Government Information Quarterly xxx (xxxx) xxx–xxx

Contents lists available at ScienceDirect

Government Information Quarterly

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

The role of privacy policy on consumers' perceived privacy

Younghoon Chang[a], Siew Fan Wong[b], Christian Fernando Libaque-Saenz[c], Hwansoo Lee[d,*]

[a] School of Management and Economics, Beijing Institute of Technology, China
[b] Department of Computing and Information Systems, Sunway University, Malaysia
[c] Department of Engineering, Universidad del Pacífico, Peru
[d] Department of Convergence Security, Dankook University, Republic of Korea

ARTICLE INFO

Keywords:
Privacy boundary management model
Privacy policy
Perceived privacy
Perceived effectiveness
Fair information practices
Trust
Privacy concerns

ABSTRACT

With today's big data and analytics capability, access to consumer data provides competitive advantage. Analysis of consumers' transactional data helps organizations to understand customer behaviors and preferences. However, prior to capitalizing on the data, organizations ought to have effective plans for addressing consumers' privacy concerns because violation of consumer privacy brings long-term reputational damage. This paper proposes and tests a Privacy Boundary Management Model, explaining how consumers formulate and manage their privacy boundary. It also analyzes the effect of the five dimensions of privacy policy (Fair Information Practices) on privacy boundary formation to assess how customers link these dimensions to the effectiveness of privacy policy. Survey data was collected from 363 customers who have used online banking websites for a minimum of six months. Partial Least Square results showed that the validated research model accounts for high variance in perceived privacy. Four elements of the Fair Information Practice Principles (access, notice, security, and enforcement) have significant impact on perceived effectiveness of privacy policy. Perceived effectiveness in turn significantly influences perceived privacy control and perceived privacy risk. Perceived privacy control significantly influences trust and perceived privacy. Perceived privacy concern and trust also significantly influence perceived privacy.

1. Introduction

We live in the era of big data that dramatically transforms the way we make decisions (Janssen, van der Voort, & Wahyudi, 2017). Big data is the "data sets whose size is beyond the ability of typical database software tools to capture, store, manage, and analyze" (Manyika, Chui, Brown et al., 2011). New information and communication technologies (ICTs) have enabled the big data trend by providing the capability to capture and store huge amounts of consumer data which serves as the core of the big data trend (Chen, Chiang, & Storey, 2012). When properly collected, stored, and processed, consumer data may allow organizations to understand customer behaviors and preferences. Such knowledge is valuable in customizing and personalizing products and services to meet customer needs, thereby equipping companies with a competitive advantage (Erevelles, Fukawa, & Swayne, 2016).

While businesses are eager to access customer data, privacy factor remains the most salient issue that must be solved before organizations could capitalize on the value of a data-centric service economy (Janssen & van den Hoven, 2015; TRUSTe, 2011). Given that each piece of data leaves behind electronic trails of customer activities, individuals are concerned about how companies collect and use their private information (Janssen & Kuk, 2016; Morey, Forbath, & Schoop, 2015) This situation, together with the increasing number of online information leaks, heightens customers' privacy concerns toward information risk (Drinkwater, 2016). Therefore, it is important that companies are aware and capable of handling the risks because they could pose long-term damaging effects on companies as well as cause economic losses (Culnan, 1993).

The risks have led governments to enact privacy regulations and policies (e.g., European Directive EC 95/461995 and United States Federal Trade Commission (FTC)'s Fair Information Practice Principles (FIPPs)) to protect people from potential harmful acts. Companies must comply with these regulations and devise effective privacy management strategies to address privacy issues. This would require knowledge of how people make decisions about revealing and concealing private information.

Petronio (2012)'s communication privacy management (CPM) theory used a boundary metaphor to explain how people make decisions about revealing and concealing information, which is known as 'privacy boundary formation.' In impersonal contexts such as those

* Corresponding author.
E-mail addresses: cf.libaques@up.edu.pe (C.F. Libaque-Saenz), hanslee992@gmail.com (H. Lee).

https://doi.org/10.1016/j.giq.2018.04.002
Received 28 June 2017; Received in revised form 23 April 2018; Accepted 23 April 2018

between customers and companies, the form by which companies use customer data (i.e., organizational information practices) is salient to the formation of an individual's privacy boundary (Dinev, Xu, Smith, & Hart, 2013; Metzger, 2007). In the process of forming privacy boundary, consumers also reference their governments' privacy regulations (Xu, Dinev, Smith, & Hart, 2011).

Weighing the interplay among consumers' privacy boundary formation, organizations' information practices, and government's regulations as well as the current findings in the literature, we realize that there are gaps that have to be addressed so that a better understanding of consumers' privacy boundary formation can be achieved. First, previous research has not fully examined the effect of government's privacy policy. In fact, these studies are either considering only some of the dimensions (e.g., Libaque-Saenz, Chang, Kim, Park, & Rho, 2016; Libaque-Saenz, Chang, Wong, & Lee, 2015; Libaque-Saenz, Wong, Chang, Ha, & Park, 2016) or have not even delved into its specific dimensions at all (e.g., Xu et al., 2011; Xu, Teo, Tan, & Agarwal, 2012). Since each principle of the privacy regulations may have different effect, organizations need to determine which is exerting stronger impact on individuals' decisions in order to draw adequate strategies (Schwaig, Kane, & Storey, 2006),

Second, while prior research has focused on various dependent variables such as privacy concerns, intrinsic motivation, trust, information sensitivity, intention to disclose personal information and compliance intention (e.g., Bansal, Zahedi, & Gefen, 2010; Dinev & Hart, 2006a; Joinson, Reips, Buchanan, & Schofield, 2010; Lee, Lim, Kim, Zo, & Ciganek, 2015; Lowry, Cao, & Everard, 2011; Tsai, Egelman, Cranor, & Acquisti, 2011), it has not placed the complete organizational information practices within the recursive and wholeness view of privacy boundary formation model to explore their effect in the online context. Recognizing this gap, researchers (e.g., Bansal & Gefen, 2015; Dinev et al., 2013; Kehr, Kowatsch, Wentzel, & Fleisch, 2015) have called for scholars to further explore online privacy boundary formation and rationality.

Our research aims to fill these two research gaps by proposing and empirically testing a Privacy Boundary Management Model (PBMM) that is grounded on Petronio (2012)'s Communication Privacy Management Theory, Higgins (1997)'s Regulatory Focus Theory and Xu et al. (2011)'s application of CPM in the context of information privacy to provide a complete view of customers' privacy boundary management process. We collected the data from bank customers in Malaysia who are using online banking services because the banking sector contains a wealth of sensitive private information that many consumers would be reluctant to disclose to third parties. Therefore, we expect these consumers to act more conservatively as regards the sharing and disclosure of their banking data.

The rest of the paper is structured as follows. Section 2 reviews the theoretical background and section 3 discusses the research model and the hypotheses. Section 4 describes the research method while section 5 discusses the results. Section 6 provides the discussion, implications, research limitations, future research, and concluding remarks.

2. Theoretical background

2.1. Online banking

Online banking refers to the use of banking services through the Internet (Yiu, Grant, & Edgar, 2007). Although it started as a channel to present information, this technology has evolved and nowadays allows customers to perform various transactions such as paying bills, transferring money, and checking account balances through the bank's website. The use of this technology has expanded worldwide due to its cost savings and convenience (Pikkarainen, Pikkarainen, Karjaluoto, & Pahnila, 2004). As a result, banks have enlarged their customer databases and they could benefit from the analysis of these data to launch personalized marketing campaigns and innovative services in order to maintain a competitive advantage.

However, there are also challenges in using customer data in the online banking context. Apart from technical challenges such as the techniques and technology requirements to handle this massive amount of data (Sun, Morris, Xu, Zhu, & Xie, 2014), privacy concerns may also represent a barrier. In the context of online banking, individuals and banks interact by exchanging not only monetary resources but also information such as the identity of the user, bank account status, transfers, and payments. These sensitive information may raise individuals' concerns about potential threats. Whereas, the occurrence of any online information leak may represent serious problems to banks because as a highly regulated market as it is, banks must comply with current regulation on personal data protection. Accordingly, individuals' assessment on how banks handle their information becomes important in this domain.

2.2. Communication privacy management theory

Petronio (2002)'s Communication Privacy Management Theory (CPM) is a communication theory that encompasses the way in which confidants handle disclosed information. CPM argues that individuals have a dynamic boundary to maintain their privacy, and they manage the boundary by their own rules (Baruh, Secinti, & Cemalcilar, 2017; Sutanto, Palme, Tan, & Phang, 2013). In the context of online banking, individuals and banks interact by exchanging not only monetary resources but also information such as the identity of the user, bank account status, transfers, and payments. This sensitive information may raise individuals' concerns about potential threats. Accordingly, individuals' assessment on how banks handle their information becomes important in this domain. Hence, CPM is appropriate for our research.

CPM uses a boundary metaphor to explain how people as data owners make decisions about revealing and concealing private information (Petronio, 2012). An individual's privacy boundary encompasses information that only he/she has, but others do not know. This privacy boundary is built on people's belief that they own their private information and therefore want to maintain control of what, when, and with whom it is shared. Information within a personal boundary is considered private and is not disclosed to others. When private information is accessible to only one individual, the boundary is considered thick because there is less possibility for the information to be leaked to the public. Once private information is shared with another party, the boundary becomes thin and permeable, which increases the possibility of information becoming public.

Accordingly, CPM posits five core principles: 1) people believe they own and have a right to control their private information; 2) people control this information through the use of personal privacy rules; 3) when others are given access to a person's private information, they become co-owners of that information; 4) co-owners of private information need to negotiate mutually agreeable privacy rules; and 5) when co-owners of private information do not effectively negotiate and follow mutually held privacy rules, turbulence ensues (Petronio, 2002).

