with E-Discounts for products or services based on your preferences profile. By showing these E-Discounts to the merchants, you can obtain cash discounts when you buy a product or service.

Scenario IV: Absence of FIPs and Non Automatic Data Collection

App Installation: You first need to install the E-Discounts app on your mobile phone.

Data Collection: To profile your preferences for future discounts usage, you have to select a list of products and services ("preference list") that best match your interests.

Options: Upon installation, the following message will appear:

"I agree with the use of my personal information."

If you don't agree with this message, you will not be able to use this app. (Notice that beyond this message, no additional information about privacy policy will be displayed).

Discounts: This app cannot automatically track your current whereabouts; therefore, to retrieve information about discounts of products and services you should enter the zip code of the zone where you are located. For example: If you are currently in a zone of Miami, FL, and want information about discounts for merchants located in this zone, you can choose the state "FL" from the menu, select the city of Miami, select the ZIP code of the zone, and then click on "search." A list of discounts based on your preferences (selected by yourself in your "preference list") will be displayed. By showing these E-Discounts to the merchants, you can obtain cash discounts when you buy a product or service.

Appendix D. Measurement Items

Control Variables

CON1	In general, consumers have lost all control over how their personal information is collected and used by online companies.
CON2	In general, most online companies handle personal information they collect about users in a proper and confidential way (R).
CON3	In general, existing laws and organizational practices provide a reasonable level of protection for user online privacy today (R).
DC1	Before I decide to provide personal information to a company, I wish the company would inform me fully about the collection of my personal information.
DC2	Before I decide to provide personal information to a company, I wish I have more information about how my personal information would be used by the company.
DT1	I usually trust people until they give me a reason not to trust them.
DT2	I generally give people the benefit of the doubt when I first meet them.
DT3	My typical approach is to trust new acquaintances until they prove I should not trust them.
EXP	How often have you heard or read during the past year about the use and potential misuse of the information collected by companies?
VAL	I value the products and services that are personalized for my usage experience.

CON = privacy concerns, DC = desire for control, DT = disposition to trust, EXP = previous experience, VAL = value for personalization, (R) = reverse coded

Theoretical Constructs

PIR1	When faced with this scenario, using "E-Discounts" service may involve a high potential for privacy loss.
PIR2	When faced with this scenario, using "E-Discounts" service may lead to an inappropriate use of my personal information.
PIR3	When faced with this scenario, using "E-Discounts" service will not involve any problem with my personal information (R).
PIR4	When faced with this scenario, using "E-Discounts" service would be risky, in general.
PDC1	When faced with this scenario, how much control do you feel you may have over your personal information collected by Company X?
PDC2	When faced with this scenario, how much control do you feel you may have over the amount of your personal information collected by Company X?
PDC3	When faced with this scenario, overall, how much control do you feel you may have over your personal information provided to Company X?
PDC4	When faced with this scenario, how much control do you feel you may have over who can get access to your personal information collected by Company X?
PDC5	When faced with this scenario, how much control do you feel you may have over how your personal information would be used by Company X?
INT1	When faced with this scenario, I intend to adopt this service.
INT2	When faced with this scenario, I predict I will use this service.
INT3	When faced with this scenario, I plan to use this service.

PIR = perceived information risks, PDC = perceived data control, INT = behavioral intention, (R) = reverse coded

Marker Variable (Fashion Leadership)

MV1	I am aware of fashion trends and want to be one of the first to try them.
MV2	I am the first to try new fashion; therefore, many people regard me as being a fashion leader.

Manipulation Check Items

CHECK1 (choice)	Based on the above description, "E-Discounts" service allows me to grant or revoke my consent to Company X for using specific personal data about me without affecting the use of this app. In other words, I could still use this app even if I revoke my consent.
CHECK2 (access)	Based on the above description, "E-Discounts" allow me to correct information about my "past" E-Discounts shopping records, if any mistake exists.
CHECK3 (notice)	Based on the above description, "E-Discounts" service informs me about Company X's practices for using my personal information, such as for how long this information is stored, how this information is used, and with whom this information may be shared.
CHECK4 (security)	Based on the above description, "E-Discounts" service provides a data encryption functionality to keep my personal data safe from potential security breaches.
CHECK5 (automatic)	Based on the above description, Company X can automatically access information about my current "whereabouts" at any time, even if I am not using this app at that moment.
FAIR	When faced with this scenario, I believe my personal information will be used fairly.