The first principle is consistent with Westin's (1967) definition of information privacy as “the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.” According to this principle, when individuals decide to disclose personal information, they assess the level of privacy they have at the time the assessment is made (Xu et al., 2011).

The second principle highlights CPM as a rule-based theory. Under this rule-based approach, CPM attempts to focus on the factors driving individuals' privacy boundary decisions. CPM posits that those factors are cost/benefit ratios, context, culture, motivation, and gender. As theorized by Xu et al. (2011), risk and control represent two important concepts that individuals assess to balance the costs and benefits involved in privacy disclosure. Depending on the assessment outcome, individuals determine how much control they have toward the

information contained within their privacy boundary, and decide if the level of control is acceptable or unacceptable (Xu et al., 2011). If acceptable, they will perceive the opening of the boundary as less risky and have higher likelihood of disclosing private information (Xu et al., 2011). Otherwise, they will close the boundary to prevent risky information sharing. In the case of context, Petronio (2002) suggested that the establishment of privacy rules vary across specific situations and domains. Since privacy is influenced by the context in which disclosure is deemed acceptable or unacceptable, we followed prior research (e.g., Xu et al., 2011) by conceptualizing perceptions of control, risk, and privacy in a situation-specific context: online banking. On the other hand, like Xu et al. (2011), we excluded culture criterion because we focused on the link between individuals and organizations regarding privacy. As for the fourth criterion, considering that motivations to disclose personal information when using online banking may be constant due to the fixed context (e.g., make monetary transactions), this construct was also excluded from the proposed research model. In terms of gender, Petronio (2002) postulated that rule formation may vary across men's and women's perspectives. Thus, we included gender as a control variable in our research model. Finally, considering that prior research has found that young individuals are less likely to be concerned about their privacy (Sheehan, 1999), we included age as a second control variable.

According to the third principle, if users decide to disclose personal information to use online banking services, banks become co-owners of the information. However, CPM also explains that these co-owners do not necessarily perceive an equal responsibility as the users (Petronio, 2002). This statement leads us to the fourth principle: a need to coordinate privacy boundary. Sharing private information moves this information to the collective boundary where data owners and data recipients become co-owners with joint responsibility to keep the information private. Ownership conveys both rights and obligations. Co-ownership implies the beginning of collective data control and mutual boundary coordination by both data owners and data recipients. The coordination process is complex because each owner approaches the information from his/her distinct viewpoints. Therefore, understanding between the parties is needed to coordinate information ownership. The parties will negotiate a set of collectively held privacy access and protection rules. They will coordinate their expectations of whether the disclosed information should be shared, with whom it should be shared, and when it should be shared. In impersonal contexts such as those between users and online banking services, privacy policies are the basis for privacy boundary formation (Metzger, 2007).

As for the fifth principle, sometimes the boundary coordination process fails and leads to boundary turbulence (Petronio, 2012). When turbulence happens, individuals may seek recourses by complaining. For example, third party assurances such as government regulations or industrial standards may serve as resources for this task (Xu et al., 2011).

In short, CPM identifies three rule management elements—boundary coordination, boundary turbulence, and boundary rule formation—that govern how people adjust, coordinate, and manage their boundaries to maintain their privacy. Both boundary coordination and the means to address boundary turbulence are related to institutional boundary identification (i.e., privacy policy and third-party assurances). Then, this boundary identification influences individuals' rules formation for privacy boundary. In turn, rule formation stage affects individuals' assessment of privacy.

2.3. Regulatory focus theory

Higgins (1997) suggested that human beings attain their motivations and regulate their behavior in two different ways with each using different motivational focus: promotion and prevention. A promotion focus concentrates on the regulation of desired positive outcomes such as successful attainment of desired goals and aspirations. A prevention focus stresses security and responsibilities that highlight avoidance-related behaviors on negative outcomes. An individual's regulatory focus can be influenced by relational and situational factors (Higgins, 1997; Wirtz & Lwin, 2009). Typically, individuals learn from their interactions with others on how to regulate their relationships in a certain situation to promote desirable outcomes and prevent undesirable outcomes.

Many scholars from different disciplines have adopted Regulatory Focus Theory (RFT) to study human motivation and behavior (Baas, De Dreu, & Nijstad, 2008). In privacy research, Wirtz and Lwin (2009) used the theory to explain consumers' response behaviors in online shopping environment. They argued that trust is promotion-focused behavior and privacy concern is a prevention-focused behavior and found that trust and privacy concerns mediates the relationship between perception of organizational practices and consumers' response behaviors. They further contended that RFT can shed light on privacy research to understand negative and defensive reactions as well as positive and cooperative behaviors (Lwin, Wirtz, & Williams, 2007; Wirtz & Lwin, 2009).

2.4. Privacy boundary management model (PBMM)

Based on the CPM and RFT theories, we proposed a privacy boundary management model (Fig. 3). Privacy boundary management refers to an individual's privacy management process that allows the individual to control who can possess and access their personal information as well as set the rules for co-ownership of their information after they disclose to third parties (Petronio, 2002). An individual's privacy boundary management follows a four-phase process, starting from institutional boundary identification — coordination, turbulence, and assurance — to boundary rule formation, boundary self-regulation, and finally to individual boundary decision. This process is recursive and iterative, where individuals constantly adjust their privacy boundary based on the latest experience and information gathered (Mattson & Brann, 2002). A decision to open up a boundary today could be replaced with an opposite choice to close the boundary in another situation.

In the institutional boundary identification phase, individuals decide on an organization's effectiveness in implementing its existing privacy policy. This phase forms the foundation for the subsequent two phases. U.S. FTC's FIPPs are commonly referenced in the literature as the basis for privacy policies (Culnan & Armstrong, 1999; Wu, Huang, Yen, & Popova, 2012). As the FIPPs focus on core privacy principles, it is less comprehensive in scope than other practices of OECD or EU (Boritz & No, 2009). However, the FIPPs are a set of internationally recognized practices for individuals' information privacy, and have provided the underlying policy for many countries including Malaysia (Gellman, 2017). The FIPPs are made up of five dimensions: notice, choice, access, security, and enforcement. Notice refers to the disclosure of an organization's information policies before any personal information is collected (Liu, Marchewka, Lu, & Yu, 2005). As for the choice dimension, it refers to providing customers with the option of selecting which personal information collected may be used and how it will be used (Liu et al., 2005). Access is the possibility of customers accessing their stored personal information to view and check for data accuracy and completeness (Wu et al., 2012). In the case of the security dimension, it refers to the assurances for keeping the data accurate and secure in order to ensure data integrity (Liu et al., 2005; Wu et al., 2012). Finally, enforcement is the administration and prosecution of privacy policy by organizations (Karyda, 2009) (Fig. 1).

We argued that three processes take place during the institutional boundary identification phase: boundary coordination, boundary turbulence, and boundary assurance. Indeed, Xu et al. (2012) theorized that individuals' perceptions related to boundary coordination and boundary turbulence are the basis for their assessment of boundary assurance (i.e., effectiveness of privacy policy).

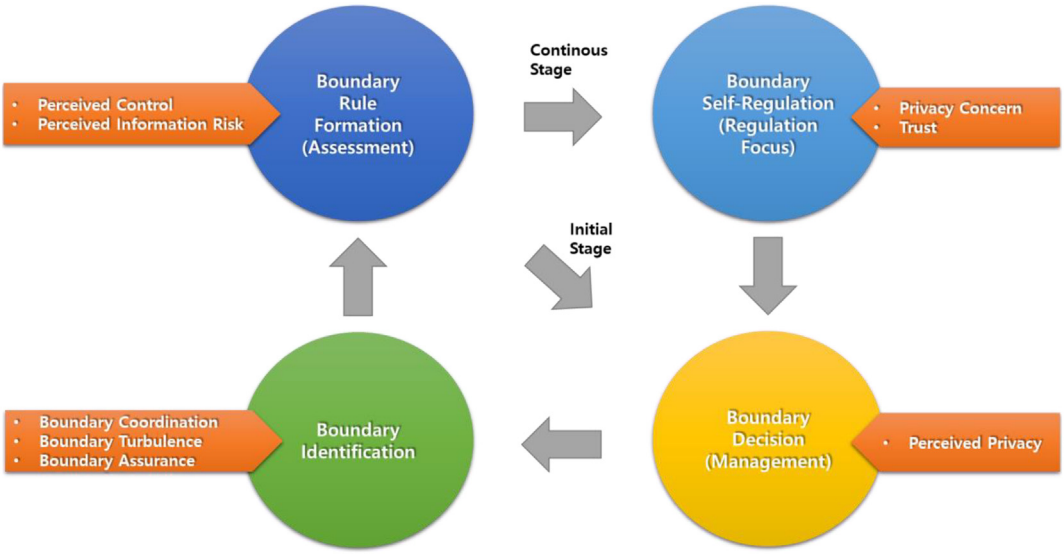

Fig. 1. The recursive model of privacy boundary management.

Notice, choice, and access dimensions are clearly related to boundary coordination. These three dimensions provided by organizations determine how individuals organize their privacy boundary. They are the means through which users and companies may agree on the way personal information will be used (i.e., boundary coordination). When undesirable incidents happen, boundary turbulence mode kicks in where consumers reference the security measures of an organization, and the enforcement avenues to protect their private data. The interplay between boundary coordination and boundary turbulence will determine boundary assurance, where consumers form an opinion toward the effectiveness of an organization's privacy policy (Xu et al., 2011).

With perceived effectiveness of privacy policy being formed, consumers move to the mutual boundary rule formation phase. Here, consumers compare the privacy boundary practiced in an organization with their own inherent need for privacy protection. Accordingly, they perform a risk-control calculation to determine how much control they have over the use of their data and how much risk they assume in information disclosure. Once the risk-control assessment is done, an individual's privacy boundary rule is formed.

Finally, consumers move to the boundary decision phase. Using the boundary rule formed in the previous phase, consumers reach a self-assessed state of perceived privacy. Perceived privacy refers to “an individual's self-assessed state in which external agents have limited access to information about himself or herself” (Dinev et al., 2013, p. 299). The initial perceived privacy may be shaped and reshaped over time. Continuous engagement and interaction with an organization requires two attitudinal and relational factors which are trust and privacy concerns (Paul A. Pavlou, 2003; Xu et al., 2011). We treated trust and privacy concerns as the boundary self-regulations. The two factors are derived from RFT and its concept of promotion and prevention focus behavior (Higgins, 1997; Wirtz & Lwin, 2009). Wirtz and Lwin (2009) emphasized that RFT can explain more about consumers' privacy responses (Fig. 2).

3. Research model

3.1. Boundary rule formation: risk-control assessment

The calculus perspective of privacy, which incorporates the interplay between risk and control (Dinev & Hart, 2006a; Dinev et al., 2013), is the most useful framework for analyzing contemporary consumer privacy concerns (Culnan & Bies, 2003). Xu et al. (2011, p. 804) defined privacy control as “a perceptual construct reflecting an individual's beliefs in his or her ability to manage the release and dissemination of personal information.” The risk-control literature posits a positive relationship between control perceptions and optimistic bias (Harris, 1996). The greater the perception of control over the outcome, the more positive the expectation about the event (Klein & Helweg-Larsen, 2002). This implies that individuals will assess the associated risk as less serious and are more willing to take risk (Brandimarte, Acquisti, & Loewenstein, 2013). The interplay between risk and control will influence individuals' perceived privacy. In information disclosure, perceived information control is defined as individuals' beliefs in their ability to manage the release and dissemination of their private data (Westin, 1967; Xu et al., 2011). When consumers feel they are in control, they tend to perceive others as having limited access to their private information (Dinev & Hart, 2006a; Dinev et al., 2013). At the same time, the lack of perceived privacy control will reduce their perceived privacy (Dinev & Hart, 2006a; Dinev et al., 2013).

H1. Perceived privacy control is positively associated with perceived privacy

On the other hand, Mayer, Davis, and Schoorman (1995) defined trust as the willingness to take risks. Therefore, lack of control may reduce individuals' trust due to their perceptions of possible opportunistic behavior by the trustee (i.e., an increase in risk perceptions). Likewise, prior research has shown that when consumers feel they are in control of their information, they tend to have higher level of trust toward the disclosure of personal information to third parties (Taddei & Contena, 2013). Liu et al. (2005) and Joinson et al. (2010) also found that the lack of perceived control reduces customers' trust toward an organization.

H2. Perceived privacy control is positively associated with trust

Perceived privacy risk is “the expectation of losses associated with the disclosure of personal information” (Xu et al., 2011, p. 804). It introduces uncertainty resulting from potential negative outcomes (Havlena & DeSarbo, 1991). The value chain of online transactions that starts from information collection to processing, dissemination, and storing, is embedded with the potential risk of data misuse and opportunistic behaviors that may result in losses for consumers. When calculating the risks of information disclosure, consumers will assess the likelihood of negative consequences and the associated severity level. If the risk level is high, consumers will perceive others as having more access to their private information and how these information will

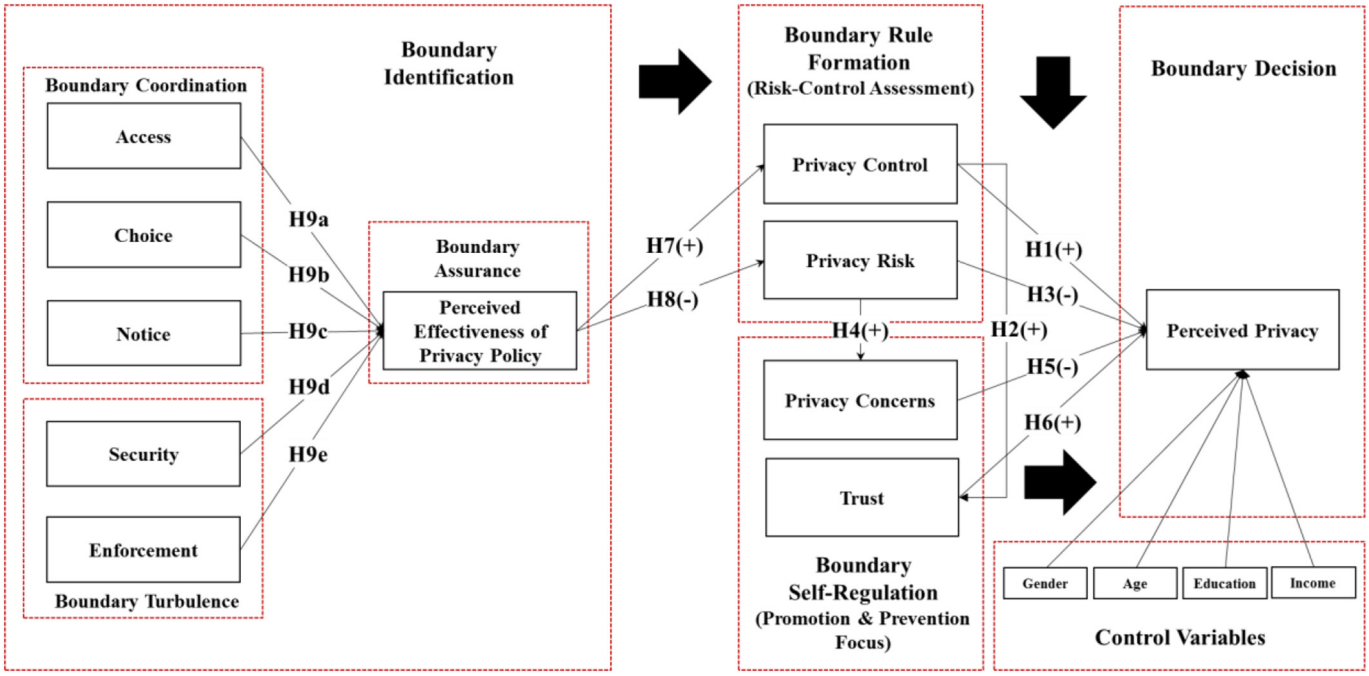

Fig. 2. The proposed privacy boundary management model.

be used (Dinev et al., 2013; Petronio, 2012). Higher sense of risk will lower their perceived privacy (Dinev et al., 2013; Petronio, 2012).

H3. Perceived privacy risk is negatively associated with perceived privacy

Privacy concern is associated with individuals' level of anxiety regarding their privacy (H. J. Smith, Milberg, & Burke, 1996). In threatening scenarios, unpleasant feelings (e.g., anxiety) tend to increase as response to risk perceptions (Dowling & Staelin, 1994). Hence, high-risk perceptions may lead individuals to have high levels of privacy concern, and vice versa for low perceptions of risk. For example, Dinev and Hart (2006a) showed that individuals' perceived risk strongly influences their perceived privacy concerns in online transactions and they contended that the relationship between perceived risk and perceived privacy concerns is a major part of privacy calculus. Xu et al. (2011) also found that perceived risk and privacy concerns are major forces that formed individuals' privacy boundary. A higher sense of risk will increase one's privacy concerns (Dinev & Hart, 2006b; Malhotra, Kim, & Agarwal, 2004; Van Slyke, Shim, Johnson, & Jiang, 2006; Xu et al., 2011).

H4. Privacy risk is positively associated with privacy concerns

3.2. Boundary self-regulation: promotion and prevention focus

Privacy concern and trust are two known proxies of perceived privacy (Dinev et al., 2013; Flavián & Guinalíu, 2006) and the mediating variables for consumer's information disclosure and response behavior (Lee et al., 2015). As mentioned in the prior hypothesis, privacy concern refers to individuals' level of anxiety regarding a third party's information practices (H. J. Smith et al., 1996). Trust in the current context is the degree to which consumers have faith and confidence in an organization's privacy practices (Bansal & Zahedi, 2008). Both privacy concern and trust are attitudinal factors indicating people's current mental state toward certain objectives (Gashami, Chang, Rho, & Park, 2016). Privacy concern is the negative mental state and trust is the positive mental state that influence the overall self-assessed state of perceived privacy (Dinev et al., 2013). Trust, in fact, refers to individuals' beliefs that trustees will act according to their expectations (Paul A Pavlou & Fygenson, 2006). Thus, as trust increases, individuals' expectations that organizations will respect their right to decide how their information will be used increase as well. Trust is especially important in the B2C IT ecosystem (Liu et al., 2005) with many research emphasize the importance of trust in information sharing and personal information disclosure (Bansal et al., 2010; Liu et al., 2005). On the other hand, according to the mood congruency effect from the Psychology literature, anxious people tend to perceive greater negativity than non-anxious people. Therefore, the higher the individuals' privacy concerns (i.e., anxiety), the higher their perceptions that organizations may not respect their right to decide about the usage of their personal information. In sum, when consumers have higher level of trust and lower level of privacy concern toward an organization, they will tend to have higher level of perceived privacy.

H5. Privacy concern is negatively associated with perceived privac.

H6. Trust is positively associated with perceived privacy.