FAIR = perceived fairness

Attention Check Items

ATC1	When providing information about me I feel comfortable. Although we ask about your feeling in this situation, please skip this question so we know you are paying attention.
ATC2	How much control do you have over the weather condition? Although we know you have no control in this situation, please select – a great deal – so we know you are paying attention.

Appendix E. Confirmatory Factor Analysis (Loadings)

Items	INT	PDC	PIR	CON	DC	DT	MV	EXP	VAL
INT1	**0.978**	0.750	−0.764	−0.205	−0.078	0.189	0.031	−0.133	0.299
INT2	**0.992**	0.773	−0.780	−0.219	−0.069	0.202	0.059	−0.115	0.272
INT3	**0.992**	0.771	−0.785	−0.220	−0.058	0.207	0.046	−0.116	0.287
PDC1	0.730	**0.948**	−0.802	−0.193	−0.130	0.086	−0.069	−0.084	0.159
PDC2	0.702	**0.929**	−0.763	−0.215	−0.075	0.127	−0.024	−0.094	0.196
PDC3	0.767	**0.952**	−0.799	−0.203	−0.091	0.100	−0.042	−0.102	0.183
PDC4	0.726	**0.904**	−0.765	−0.260	−0.195	0.161	0.005	−0.075	0.172
PDC5	0.662	**0.904**	−0.729	−0.214	−0.082	0.088	−0.012	−0.098	0.169
PIR1	−0.734	−0.780	**0.936**	0.260	0.179	−0.156	−0.009	0.145	−0.210
PIR2	−0.745	−0.783	**0.945**	0.343	0.156	−0.157	0.021	0.204	−0.267
PIR3	−0.719	−0.777	**0.941**	0.315	0.122	−0.178	−0.011	0.234	−0.235
PIR4	−0.762	−0.795	**0.943**	0.270	0.152	−0.144	0.022	0.167	−0.209
CON1	−0.179	−0.226	0.286	**0.838**	0.200	−0.090	−0.053	0.378	−0.208
CON2	−0.181	−0.190	0.269	**0.866**	0.156	−0.251	−0.056	0.235	−0.334
CON3	−0.198	−0.180	0.252	**0.859**	0.209	−0.151	−0.179	0.281	−0.284
DC1	−0.094	−0.139	0.173	0.204	**0.969**	0.023	−0.012	0.172	−0.041
DC2	−0.016	−0.079	0.117	0.216	**0.902**	0.036	0.014	0.207	0.022

DT1	0.224	0.139	−0.187	−0.201	0.016	**0.965**	0.135	0.048	0.219
DT2	0.176	0.110	−0.159	−0.160	0.037	**0.942**	0.103	0.047	0.255
DT3	0.170	0.089	−0.127	−0.177	0.034	**0.956**	0.132	0.061	0.206
MV1	0.047	−0.032	−0.001	−0.114	0.002	0.131	**0.971**	−0.031	0.203
MV2	0.041	−0.029	0.014	−0.099	−0.007	0.120	**0.962**	−0.052	0.143
EXP	−0.123	−0.097	0.199	0.351	0.196	0.054	−0.042	**1.000**	−0.125
VAL	0.289	0.189	−0.244	−0.320	−0.019	0.238	0.181	−0.125	**1.000**

INT = behavioral intention, PDC = perceived data control, PIR = perceived information risks, CON = privacy concerns, DC = desire for control, DT = disposition to trust, MV = marker variable, EXP = previous experience, VAL = value for personalization

Appendix F. Supplementary data

Supplementary material related to this article can be found, in the online version, at doi:https://doi.org/10.1016/j.im.2020.103284.