3.3. Boundary identification: privacy policies and its perceived effectiveness

3.3.1. Boundary assurance: perceived effectiveness of privacy policy

In order to adequately protect an individual's privacy, a baseline policy framework of protection or principles is required. Privacy policies can help to build customer trust and reduce privacy concerns (Westin, 1967; Wu et al., 2012). These policies inform customers about how their personal data will be used, which indirectly tell them about the security and protection systems of the websites they use (Xu et al., 2011). Many online companies place their privacy policies on websites to reduce the customers' fears about their personal information being disclosed (Chua, Herbland, Wong, & Chang, 2017; Westin, 1967). Many current privacy policies are built around the United States Federal Trade Commission's FIPPs. The FIPPs are the prevailing global data protection principles that define the guidelines for individual rights and organizational responsibilities (Bennett, 1992; Culnan & Williams, 2009). While the implementation of the FIPPs is voluntary, its adoption provides an evaluation tool for consumers to judge an organization's information practices and its degree of responsiveness (H. J. Smith, 1993). Moreover, the FIPPs serve to assure the consumers that their

disclosed information will be safe because the receiving organization will now become the custodian of the information, and thus shoulder the responsibility of keeping the information safe and private (Petronio, 2012; Xu et al., 2011).

Previous studies have mainly discussed the impact of perceived usefulness of information systems or Internet services on privacy risk and control. From a policy point of view, perceived effectiveness of privacy policy is the concept refining perceived usefulness. The usefulness of the policy is about an assessment of whether the policy actually works well. Therefore, perceived effectiveness of privacy policy in this study means "the extent to which a consumer believes that the privacy policy notice posted online is able to provide accurate and reliable information about the firm's information privacy practices" (Xu et al., 2011, p. 806). In other words, it is the usefulness of the policy.

Previous literature found that an organization's provision of privacy notice increases the consumers' perceived privacy control (Culnan & Bies, 2003; Milne & Culnan, 2004; Xu et al., 2011). It gives assurance of security and safety. Similarly, by informing consumers about their information handling procedures, organizations also instill greater perception of confidence and procedural fairness, which reduces the perception of risk for information disclosure (Culnan & Armstrong, 1999; Xu et al., 2011). Indeed, privacy policies are mechanisms to load individuals with beliefs that companies will behave appropriately (Xu, 2007).

H7. Perceived effectiveness of privacy policy is positively associated with perceived privacy control.

H8. perceived effectiveness of privacy policy is negatively associated with perceived privacy risk.

3.3.2. Boundary coordination: notice, choice, access

Petronio (2013) defined boundary coordination as the process of integrating demand and response. In the online privacy context, demand can be interpreted as an individual's expectation, while response refers to one's perception toward the boundary guideline. In the CPM theory, a decision to disclose personal information is the process of coordinating expectations. This means that individuals have to confirm that the data subject and the data recipients have similar collective control over the information (Petronio, 2013; Xu et al., 2011). The way to identify collective control is to check the FIPPs, especially notice, choice, and access. In this paper, we positioned notice, choice, and access as the components of boundary coordination because these three dimensions are usually involved with the initial stage of information disclosure by the data owner (Wu et al., 2012). Individuals will be presented with companies' privacy policies before they decide whether to disclose their personal information. Privacy policies are usually made up of statements about how customer information will be used (notice), and if individuals have mechanisms to decide what information about them can and cannot be used (access and choice). In consequence, these principles form individuals' perceptions of boundary assurance (Xu et al., 2011).

Among the five core principles of FIPPs, notice is the most fundamental principle. Malhotra et al. (2004) operationalized notice using the awareness of privacy policies to identify the extent to which customers are being informed about the intended use of their data. Privacy notices are an important means to reduce consumers' privacy concerns (Wu et al., 2012) and improve their privacy perception (Faja & Trimi, 2006). These help consumers to decide whether they want to provide private data or choose not to engage with the particular website (Culnan & Milberg, 1998). In an online environment, informativeness reduces perceived uncertainties (P. A. Pavlou, Liang, & Xue, 2007). When customers see a website providing resourceful coverage of its privacy policies, consumer confidence toward the website increases (Chua, Wong, Chang, & Libaque-Saenz, 2017; Earp & Baumer, 2003). This suggests that their perception toward the effectiveness of privacy policy of the website will also increase. The rationale is that disclosing the ways in which companies will use customer data will entice companies to honor these guidelines to avoid damaging their reputation (Libaque-Saenz, Chang, et al., 2016).

Besides notifying consumers on privacy practices, the government should regulate organizations to give choices to consumers on selecting which private information collected can be used and how it will be used (Liu et al., 2005). A close example is the permission-based opt-in/opt-out service subscription feature where customers self-select the services they wish to subscribe and decide how the information they provide may be used. Since most consumers are concerned about losing control over the ways in which websites handle their information (Wu et al., 2012), a choice puts the decision into the hands of the consumers to decide how their private information will be collected and used. According to Brandimarte et al. (2013), when people feel in control they tend to have optimistic expectations about an output. Consequently, individuals who can choose (i.e., control) which personal information could be used by a company may perceive the privacy policy to be effective at avoiding negative results (i.e., effectiveness). Hence, similar to the notification policy, when consumers are given choices, they will have better perception toward the privacy policy implementation, as well as its level of effectiveness, in an organization.

The government should provide the options for customers to access their private information to view and check for data accuracy and completeness (Wu et al., 2012). Similar to the principles of notice and choice, when consumers know that they are able to check and update their data, they will have a more favorable perception toward the effectiveness of the privacy policy in an organization.

Actually, among privacy violation, we have false light on the public eye (Prosser, 1960). This violation refers to the wrong insights that could be obtained from an individual due to incomplete and inaccurate personal data. Thus, privacy policies that allow access to individuals to check the completeness and accuracy of their collected data may be perceived to be effective at avoiding this privacy violation (i.e., false light). Based on the arguments above, we hypothesized that the presence of access, choice, and notice dimensions of the privacy policy will help to improve consumer perception toward the effectiveness of the policy.

H9. a: Access is positively associated with perceived effectiveness of privacy policy.

H9. b: Choice is positively associated with perceived effectiveness of privacy policy.

H9. c: Notice is positively associated with perceived effectiveness of privacy policy.

3.3.3. Boundary turbulence: security, enforcement

Boundary turbulence is related to policy mechanisms to prevent actual invasion from outside sources. Unlike boundary coordination, boundary turbulence relates to industry self-regulation and the effort to solve potential and actual privacy invasion (Xu et al., 2011). In this study, we positioned security and enforcement as the components of boundary turbulence. As individuals disclose their information, the responsibility to protect the information is immediately transferred to the data recipients (Dinev et al., 2013). Therefore, data recipients must demonstrate how they self-regulate in order to abide by the government's policy guidelines in protecting the data. It is important to give boundary assurance to individuals (Wu et al., 2012). Information accuracy and security are important (Liu et al., 2005; Wu et al., 2012) to ensure data integrity. Old data has to be deleted and outdated data ought to be updated with newest information. All data should also be encrypted or converted into an anonymous form in transactions and then stored on physical properties. Consumers often measure the risk of online activities via the possibility of information privacy misuse or revelation (Milne & Culnan, 2004). In fact, previous research has

established the link between perceived security and trust in e-commerce transactions (Chellappa & Pavlou, 2002; Liu et al., 2005). Therefore, many websites try to fortify security perceptions by establishing relationships with third party assurance such as TRUSTe, which acts as a proxy control to increase the perception of self-control (Bandura, 2001; Yamaguchi, 2001). However, in a field experiment that assessed two types of privacy assurance methods, Hui, Teo, and Lee (2007) found that the existence of a privacy statement on websites induces more people to disclose their information, but a privacy seal did not. This finding underscores the importance of the first principle of FIPPs, which is “notice.” If consumers have a guarantee that the information they provide online is secured and will be used properly, there is higher likelihood that they will perceive the privacy practices in the organization as effective. Typically, security statements are provided in companies' privacy policies. If adequate and clear security means are displayed in these documents, consumers will choose to believe that privacy violations such as intrusion into their private information, disclosure of embarrassing private facts, and appropriation of their data by third parties will be effectively avoided.

Enforcement ensures that organizations are observant and obedient to the imposed regulations and policies. In this study, it is the FIPPs. Enforcement can only be effective if there is a mechanism or instrument in place to enforce the principles (Wu et al., 2012). When FIPPs are enforced in organizations by the law, consumers will have a better perception toward the effectiveness of the privacy policy because companies will abide by the regulation to avoid any privacy violation. Based on the arguments above, we hypothesized that the presence of security and enforcement dimensions of the privacy policy will help to improve consumer perception toward the effectiveness of the policy.

H9. d: Security is positively associated with perceived effectiveness of privacy policy.

H9. e: Enforcement is positively associated with perceived effectiveness of privacy policy.

4. Method

4.1. Scale development

We adapted validated measurement items from the literature. Items for measuring perceived privacy were adopted from Dinev et al. (2013). Perceived privacy risk was measured using four Likert-scale questions adapted from Dinev and Hart (2006a) and Malhotra et al. (2004). Perceived privacy control, privacy concerns and perceived effectiveness of privacy policy were measured using items taken from Xu et al. (2011). Trust were adapted from Paul A. Pavlou (2003) and Wu et al. (2012). Items that measure the five dimensions of FIPPs came from Wu et al. (2012). A seven-point Likert scale was adopted to measure the degree of agreement with each item. Table 1 shows the measurement items.

For all the questions, we put in the context of an online banking service to capture the respondents' perception toward privacy practices of the particular website. This is in line with previous research (Ackerman & Mainwaring, 2005; Margulis, 2003; Petronio, 2012; Solove, 2006, 2008; Xu et al., 2011; Xu et al., 2012) that notes the importance of theoretically distinguishing between general concerns for privacy and context-specific concerns. Furthermore, context-specific privacy is much more understandable (Bennett, 1992) and has higher percentages of explained variance (Xu et al., 2011). Prior research suggests that consumers' personal characteristics may affect their evaluation of privacy issues such as privacy concerns, the outcome of information disclosure, and the adoption of related services (Sheehan, 1999; Xu et al., 2012). Therefore, we included gender and age as the control variables in the research model.

4.2. Survey administration

In this study, research samples from Malaysia were used to verify the research model. Malaysia is the first country in South-East Asia to enact a comprehensive information protection law based on the basic FIPPs of the United States of America (Cieh, 2013). The level of privacy concerns of Malaysian is also very high (T. Smith, 2011). Thus, Malaysia is a good research sample for a study that examines the relationship between privacy policy and individuals' privacy perception.

We approached potential participants at random in six of the largest shopping malls in Malaysia and asked their willingness to participate in the study. Once they agreed, they were given the paper-based questionnaire to answer on the spot. To qualify for the study, the participants must meet the requirement of having used at least one online banking service for a minimum of six months. The constraint was placed to ensure that the participants have sufficient experience with online banking services. A total of 363 participants met the requirements and answered our survey. The response rate of our survey was 36%. To achieve a sincere response, the purpose of the survey was explained in detail and the respondents were allowed to answer without time limits. In answering the questions, the participants were asked to recall their experiences in using one banking website that they frequented the most in the past one month. The participants received a RM10 (Ringgit Malaysia) voucher after answering the survey. We conducted a homogeneity test using Chi Square test and compared our sample's gender, age, education, and income distribution with the distribution data provided by the Malaysia government (https://www.dosm.gov.my/v1/). We found that there was no significant difference between our sample and the government's information. Table 2 shows the demographic information of the participants.

5. Results

We used Partial Least Squares (PLS) to analyze the data. PLS is a powerful second generation modeling technique that is suitable for theory testing in exploratory studies. It simultaneously assesses measurement and structural models in an optimal fashion and analyzes complex causal models involving multiple constructs with multiple observed items (Chin, 1998). PLS also places minimal restrictions on measurement scales, sample size, and residual distributions (Chin, 1998). To decide the minimum sample size of PLS, we used the rule of thumbs suggested in Kock and Hadaya (2018). According to the rule, a sample size should be over ten-times the number of the constructs. The sample size (n = 364) of this study met the criteria (n = 110), so a high level of statistical power is expected. We utilized SmartPLS 3.0 software and modeled all constructs using reflective measures.

5.1. Measurement model

To establish the psychometric properties of the measurement model, we examined the convergent validity and discriminant validity of the research instrument (Gefen, Straub, & Boudreau, 2000; J. F. J. Hair, Black, Babin, & Anderson, 2009). Convergent validity is determined by item reliability, composite reliability, and average variance extracted (AVE). The Cronbach's alpha and Dijkstra-Henseler's rho (ρA) were tested to determine the reliability. In Table 3, the reliability coefficients and the composite reliabilities were all greater than the recommended 0.70 level (Henseler, Hubona, & Ray, 2016; Nunnally, 1978; Teo, Lim, & Lai, 1999), whereas the AVEs were > 0.50 for all constructs (Fornell & Larcker, 1981)(See Table 3). Also, all item loadings were > 0.70, suggesting that more variance was shared between an item and its construct than there was error variance (J. F. Hair, Sarstedt, Ringle, & Mena, 2012; King & Teo, 1996). Therefore, our measurement model demonstrated good convergent validity.

Discriminant validity is the degree to which items measuring different constructs are distinct (Campbell & Fiske, 1959). The square

Table 1
Measurement items.

Construct	Items	Measurement Items	Reference Sources
Perceived Privacy		When you answer the following questions about your privacy, please think about the limited access the online banking service has to your personal information:	Dinev et al. (2013)
	PP1	I feel I have enough privacy when I use this online banking service.	
	PP2	I am comfortable with the amount of privacy I have when using this online banking service.	
	PP3	I think my online privacy is preserved when I use this online banking service.	
Perceived Privacy Control	PPC1	I believe I have control over who can get access to my personal information collected by this online banking service.	Xu et al. (2011)
	PPC2	I think I have control over what personal information is released by this online banking service.	
	PPC3	I believe I have control over how personal information is used by this online banking service.	
	PPC4	I believe I can control my personal information provided to this online banking service.	
Perceived Privacy Risk	PPR1	There is high risk that others can find private and personal information about me from this online banking service.	Dinev and Hart (2006a); Malhotra et al. (2004)
	PPR2	There would be high potential for privacy loss associated with giving personal information to this online banking service.	
	PPR3	Personal information could be inappropriately used by this online banking service.	
	PPR4	Providing this online banking service with my personal information would involve many unexpected problems.	
Privacy Concern	PC1	I am concerned that the information I submit to this online banking service could be misused.	Xu et al. (2011)
	PC2	I am concerned that others can find private and personal information about me from this online banking service.	
	PC3	I am concerned about providing personal information to this online banking service because of what others might do with it.	
	PC4	I am concerned about providing personal information to this online banking service because it could be used in a way I did not foresee.	
Trust	TRU1	The bank's online banking policy with respect to how they will share my personal information with third parties makes me feel the company is trustworthy.	Paul A. Pavlou (2003); Wu et al. (2012)
	TRU2	The bank's online banking policy on how it would use any personal information about me makes me feel that the company is trustworthy.	
	TRU3	The ability to access my personal information to ensure that it is accurate and complete makes me feel that the bank is trustworthy.	
	TRU4	The bank's online security policy makes me feel that the company is trustworthy.	
	TRU5	The bank's level of online encryption and other security measures makes me feel that the company is trustworthy.	
	TRU6	The bank's online banking privacy policy concerning the notice of personal information collection makes me feel this company is trustworthy.	
Perceived Effectiveness of Privacy Policy	PEPP1	I feel confident that the privacy statements posted by the bank on its online banking service websites reflect their commitments to protect my personal information.	Xu et al. (2011)
	PEPP 2	With their privacy statements, I believe that my personal information will be kept private and confidential by the bank.	
	PEPP 3	I believe that the privacy statements posted by the bank on its online banking service websites are an effective way to demonstrate their commitments to privacy.	
Notice	NTC1	This online banking service discloses what personal information is going to be collected.	Wu et al. (2012)
	NTC2	This online banking service explains why personal information is going to be collected.	
	NTC3	This online banking service explains how the collected personal information will be used.	
Choice	CHO1	This online banking service informs me whether my personal information will be disclosed to a third party and explains under what conditions it will be disclosed.	Wu et al. (2012)
	CHO2	This online banking service gives clear choice (asking permission) before disclosing personal information to third party.	
	CHO3	This online banking service gives clear choice (asking permission) before it uses my personal information for secondary purposes.	
Access	ACC1	This online banking service allows me to review the collected personal information.	Wu et al. (2012)
	ACC2	This online banking service allows me to correct inaccuracies in the personal information collected.	
	ACC3	This online banking service allows me to delete personal information from the online banking service website.	
Security	SEC1	This online banking service explains the steps it takes to provide security for the personal information collected.	Wu et al. (2012)
	SEC2	This online banking service informs that any personal information will not be disclosed to a third party without my permission.	
	SEC3	This online banking service uses advanced technology to protect my personal information.	

(*continued on next page*)

Table 1 (*continued*)

Construct	Items	Measurement Items	Reference Sources
Enforcement	ENF1	This online banking service discloses that there is a law sanctioning those who violate the privacy statements.	Wu et al. (2012)
	ENF2	This online banking service discloses that it will take actions according to the law against those who violate the privacy statements.	
	ENF3	This online banking service discloses that it will take strong action when someone breaches the company's privacy policy.	

Table 2
Demographic information of the participants.

Respondents		n = 363	
		Frequency	Percent (%)
Gender	Male	200	55.1
	Female	163	44.9
Age	20–29	122	33.6
	30–39	112	30.9
	40–49	86	23.7
	50–59	30	8.3
	60 and above	13	3.6
Education	Elementary	5	1.4
	Secondary	56	15.4
	Diploma	104	28.7
	Bachelor	166	45.7
	Master	27	7.4
	Doctoral	5	1.4
Family Income	< 2000	14	3.9
	2001–4000	50	13.8
	4001–6000	101	27.8
	6001–8000	76	20.9
	8001–10,000	46	12.7
	> 10,000	76	20.9
Online Banking Experience	< 1 year	65	17.9
	1–2 years	99	27.3
	3–4 years	136	37.5
	5–7 years	56	15.4
	8–10 years	1	0.3
	> 10 years	6	1.7

Table 3
Reliability and convergent validity.

Construct	Mean (Standard Deviation)	Cronbach's Alpha	rho_A	Composite Reliability
Perceived Privacy	4.381(1.529)	0.963	0.963	0.976
Perceived Privacy Control	4.443(1.281)	0.945	0.946	0.96
Privacy Risk	4.654(1.219)	0.909	0.91	0.936
Privacy Concern	4.546(1.396)	0.912	0.915	0.938
Trust	4.466(1.412)	0.957	0.957	0.965
Perceived effectiveness of privacy policy	4.542(1.220)	0.925	0.926	0.952
Access	4.838(1.197)	0.873	0.876	0.922
Choice	4.551(1.193)	0.917	0.922	0.947
Notice	4.739(1.258)	0.898	0.912	0.936
Security	4.769(1.117)	0.905	0.908	0.94
Enforcement	4.739(1.258)	0.936	0.937	0.959

roots of all AVEs were much larger than the corresponding cross-correlations (Table 4), and each item loaded most strongly on its corresponding construct (Table 5). As an alternative way to check the discriminant validity, the HTMT ratio can be used. The HTMT ratio of all constructs should be lower than 0.85 (Henseler et al., 2016). In our research model, the ratio of the majority of the constructs were below the criterion except for one relationship between security and access (0.853). These results suggest adequate discriminant validity of our research model (Fornell & Larcker, 1981).