References

[1] S. Conger, J.H. Pratt, K.D. Loch, Personal information privacy and emerging technologies, Inf. Syst. J. 23 (2013) 401–417.
[2] G. Chittaranjan, J. Blom, D. Gatica-Perez, Mining large-scale smartphone data for personality studies, Pers. Ubiquitous Comput. 17 (2013) 433–450.
[3] K. Shilton, D. Greene, Linking Platforms, Practices, and Developer Ethics: Levers for Privacy Discourse in Mobile Application Development, J. Bus. Ethics (2017) 1–16.
[4] N. Kshetri, Big data′ s impact on privacy, security and consumer welfare, Telecomm. Policy 38 (2014) 1134–1145.
[5] A. McAfee, E. Brynjolfsson, Big data: the management revolution, Harv. Bus. Rev. 90 (2012) 60–66.
[6] C.F. Libaque-Saenz, Y. Chang, J. Kim, M.-C. Park, J.J. Rho, The role of perceived information practices on consumers' intention to authorise secondary use of personal data, Behav. Inf. Technol. 35 (2016) 339–356.
[7] H. Xu, S. Gupta, M.B. Rosson, J.M. Carroll, Measuring mobile users' concerns for information privacy, Proceedings of the 33rd International Conference on Information Systems (ICIS 2012), Orlando, FL, 2012.
[8] A.P. Oghuma, Y. Chang, C.F. Libaque-Saenz, M.-C. Park, J.J. Rho, Benefit-confirmation model for post-adoption behavior of mobile instant messaging applications: a comparative analysis of KakaoTalk and Joyn in Korea, Telecomm. Policy 39 (2015) 658–677.
[9] X. Hu, W. Li, Q. Hu, Are mobile payment and banking the killer apps for mobile commerce? Proceedings of the 41st Hawaii International Conference on System Sciences (HICSS 2008), Waikoloa, Hawaii, 2008.
[10] D. Takahashi, The App Economy Could Double to $101 Billion by 2020, Venturebeat, 2016.
[11] K. Martin, Understanding privacy online: development of a social contract approach to privacy, J. Bus. Ethics 137 (2016) 551–569.
[12] M.J. Culnan, R.J. Bies, Consumer privacy: balancing economic and justice considerations, J. Soc. Issues 59 (2003) 323–342.
[13] T. Dinev, H. Xu, J.H. Smith, P. Hart, Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts, Eur. J. Inf. Syst. 22 (2013) 295–316.
[14] M.J. Culnan, P.K. Armstrong, Information privacy concerns, procedural fairness, and impersonal trust: an empirical investigation, Organ. Sci. 10 (1999) 104–115.
[15] G. Midgley, Systemic intervention for public health, Am. J. Public Health 96 (2006) 466–472.
[16] W. Bonner, M. Chiasson, If fair information principles are the answer, what was the question? An actor-network theory investigation of the modern constitution of privacy, Inf. Organ. 15 (2005) 267–293.
[17] M. Karyda, S. Gritzalis, J.H. Park, S. Kokolakis, Privacy and fair information practices in ubiquitous environments: research challenges and future directions, Internet Res. 19 (2009) 194–208.
[18] S. Pearson, Taking account of privacy when designing cloud computing services, Proceedings of the First International Workshop on Software Engineering Challenges for Cloud Computing (ICSE CLOUD 2009), Vancouver, Canada, 2009.
[19] K.S. Schwaig, G.C. Kane, V.C. Storey, Compliance to the fair information practices: How are the Fortune 500 handling online privacy disclosures? Inf. Manag. 43 (2006) 805–820.
[20] M.J. Culnan, Protecting privacy online: Is self-regulation working? J. Public Policy Mark. 19 (2000) 20–26.
[21] M. Warkentin, A.C. Johnston, J. Shropshire, The influence of the informal social learning environment on information privacy policy compliance efficacy and intention, Eur. J. Inf. Syst. 20 (2011) 267–284.
[22] C.F. Libaque-Sáenz, S.F. Wong, Y. Chang, Y.W. Ha, M.-C. Park, Understanding antecedents to perceived information risks: an empirical study of the Korean telecommunications market, Inf. Dev. 32 (2016) 91–106.
[23] G.R. Milne, M.-E. Boza, Trust and concern in consumers' perceptions of marketing information management practices, J. Interact. Mark. 13 (1999) 5–24.
[24] S. Bellman, E.J. Johnson, S.J. Kobrin, G.L. Lohse, International differences in information privacy concerns: a global survey of consumers, Inf. Soc. 20 (2004) 313–324.
[25] H. Xu, T. Dinev, J. Smith, P. Hart, Information privacy concerns: linking individual perceptions with institutional privacy assurances, J. Assoc. Inf. Syst. 12 (2011) 798–824.
[26] H. Xu, H.-H. Teo, B.C. Tan, R. Agarwal, Research note—effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: a study of location-based services, Inf. Syst. Res. 23 (2012) 1342–1363.
[27] H.R. Nemati, T. Van Dyke, Do privacy statements really work? The effect of privacy statements and fair information practices on trust and perceived risk in e-commerce, Int. J. Inf. Secur. Priv. 3 (2009) 45–64.
[28] C. Liu, J.T. Marchewka, J. Lu, C.-S. Yu, Beyond concern: a privacy-–trust–behavioral intention model of electronic commerce, Inf. Manag. 42 (2004) 127–142.
[29] N.F. Awad, M.S. Krishnan, The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization, Mis Q. 30 (2006) 13–28.
[30] R.K. Chellappa, P.A. Pavlou, Perceived information security, financial liability and consumer trust in electronic commerce transactions, Logist. Inf. Manag. 15 (2002) 358–368.
[31] H. Li, R. Sarathy, H. Xu, Understanding situational online information disclosure as a privacy calculus, J. Comput. Inf. Syst. 51 (2010) 62–71.
[32] G.R. Milne, A.J. Rohm, Consumer privacy and name removal across direct marketing channels: exploring opt-in and opt-out alternatives, J. Public Policy Mark. 19 (2000) 238–249.
[33] L. Brandimarte, A. Acquisti, G. Loewenstein, Misplaced confidences: privacy and the control paradox, Soc. Psychol. Personal. Sci. 4 (2013) 340–347.
[34] E. Kim, C.F. Libaque-Saenz, M.-C. Park, Understanding shopping routes of offline purchasers: selection of search-channels (online vs. offline) and search-platforms (mobile vs. PC) based on product types, Service Business (2018) 1–34.
[35] M. Hiltunen, M. Laukka, J. Luomala, Mobile User Experience, IT press, Edita, Finland, 2002.
[36] M. Chae, J. Kim, What's so different about the mobile Internet? Commun. ACM 46 (2003) 240–247.
[37] R.T. Watson, L.F. Pitt, P. Berthon, G.M. Zinkhan, U-commerce: expanding the universe of marketing, J. Acad. Mark. Sci. 30 (2002) 333–347.
[38] P. Kannan, A.-M. Chang, A.B. Whinston, Wireless commerce: marketing issues and possibilities, Proceedings of the 34th Annual Hawaii International Conference on System Sciences, IEEE, 2001, p. 6.
[39] H. Chen, R.H. Chiang, V.C. Storey, Business intelligence and analytics: from big data to big impact, Mis Q. 36 (2012) 1165–1188.
[40] A. Ghose, TAP: Unlocking the Mobile Economy, MIT Press, 2017.
[41] J. Phelps, G. Nowak, E. Ferrell, Privacy concerns and consumer willingness to provide personal information, J. Public Policy Mark. 19 (2000) 27–41.
[42] AV-Comparatives, IT Security Survey 2019, (2019).
[43] T. Dinev, P. Hart, An extended privacy calculus model for e-commerce transactions, Inf. Syst. Res. 17 (2006) 61–80.
[44] L. Ashworth, C. Free, Marketing dataveillance and digital privacy: using theories of justice to understand consumers' online privacy concerns, J. Bus. Ethics 67 (2006) 107–123.
[45] S. Stieger, C. Burger, M. Bohn, M. Voracek, Who commits virtual identity suicide? Differences in privacy concerns, Internet addiction, and personality between Facebook users and quitters, Cyberpsychol. Behav. Soc. Netw. 16 (2013) 629–634.
[46] M. Miller, Facebook May Soon Be Tracking You at All Times, Forbes, 2013.
[47] B. Hernandez, Virtual Identity Suicide' vs. Facebook, NBC Bay Area, 2013.
[48] H. Zo, Personalization vs. Customization: which is more effective in e-services? Proceedings of the 9th Americas Conference on Information Systems (AMCIS 2003), Tampa, FL, 2003.
[49] H. Sheng, F.F.-H. Nah, K. Siau, An experimental study on ubiquitous commerce adoption: impact of personalization and privacy concerns, J. Assoc. Inf. Syst. 9 (2008) 344–376.
[50] H. Xu, X.R. Luo, J.M. Carroll, M.B. Rosson, The personalization privacy paradox: an exploratory study of decision making process for location-aware marketing, Decis. Support Syst. 51 (2011) 42–52.
[51] J. Sutanto, E. Palme, C.-H. Tan, C.W. Phang, Addressing the personalization-privacy paradox: an empirical assessment from a field experiment on smartphone users, Mis Q. 37 (2013) 1141–1164.
[52] A. Proia, D. Simshaw, K. Hauser, Consumer cloud robotics and the fair information practice principles: recognizing the challenges and opportunities ahead, Minn. JL