5.2. Structural model

After confirmation of acceptable psychometric properties for the measurement model, we examined the structural model (Fig. 3). The predictive power of the structural model is assessed using R^2 in the endogenous constructs (Chin, 1998; Gefen et al., 2000). The model accounted for 65.7% of the variance in perceived privacy, 53.3% of the variance in perceived privacy control, 9.5% of the variance in perceived privacy risk, 36.4% of the variance in privacy concern, 44.0% of the variance in perceived trust, and 60.2% of the variance in perceived effectiveness of privacy policy. Since the percentages of variance explained were far > 10%, these indicate a satisfactory and substantive model (Falk & Miller, 1992).

The results show that perceived privacy is determined by perceived privacy control, privacy concern, and trust. Privacy control and privacy risk are positively associated with trust and privacy concern respectively. Perceived effectiveness of privacy policy has significant effects on both perceived privacy control and perceived privacy risk. Enforcement has the strongest effect on perceived effectiveness of privacy policy, followed by access, notice, and security. Choice does not have any significant effect on perceived effectiveness of privacy policy. Our examination of the control variables show that gender, age, education level, and income level have no significant effect on perceived privacy.

5.3. Test for common method bias

We conducted two types of statistical analyses to check for common method bias (CMB): Harman's one-factor test and the latent method factor (LMF). First, for Harman's one-factor test (Podsakoff, MacKenzie, Lee, & Podsakoff, 2003), we loaded all the measurement items into an exploratory factor analysis in SPSS and analyzed the unrotated factor solution. The result shows that no single factor emerged to account for the majority of the variance. In fact, the first factor explained 47.92% of the total variance, which is below the threshold of 50% (Hazen, Cegielski, & Hanna, 2011). This indicates that CMB is unlikely to be a significant issue.

Second, we followed the procedures of Liang, Saraf, Hu, and Xue (2007) to conduct the modeling of the LMF using the PLS approach. We converted each indicator into a single-indicator construct and added an LMF to the theoretical model as a second-order construct. All first-order single-indicator constructs were then linked to this LMF. The ratio of substantive variance to method variance was calculated and evaluated. The results (Appendix A) show that the average substantively explained variance of all of the indicators was 0.832, whereas the average method-based variance was 0.005. The ratio of substantive variance to method variance was approximately 166:1, which suggests that the method variance identified was very small in magnitude. Moreover, most of the method factor loadings were not significant and the significance of all of the proposed model paths had not changed after including the LMF. Therefore, the results again show that CMB is unlikely to be a serious concern in our study.

Table 4
Correlations (HTMT) and square root of AVE.

Construct	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Perceived Privacy	**0.965**														
Perceived Privacy Control	0.629	**0.926**													
	(0.659)														
Privacy Risk	−0.321	−0.283	**0.887**												
	(0.342)	(0.304)													
Privacy Concern	−0.414	−0.331	0.603	**0.889**											
	(0.440)	(0.353)	(0.662)												
Trust	0.765	0.663	−0.231	−0.243	**0.907**										
	(0.797)	(0.697)	(0.246)	(0.257)											
Perceived effectiveness of	0.729	0.730	−0.308	−0.384	0.768	**0.932**									
privacy policy	(0.773)	(0.780)	(0.335)	(0.416)	(0.817)										
Access	0.568	0.619	−0.201	−0.287	0.603	0.694	**0.893**								
	(0.617)	(0.617)	(0.222)	(0.318)	(0.658)	(0.770)									
Choice	0.435	0.477	−0.022	−0.261	0.429	0.561	0.648	**0.926**							
	(0.461)	(0.512)	(0.054)	(0.285)	(0.458)	(0.607)	(0.722)								
Notice	0.500	0.569	−0.050	−0.263	0.549	0.656	0.676	0.747	**0.91**						
	(0.531)	(0.612)	(0.072)	(0.287)	(0.585)	(0.711)	(0.756)	(0.829)							
Security	0.608	0.624	−0.197	−0.296	0.588	0.694	0.761	0.682	0.701	**0.916**					
	(0.650)	(0.650)	(0.216)	(0.326)	(0.631)	(0.758)	(0.853)	(0.747)	(0.779)						
Enforcement	0.584	0.633	−0.227	−0.237	0.601	0.696	0.708	0.592	0.645	0.768	**0.942**				
	(0.614)	(0.614)	(0.246)	(0.254)	(0.635)	(0.747)	(0.779)	(0.637)	(0.698)	(0.832)					
Gender	0.035	0.002	0.036	0.060	0.070	0.020	0.001	−0.009	0.018	−0.072	−0.038	**1**			
	(0.036)	(0.036)	(0.053)	(0.064)	(0.071)	(0.047)	(0.014)	(0.017)	(0.030)	(0.075)	(0.041)				
Age	0.017	0.045	−0.174	−0.037	0.042	0.027	0.052	−0.080	−0.028	0.030	0.008	0.085	**1**		
	(0.017)	(0.047)	(0.183)	(0.053)	(0.043)	(0.032)	(0.056)	(0.082)	(0.043)	(0.043)	(0.017)	(0.085)			
Education	0.199	0.180	−0.076	−0.038	0.174	0.157	0.143	0.109	0.191	0.189	0.188	0.070	0.061	**1**	
	(0.203)	(0.148)	(0.080)	(0.040)	(0.178)	(0.163)	(0.151)	(0.113)	(0.198	(0.202)	(0.195)	(0.070)	(0.061)		
Income	−0.023	−0.042	−0.033	−0.004	−0.048	−0.027	−0.051	0.007	0.034	−0.048	0.014	0.106	0.114	0.069	**1**
	(0.024)	(0.044)	(0.083)	(0.019)	(0.050)	(0.029)	(0.055)	(0.031)	(0.051)	(0.038)	(0.026)	(0.106)	(0.114)	(0.069)	

Note: The diagonal elements (in bold) represent the square root of the AVE.

6. Discussion and implications

6.1. Discussion of the findings

The results showed that the proposed model accounted for high percentage of the variance in perceived privacy. For organizations, the results imply that the factors identified in our privacy boundary management model for the formation of perceived privacy can be manipulated to yield the desired effects. All hypotheses are supported, except that on the relationship between choice and perceived effectiveness of privacy policy and privacy risk to perceived privacy.

Choice implies that customers have the options to decide whether to disclose their information and how their information will be used. In fact, customers could select the extent to which their information may be shared during the information disclosing process, and they can refuse to disclose the information if they do not want to. Thus, choice essentially positions the decision-making power into the hands of the customers. When customers can decide, thus having control, they are likely to unlink their own decision (i.e., choice) from an organization's information practices.

Among all the FIPPs dimensions, enforcement has the strongest effect on perceived effectiveness of privacy policy. The banking sector involves highly confidential financial data that many customers would want to keep private. Customers value the enforcement clause in the FIPPs that provides an assurance that a mechanism is in place to govern the disclosure, sharing and use of their financial data. The clause also informs them that sanctions and penalties can be imposed should there be any violation. We believe the same sentiment toward enforcement is present in many other sectors such as the insurance industry and the healthcare services.

With enforcement having the strongest effect, we would expect to see security coming in second place especially when the context of our study is online banking. However, the results show that security, while significant, is the weakest among the four important dimensions of the FIPPs that may influence a customer's perception toward the effectiveness of privacy policy. Since our respondents are asked to evaluate their experience with one banking website that they frequented the most in the past month, it is possible that they were already comfortable with the existing security system of the bank, thus it rendered a much smaller effect. Nonetheless, the significant effect of security on perceived effectiveness of the privacy policy continues to underscore its role as a fundamental technological feature that should be present in all digital transactions.

Access and notice have rather similar significant effect on one's perceived effectiveness of privacy policy. This means customers value an organization's effort to inform them about its information practices and to allow them to make changes to personal data. When the customers perceive privacy policy as more effective, they will see themselves as having more control toward how their data will be used and thus able to avoid any potential risk associated with the sharing of the data.

For risk-control assessment, only perceived privacy control has direct significant effects on perceived privacy while perceived privacy risk exerts effect via perceived privacy concerns. As expected, boundary self-regulation factors significantly affect perceived privacy. The effect of trust on perceived privacy is more than twice that of perceived privacy concerns. This suggests that in the banking sector, the customers tend to feel more confident when they trust the company which they are sharing their private information and data. When they have higher level of trust, then they will have higher level of perceived privacy.

6.2. Contributions and implications

This study has several contributions. First, it builds a comprehensive model to explain individuals' privacy boundary management process that is founded on the well-established CPM and RFT. With increasing consumer awareness, an organization's strategies in executing privacy policies may reflect how effective the organization is in protecting consumer data. Therefore, a wholesome understanding of the process at which consumers formulate and reach perceived privacy decisions

Table 5
Loadings and cross-loadings.

	PP	PPC	PPR	PC	TRU	PEPP	ACC	CHO	NTC	SEC	ENF
PP1	**0.967**	0.605	−0.301	−0.391	0.744	0.701	0.560	0.424	0.501	0.597	0.560
PP2	**0.970**	0.625	−0.316	−0.409	0.745	0.712	0.541	0.426	0.491	0.600	0.570
PP3	**0.957**	0.590	−0.311	−0.398	0.725	0.698	0.544	0.410	0.454	0.563	0.559
PPC1	0.553	**0.907**	−0.208	−0.246	0.602	0.63	0.577	0.436	0.516	0.546	0.559
PPC2	0.569	**0.934**	−0.259	−0.307	0.596	0.668	0.556	0.456	0.505	0.580	0.583
PPC3	0.587	**0.936**	−0.254	−0.323	0.628	0.690	0.563	0.455	0.536	0.601	0.583
PPC4	0.618	**0.926**	−0.322	−0.347	0.630	0.713	0.595	0.420	0.550	0.583	0.618
PPR1	−0.212	−0.225	**0.844**	0.562	−0.094	−0.209	−0.132	−0.028	−0.034	−0.152	−0.174
PPR2	−0.280	−0.248	**0.921**	0.544	−0.198	−0.292	−0.198	−0.019	−0.035	−0.194	−0.235
PPR3	−0.294	−0.273	**0.906**	0.546	−0.211	−0.275	−0.178	−0.036	−0.068	−0.174	−0.193
PPR4	−0.348	−0.255	**0.873**	0.489	−0.31	−0.313	−0.201	0.004	−0.039	−0.177	−0.202
PC1	−0.367	−0.312	0.556	**0.862**	−0.231	−0.338	−0.274	−0.216	−0.237	−0.23	−0.225
PC2	−0.411	−0.342	0.560	**0.905**	−0.275	−0.376	−0.271	−0.192	−0.217	−0.277	−0.237
PC3	−0.362	−0.278	0.529	**0.914**	−0.198	−0.351	−0.260	−0.250	−0.258	−0.296	−0.228
PC4	−0.327	−0.239	0.495	**0.875**	−0.150	−0.297	−0.210	−0.279	−0.224	−0.249	−0.145
TR1	0.640	0.613	−0.234	−0.210	**0.879**	0.674	0.539	0.404	0.498	0.514	0.540
TR2	0.691	0.636	−0.243	−0.244	**0.926**	0.716	0.573	0.410	0.514	0.540	0.532
TR3	0.708	0.595	−0.194	−0.199	**0.919**	0.686	0.555	0.390	0.504	0.517	0.557
TR4	0.725	0.599	−0.215	−0.261	**0.920**	0.716	0.543	0.386	0.507	0.541	0.539
TR5	0.691	0.561	−0.195	−0.205	**0.894**	0.673	0.543	0.358	0.480	0.536	0.543
TR6	0.706	0.604	−0.178	−0.200	**0.901**	0.712	0.528	0.385	0.482	0.549	0.559
PEPP1	0.677	0.681	−0.304	−0.382	0.713	**0.932**	0.659	0.549	0.630	0.656	0.643
PEPP2	0.675	0.714	−0.298	−0.359	0.704	**0.941**	0.630	0.529	0.601	0.654	0.653
PEPP3	0.688	0.646	−0.258	−0.333	0.733	**0.924**	0.652	0.49	0.605	0.632	0.651
ACC1	0.495	0.536	−0.182	−0.264	0.521	0.616	**0.918**	0.603	0.604	0.669	0.614
ACC2	0.462	0.480	−0.132	−0.211	0.498	0.576	**0.883**	0.554	0.572	0.642	0.599
ACC3	0.558	0.631	−0.217	−0.288	0.59	0.660	**0.878**	0.576	0.632	0.721	0.677
CHO1	0.349	0.424	0.038	−0.188	0.383	0.475	0.562	**0.908**	0.719	0.58	0.516
CHO2	0.408	0.445	−0.015	−0.240	0.417	0.534	0.613	**0.945**	0.703	0.657	0.554
CHO3	0.446	0.453	−0.077	−0.290	0.390	0.545	0.620	**0.924**	0.659	0.651	0.572
NTC1	0.512	0.562	−0.119	−0.272	0.571	0.673	0.661	0.651	**0.905**	0.625	0.627
NTC2	0.437	0.521	−0.022	−0.234	0.481	0.582	0.612	0.677	**0.928**	0.64	0.581
NTC3	0.402	0.459	0.024	−0.203	0.428	0.516	0.561	0.723	**0.897**	0.652	0.544
SEC1	0.541	0.585	−0.180	−0.292	0.526	0.610	0.715	0.617	0.642	**0.905**	0.658
SEC2	0.532	0.549	−0.161	−0.249	0.523	0.620	0.673	0.630	0.641	**0.917**	0.692
SEC3	0.596	0.581	−0.199	−0.273	0.565	0.675	0.704	0.628	0.643	**0.927**	0.758
ENF1	0.564	0.614	−0.238	−0.271	0.573	0.666	0.701	0.593	0.645	0.761	**0.936**
ENF2	0.554	0.610	−0.201	−0.212	0.571	0.670	0.672	0.573	0.612	0.727	**0.952**
ENF3	0.530	0.563	−0.203	−0.186	0.554	0.629	0.624	0.505	0.564	0.680	**0.937**

Bold numbers represent the loadings on their assined factor.
Note: PP = Perceived privacy; PPC = Perceived privacy control; PPR = Perceived privacy risk; PC = Privacy concern; TRU = Trust; PEPP = Perceived effectiveness of privacy policy; ACC = Access; CHO = Choice; NTC = Notice; SEC = Security; ENF = Enforcement.

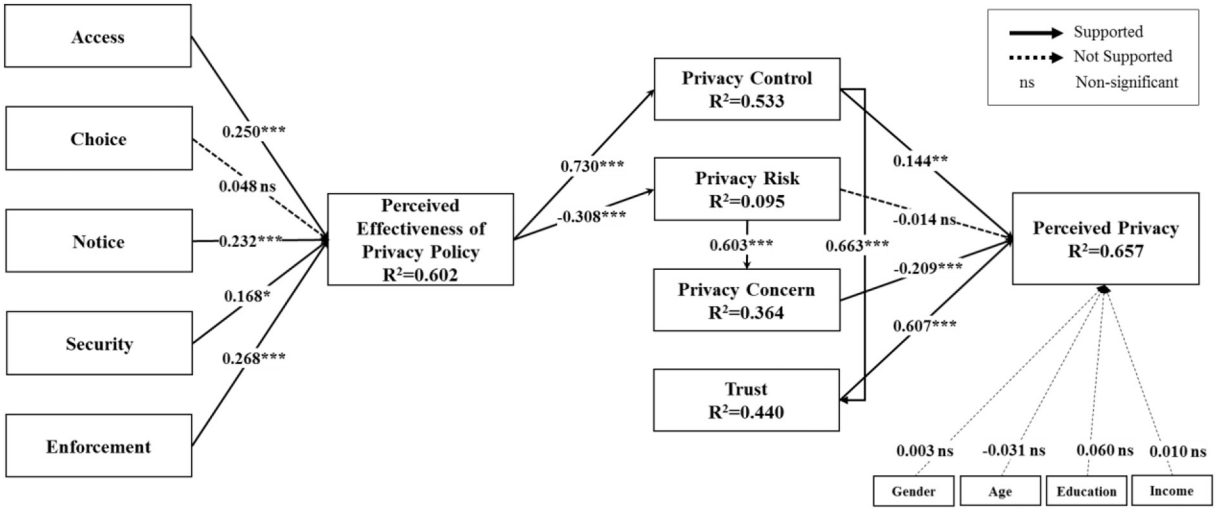

Fig. 3. PLS results for the privacy boundary management model.

would help organizations to develop effective privacy practices and governance strategy. With a partial approach, most studies have focused on antecedents that directly explain self-disclosure (Dienlin & Metzger, 2016). Efforts to explain the entire privacy mechanism were not enough while many scholars have tried to integrate the fragmented perspectives of privacy. Dinev et al. (2013) proposed a comprehensive model that integrates various privacy related concepts, and rigorously validated it with 192 samples. However, some included constructs (e.g.,

perceived benefit of information disclosure and regulatory expectations) were still broad and abstract even though the model explains well the variance in perceived privacy. Moreover, only individual level constructs were examined to understand perceived privacy. The model proposed in this paper identifies how individuals process institutional level policy, and compare that with their own inherent need for privacy protection in order to reach a privacy boundary decision at the individual level. By capturing the decision-making process, the model contributes to the theoretical development of privacy decision-making, which adds value to the privacy literature. More valuably, the introduction of RFT into the privacy context shows that the introduction of both promotion-focused and prevention-focused attitudes provide a more complete view of an individual's boundary management process.

Second, this study tests all five dimensions of FIPPs that influence consumers' perception toward the effectiveness of privacy policy. A negative perception could adversely impact the reputation of an organization (Wu et al., 2012). On the other hand, a positive perception could elevate the status of an organization among its peers. The results identify the elements that organizations could manipulate to increase positive perception toward privacy policy implementation in organizations. Besides enriching existing understanding of consumer privacy in the literature, the findings also suggest it is worthwhile for future work to focus along similar lines. Furthermore, even though the FIPPs were developed in the United States, many international institutions and countries have relied on the FIPPs as core principles to design their data protection clauses. Examples of these clauses are the Organization for Economic Cooperation and Development (OECD)'s guidelines on the Protection of Privacy and Transborder Flows of Personal Data (Organization for Economic Cooperation and Development (OECD), 1980) and the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Council of Europe, 1987). Since the core principles are similar, our findings could be generalized to contexts and places where the FIPPs are used as the designing guidelines. For the Malaysian PDPA, we suggest that the government enhance the enforcement principle of the Act. This study found that perception of the enforcement principle is the strongest factor contributing to the perception of the effectiveness of privacy policy. With news on privacy invasion and data breaches regularly making headlines, the government may wish to explore options for revising the Act to reflect the evolving business environment.