Sci. & Tech. 16 (2015) 145.
[53] R. Gellman, Fair Information Practices: a Basic History, Available at SSRN 2415020 (2017).
[54] C. Tankard, What the GDPR means for businesses, Netw. Secur. 2016 (2016) 5–8.
[55] S. Wachter, Normative challenges of identification in the Internet of Things: privacy, profiling, discrimination, and the GDPR, Comput. Law Secur. Rep. 34 (2018) 436–449.
[56] E. Commission, Data Protection - Rules for the Protection of Personal Data Inside and Outside the EU, E. Commission (Ed.), (2018).
[57] J.K. Serrato, C. Cwanlina, A. Rudawski, T. Coughlin, K. Fardelmann, US States Pass Data Protection Laws on the Heels of the GDPR, in: Data Protection Report, Norton Rose Fulbright, Norton Rose Fulbright, 2018.
[58] P.G. Patel, N.D. Taylor, A.E. Laks, The 2018 California consumer privacy act: California scraps ballot initiative and passes sweeping data privacy regulation, Morrison & Foerster LLP, Morrison & Foerster LLP, 2018.
[59] CCPA, About the California Consumer Privacy Act, in: CAPrivacy.org (Ed.), CAPrivacy.org., 2018.
[60] K. Patrick, States and cities turn away from Federal tech policy, Government Technology, Government Technology, (2018) online.
[61] M. Ramey, Brazil's New General Data Privacy Law Follows GDPR Provisions, in, Covington, insideprivacy.com, 2018.
[62] S. Balaji, India Finally Has a Data Privacy Framework – What Does It Mean for Its Billion-dollar Tech Industry? Forbes, Forbes, Forbes online, 2018.
[63] OAIC, Notifiable Data Breaches scheme, A.I.C. (OAIC) (Ed.), (2018).
[64] M. Evans, UK government guidance on continued EU-UK data flows upon a no deal brexit, Data Protection Report, Norton Rose Fulbright, 2018.
[65] N.K. Malhotra, S.S. Kim, J. Agarwal, Internet users' information privacy concerns (IUIPC): the construct, the scale, and a causal model, Inf. Syst. Res. 15 (2004) 336–355.
[66] P. Harris, Sufficient grounds for optimism? The relationship between perceived controllability and optimistic bias, J. Soc. Clin. Psychol. 15 (1996) 9–52.
[67] V.H. Vroom, Work and Motivation, Wiley, New York, NY, 1964.
[68] W.M. Klein, Z. Kunda, Exaggerated self-assessments and the preference for controllable risks, Organ. Behav. Hum. Decis. Process. 59 (1994) 410–427.
[69] N.D. Weinstein, Why it won't happen to me: perceptions of risk factors and susceptibility, Health Psychol. 3 (1984) 431–457.
[70] I. Ajzen, M. Fishbein, Understanding Attitudes and Predicting Social Behaviour, Prentice-Hall, Englewood Cliffs, NJ, 1980.
[71] M. Workman, A test of interventions for security threats from social engineering, Inf. Manag. Comput. Secur. 16 (2008) 463–483.
[72] M. Workman, W.H. Bommer, D. Straub, Security lapses and the omission of information security measures: a threat control model and empirical test, Comput. Human Behav. 24 (2008) 2799–2816.
[73] D.W. Straub, R.J. Welke, Coping with systems risk: security planning models for management decision making, Mis Q. (1998) 441–469.
[74] V. Pupavac, Therapeutic governance: psycho-social intervention and trauma risk management, Disasters 25 (2001) 358–372.
[75] S. Milne, P. Sheeran, S. Orbell, Prediction and intervention in health-related behavior: a meta-analytic review of protection motivation theory, J. Appl. Soc. Psychol. 30 (2000) 106–143.
[76] G. Midgley, Systemic intervention, Systemic Intervention, Springer, 2000, pp. 113–133.
[77] Y. Chang, S.F. Wong, C.F. Libaque-Saenz, H. Lee, The role of privacy policy on consumers' perceived privacy, Gov. Inf. Q. 35 (2018) 445–459.
[78] K.-W. Wu, S.Y. Huang, D.C. Yen, I. Popova, The effect of online privacy policy on consumer privacy concern and trust, Comput. Human Behav. 28 (2012) 889–897.
[79] J. Angwin, J. Valentino-Devries, Apple, Google collect user data, The Wall Street Journal (2011).
[80] F. Bélanger, R.E. Crossler, Privacy in the digital age: a review of information privacy research in information systems, Mis Q. 35 (2011) 1017–1042.
[81] T. Donaldson, T.W. Dunfee, Toward a unified conception of business ethics: integrative social contracts theory, Acad. Manag. Rev. 19 (1994) 252–284.
[82] B. Suh, I. Han, The impact of customer trust and perception of security control on the acceptance of electronic commerce, Int. J. Electron. Commer. 7 (2003) 135–161.
[83] A. Bandura, Social cognitive theory: an agentic perspective, Annu. Rev. Psychol. 52 (2001) 1–26.
[84] H. Xu, The effects of self-construal and perceived control on privacy concerns, Proceedings of the 28th Annual International Conference on Information Systems (ICIS 2007), Montréal, Canada, 2007.
[85] A.F. Westin, Privacy and Freedom, Atheneum, New York, NY, 1967.
[86] M. Ohkubo, K. Suzuki, S. Kinoshita, RFID privacy issues and technical challenges, Commun. ACM 48 (2005) 66–71.
[87] S. Yamaguchi, Culture and control orientations, in: D. Matsumoto (Ed.), The Handbook of Culture and Psychology, Oxford University Press, New York, 2001, pp. 223–243.
[88] I.A. Junglas, N.A. Johnson, C. Spitzmüller, Personality traits and concern for privacy: an empirical study in the context of location-based services, Eur. J. Inf. Syst. 17 (2008) 387–402.
[89] T.K. Das, B.-S. Teng, Trust, control, and risk in strategic alliances: an integrated framework, Organ. Stud. 22 (2001) 251–283.
[90] Y. Li, Empirical studies on online information privacy concerns: literature review and an integrative framework, Commun. Assoc. Inf. Syst. 28 (2011) 453–496.
[91] M.J. Metzger, Communication privacy management in electronic commerce, J. Comput. Commun. 12 (2007) 335–361.
[92] S.S. Petronio, Boundaries of Privacy: Dialectics of Disclosure, Suny Press, Albany, NY, 2002.
[93] H.-S. Choi, Hackers Steal 12m KT Users' Information, The Korea Herald, 2014.
[94] M. Janssen, N. Helbig, Innovating and Changing the Policy-cycle: Policy-makers Be Prepared, Government Information Quarterly, 2016.
[95] M.-C. Lee, Factors influencing the adoption of Internet banking: an integration of TAM and TPB with perceived risk and perceived benefit, Electron. Commer. Res. Appl. 8 (2009) 130–141.
[96] P.A. Pavlou, Consumer acceptance of electronic commerce: integrating trust and risk with the technology acceptance model, Int. J. Electron. Commer. 7 (2003) 101–134.
[97] C. Van Slyke, J. Shim, R. Johnson, J.J. Jiang, Concern for information privacy and online consumer purchasing, J. Assoc. Inf. Syst. 7 (2006) 415–444.
[98] B. Erdogan, Antecedents and consequences of justice perceptions in performance appraisals, Hum. Resour. Manag. Rev. 12 (2002) 555–578.
[99] R. Vaidyanathan, P. Aggarwal, Who is the fairest of them all? An attributional approach to price fairness perceptions, J. Bus. Res. 56 (2003) 453–463.
[100] R.M. Chory-Assad, Classroom justice: perceptions of fairness as a predictor of student motivation, learning, and aggression, Commun. Q. 50 (2002) 58–77.
[101] G. Camponovo, S. Debetaz, Y. Pigneur, A comparative analysis of published scenarios for m-business, Proceedings of the 3rd International Conference on Mobile Business (ICMB 2004), New York, NY, 2004.
[102] J.L. Huang, P.G. Curran, J. Keeney, E.M. Poposki, R.P. DeShon, Detecting and deterring insufficient effort responding to surveys, J. Bus. Psychol. 27 (2012) 99–114.
[103] J. Kirk, Age Gap Hampers Technology Adoption, InfoWorld, 2006.
[104] J.F. Hair, C.M. Ringle, M. Sarstedt, Editorial-partial least squares structural equation modeling: rigorous applications, better results and higher acceptance, Long Range Plann. 46 (2013) 1–12.
[105] A.N. Joinson, C. Paine, T. Buchanan, U.-D. Reips, Watching me, watching you: privacy attitudes and reactions to identity card implementation scenarios in the United Kingdom, J. Inf. Sci. 32 (2006) 334–343.
[106] R.K. Chellappa, R.G. Sin, Personalization versus privacy: an empirical examination of the online consumer's dilemma, Inf. Technol. Manag. 6 (2005) 181–202.
[107] T. Ravichandran, C. Lertwongsatien, C. Lertwongsatien, Effect of information systems resources and capabilities on firm performance: a resource-based perspective, J. Manag. Inf. Syst. 21 (2005) 237–276.
[108] D.H. McKnight, V. Choudhury, C. Kacmar, Developing and validating trust measures for e-commerce: an integrative typology, Inf. Syst. Res. 13 (2002) 334–359.
[109] C.M. Ringle, S. Wende, J.-M. Becker, SmartPLS 3, Boenningstedt: SmartPLS GmbH, (2015) . http://www.smartpls.com.
[110] W.W. Chin, The partial least squares approach for structural equation modeling, in: G.A. Marcoulides (Ed.), Ed.) Modern Methods for Business Research, Lawrence Erlbaum Associates, Mahwah, NJ, 1998, pp. 295–336.
[111] J.F. Hair, M. Sarstedt, C.M. Ringle, J.A. Mena, An assessment of the use of partial least squares structural equation modeling in marketing research, J. Acad. Mark. Sci. 40 (2012) 414–433.
[112] J.F. Hair, C.M. Ringle, M. Sarstedt, PLS-SEM: Indeed a silver bullet, J. Mark. Theory Pract. 19 (2011) 139–152.
[113] M.K. Lindell, D.J. Whitney, Accounting for common method variance in cross-sectional research designs, J. Appl. Psychol. 86 (2001) 114.
[114] P.M. Podsakoff, D.W. Organ, Self-reports in organizational research: problems and prospects, J. Manage. 12 (1986) 531–544.
[115] C.M. Fuller, M.J. Simmering, G. Atinc, Y. Atinc, B.J. Babin, Common methods variance detection in business research, J. Bus. Res. 69 (2016) 3192–3198.
[116] J.C. Numally, Psychometric Theory, McGraw-Hill, New York, NY, 1978.
[117] X. Hu, Z. Lin, A.B. Whinston, H. Zhang, Hope or hype: on the viability of escrow services as trusted third parties in online auction environments, Inf. Syst. Res. 15 (2004) 236–249.
[118] D. Gefen, D. Straub, A practical guide to factorial validity using PLS-Graph: tutorial and annotated example, Commun. Assoc. Inf. Syst. 16 (2005) 91–109.
[119] B. Hultén, Customer segmentation: the concepts of trust, commitment and relationships, Journal of Targeting, Measur. Analys. Mark. 15 (2007) 256–269.
[120] R.B. Kline, Principles and Practice of Structural Equation Modeling, Guilford Press, New York, NY, 2011.
[121] A.H. Gold, A. Malhotra, A.H. Segars, Knowledge management: an organizational capabilities perspective, J. Manag. Inf. Syst. 18 (2001) 185–214.
[122] J. Cohen, Statistical Power Analysis for the Behavioral Sciencies, Lawrence Erlbaum Associates, Hillsdale, NJ, 1988.
[123] J. Henseler, G. Hubona, P.A. Ray, Using PLS path modeling in new technology research: updated guidelines, Ind. Manag. Data Syst. 116 (2016) 2–20.
[124] X. Zhao, J.G. Lynch Jr., Q. Chen, Reconsidering Baron and Kenny: Myths and truths about mediation analysis, J. Consum. Res. 37 (2010) 197–206.
[125] D.-H. Shin, Demystifying big data: anatomy of big data developmental process, Telecomm. Policy 40 (2016) 837–854.
[126] R. Glazer, Marketing in an information-intensive environment: strategic implications of knowledge as an asset, J. Mark. 55 (1991) 1–19.
[127] M.S. Featherman, P.A. Pavlou, Predicting e-services adoption: a perceived risk facets perspective, Int. J. Hum. Stud. 59 (2003) 451–474.
[128] H. Cha, Factors influencing the adoption of location-based smartphone applications: an application of the privacy calculus model, Asia Pacific J. Inf. Syst. 22 (2012) 7–29.
[129] C. Martins, T. Oliveira, A. Popovič, Understanding the Internet banking adoption: a unified theory of acceptance and use of technology and perceived risk application, Int. J. Inf. Manage. 34 (2014) 1–13.
[130] Z.R. Steelman, B.I. Hammer, M. Limayem, Data collection in the digital age: innovative alternatives to student samples, Mis Q. 38 (2014) 355–378.

[131] P.G. Ipeirotis, F. Provost, J. Wang, Quality management on amazon mechanical turk, Proceedings of the ACM SIGKDD Workshop on Human Computation (KDD-HCOMP 2010), Washington DC, WA, 2010.
[132] P.B. Lowry, J. D'Arcy, B. Hammer, G.D. Moody, 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, J. Strateg. Inf. Syst. 25 (2016) 232–240.
[133] K.B. Sheehan, Toward a typology of Internet users and online privacy concerns, Inf. Soc. 18 (2002) 21–32.
[134] H.J. Smith, S.J. Milberg, S.J. Burke, Information privacy: measuring individuals' concerns about organizational practices, Mis Q. 20 (1996) 167–196.
[135] H. Xu, T. Dinev, J. Smith, P. Hart, Information privacy concerns: linking individual perceptions with institutional privacy assurances, J. Assoc. Inf. Syst. 12 (2011) 1.

Christian Fernando Libaque-Saenz (cf.libaques@up.edu.pe) is an associate professor and the head of the Engineering Department at Universidad del Pacífico (Peru). Christian has received his B.S. degree in Telecommunications Engineering from the National University of Engineering (Peru), and his M.A. and Ph.D. degrees in Information and Telecommunication Technology from the Korea Advanced Institute of Science and Technology (KAIST). Before starting his studies at KAIST, Christian worked for the Peruvian Ministry of Transport and Communications. Christian's research interests include digital divide, privacy, ICT strategy, human-computer interaction, and spectrum management. His publications have appeared in journals such as the Government Information Quarterly, Telecommunications Policy, Behaviour and Information Technology, Telematics and Informatics, Telecommunication Systems as well as in international conferences.

Siew Fan Wong (siewfanw@sunway.edu.my) is an adjunct professor with Sunway University, Malaysia. She received her Ph.D. degree in MIS from the University of Houston, Texas. Her research interests involve organizational IT strategy, information privacy, business analytics, and technology addiction. Her publications have appeared in journals such as the Information & Management, Journal of Global Information Management, International Journal of Information Management, Government Information Quarterly, Industrial Management & Data Systems, and Cyberpsychology, Behavior, and Social Networking.

Younghoon Chang (younghoonchang@bit.edu.cn) is an associate professor in the School of Management and Economics at Beijing Institute of Technology, Beijing, China. He received his Ph.D. degree in Business & Technology Management from Korea Advanced Institute of Science and Technology (KAIST), South Korea. His research interests include Information privacy, AI and robot management, e-business, business analytics, and digital health. His articles have appeared in the Information & Management, Information Systems Frontiers, Government Information Quarterly, Telecommunications Policy, Journal of Global Information Management, Behavior and Information Technology, Industrial Management & Data Systems as well as in the proceedings of international conferences. He is currently serving as an associate editor of Asia Pacific Journal of Information Systems, and an editorial review board member of Journal of Computer Information Systems and Industrial Management and Data Systems.

Edgardo R. Bravo (er.bravoo@up.edu.pe) is currently an associate professor in the Engineering Department at Universidad del Pacifico (Peru). He received his Ph.D. in Management Sciences from ESADE (Spain), his MBA from ESAN-University (Peru), and his B.S. in Systems Engineering from National University of Engineering (Peru). His research interests are human-computer interaction, digital divide, privacy, and social networks. He has published in Behavior & Information Technology, Information Technology & People, Cognition, Technology & Work, Energies, and top international conferences. He has managed diverse areas in public and private organizations for more than eighteen years. Also, he has been a consultant for international agencies.