Third, this study helps to understand the dynamics of the effectiveness of privacy policy on privacy perception mechanism. Xu et al. (2011) empirically tested the effect of privacy policy on privacy control and risk at four different websites. According to the results, privacy policy was identified as a factor lowering privacy risk rather than strengthening privacy control. Dinev et al. (2013) also showed similar results that regulatory expectations are relatively more associated with privacy risk. However, in this study, the effectiveness of privacy policy was associated more with privacy control than with risk. The differences in the results could be due to the characteristics of the samples.

The results of the study highlight several practical implications. First, for policy makers, the results emphasize the importance of having the enforcement clause in enacting digital data policies and regulations because consumers clearly place a high level of importance on such a clause. This is especially the case in data intensive sectors such as banking and the financial sectors, and healthcare. As suggested in the literature (Petronio, 2012; Xu et al., 2011), information privacy is context specific, thus, policy makers may need to design industry-specific guidelines to fit different consumer privacy needs. Moreover, with the changing business environment, it is timely to revisit and revise the FIPPs to fit the latest business conditions.

Second, for banks, it is essential that they comply with the FIPPs since customers significantly link four out of five dimensions in FIPPs to their perceived effectiveness of privacy policy. Since customers value organizational effort to notify them about data collection and usage, banks have to ensure that these practices are built into their daily operational models. Furthermore, it is useful to invest in the latest security system to provide a safe financial transaction experience to customers. All these business practices and investments will increase the customer's confidence that they have control toward the sharing and usage of personal data.

Finally, although choice is conceptually very important in FIPPs, it insignificantly affects the effectiveness of privacy policy. Banks, however, should know why choice does not actually contribute to the recognition of privacy policy effects. One possible reason is that people are less likely to be exposed to a situation of choice in relation to privacy issues. If customers did not accept certain conditions related to privacy policy, they would not be able to use financial services because a bank uses privacy policies for its own purposes (Bélanger & Crossler, 2011). Customers sometimes do not even know they have a choice. Thus, a bank needs to give customers more choices on privacy protection and try to improve the privacy policy in order for it to become more effective. Improving privacy policy contributes to the services becoming more trustworthy (Aïmeur, Lawani, & Dalkir, 2016).

6.3. Limitations and future research

Privacy boundary management is a complex process and there is a need to extend research efforts to fully understand it. In impersonal relationships such as that between users and online banking services, boundary coordination may happen only through privacy policies (Metzger, 2007). Accordingly, our research model attempts to capture the coordination process in these contexts by analyzing individuals' perceptions of the different dimensions encompassing privacy policies. However, as with other empirical research, the current study has some limitations that should be considered. First, the paper only focuses on the use of banking websites. Some may argue that this limits the generalization of the findings. However, previous research (Petronio, 2012; Xu et al., 2011) support our decision to focus on one sector and contend that privacy decision is context-specific. Therefore, privacy research should consider context differences. We believe that on a higher, more general level, our model is extendable to other settings. Compared to many other online transactional data, the banking sector contains a wealth of sensitive private information that many consumers would be reluctant to disclose to third parties. Therefore, we expect consumers to act more conservatively as regards the sharing and disclosure of their banking data.

Second, this paper only collects data from one country. Prior research (Harding, 2001; Xu et al., 2011) contend that the degree of policy implementation and enforcement will have an effect on people's privacy boundary formation. Therefore, future studies could collect data from countries with varying levels of implementation and enforcement to examine these effects on privacy boundary formation. In addition, this study did not consider the effect of the period of online banking use. Research results would be more accurate if the period of use was included into a research model as a control variable.

There are also other potential avenues for future research. First, future studies could compare consumer privacy boundary decisions in different contexts such as e-commerce and social network sectors as they carry information with different sensitivity levels. Banks, as studied in this research, carry the most sensitive information. E-commerce contains data with medium level of sensitivity, while social network has data with low sensitivity. It will be interesting to identify how consumers' privacy boundary management would differ based on the sensitivity level of their private data.

Second, future study could adopt more variables related to privacy such as liability, responsibility, and mitigation factors to expand our current understanding on privacy boundary management. Our study has provided a comprehensive view of individuals' privacy boundary formation by confirming the effect of the four boundary management processes. Future research could go deeper into each of the processes and explore how each works. In addition, future study should collect

more samples which strengthen the reliability of the study.

Third, examining the effect of the five dimensions of FIPPs on the effectiveness of privacy policy is relevant because the study was conducted with the sample of Malaysia, which is enacted based on the U.S. FIPPs. However, the FIPPs are less comprehensive in scope than other policies such as EU or OECD. Thus, it would be interesting for future study to extend the dimensions of FIPPs and include those from the EU or OECD and investigate the effect of each dimension on privacy policy effectiveness.

Fourth, it is possible to discuss the second-order or third-order conceptualization of FIPPs as the validity of sub-constructs of FIPPs was confirmed through this study. Hong and Thong (2013) identified various conceptualizations of information privacy concerns through an extensive literature review and developed a third-ordered instrument to measure the concerns. Following this study, refinement of the FIPPs' measurement structure would be a good attempt.

Finally, future research may also focus on the process for boundary formation in interpersonal relationships, which may be more dynamic than those in impersonal relationships. Indeed, in impersonal relationships, this procedure happens in a static manner by analyzing privacy policies. In contrast, in interpersonal relationships, this process may require an active interaction between data owners and potential co-owners to clearly define the rules for data usage.

6.4. Concluding remarks

This study contributes to the privacy literature by proposing and empirically testing a privacy boundary management model that explains how individuals develop and manage their privacy boundary. Given the elusive and complex nature of information privacy, as well as the increasing concern consumers have toward their private information, it is obvious that more research is needed to understand consumer information privacy management. This study is novel in that the existing empirical research has not linked all the dimensions of the FIPPs to perceived effectiveness. More importantly, the study provides a cognitive process model to trace individuals' privacy boundary management. The process starts from institutional boundary identification and proceeds to boundary rule formation, and finally to boundary decision.

Acknowledgement

This work is supported by funding from the Malaysia Ministry of Higher Education, Fundamental Research Grant Scheme (FRGS), Project number: FRGS/1/2014/SS05/SYUC/02/1.

Appendix A. Assessment of the potential common method variance

Construct	Indicator	Substantive factor loading (R1)	$R1^2$	Method factor loading (R2)	$R2^2$
Perceived Privacy	PP1	0.967***	0.935	0.008	0.000
	PP2	0.970***	0.941	0.018	0.000
	PP3	0.957***	0.916	−0.026	0.001
Perceived Privacy Control	PPC1	0.909***	0.826	−0.051	0.003
	PPC2	0.936***	0.876	−0.049	0.002
	PPC3	0.936***	0.876	0.011	0.000
	PPC4	0.923***	0.852	0.088*	0.008
Perceived Privacy Risk	PPR1	0.694***	0.482	0.049	0.002
	PPR2	0.895***	0.801	0.003	0.000
	PPR3	0.908***	0.824	−0.006	0.000
	PPR4	0.886***	0.785	−0.045	0.002
Privacy Concern	PC1	0.855***	0.731	−0.026	0.001
	PC2	0.900***	0.810	−0.037	0.001
	PC3	0.919***	0.845	0.008	0.000
	PC4	0.883***	0.780	0.055	0.003
Trust	TRU1	0.880***	0.774	0.028	0.001
	TRU2	0.926***	0.857	0.017	0.000
	TRU3	0.919***	0.845	−0.033	0.001
	TRU4	0.920***	0.846	0.005	0.000
	TRU5	0.894***	0.799	−0.029	0.001
	TRU6	0.900***	0.810	0.014	0.000
Perceived Effectiveness of Privacy Policy	PEPP1	0.892***	0.796	0.046	0.002
	PEPP2	0.943***	0.889	−0.024	0.001
	PEPP3	0.962***	0.925	−0.022	0.000
Access	ACC1	0.922***	0.850	−0.078	0.006
	ACC2	0.893***	0.797	−0.146**	0.021
	ACC3	0.864***	0.746	0.235***	0.055
Choice	CHO1	0.915***	0.837	−0.055	0.003
	CHO2	0.944***	0.891	0.006	0.000
	CHO3	0.919***	0.845	0.049	0.002
Notice	NTC1	0.886***	0.785	0.179**	0.032
	NTC2	0.934***	0.872	−0.051	0.003
	NTC3	0.913***	0.834	−0.122*	0.015
Security	SEC1	0.908***	0.824	−0.007	0.000
	SEC2	0.919***	0.845	−0.067	0.004
	SEC3	0.923***	0.852	0.073	0.005

Enforcement	ENF1	0.934***	0.872	0.102*	0.010
	ENF2	0.952***	0.906	0.001	0.000
	ENF3	0.939***	0.882	−0.102**	0.010
Average(by absolute value)		0.911	0.832	0.051	0.005

* $p < 0.05$
** $p < .01$
*** $p < .001$.

References

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

Aïmeur, E., Lawani, O., & Dalkir, K. (2016). When changing the look of privacy policies affects user trust: An experimental study. *Computers in Human Behavior, 58*, 368–379.

Baas, M., De Dreu, C. K., & Nijstad, B. A. (2008). A meta-analysis of 25 years of mood-creativity research: Hedonic tone, activation, or regulatory focus? *Psychological Bulletin, 134*(6), 779–806.

Bandura, A. (2001). Social cognitive theory: An agentic perspective. *Annual Review of Psychology, 52*(1), 1–26.

Bansal, G., & Gefen, D. (2015). The role of privacy assurance mechanisms in building trust and the moderating role of privacy concern. *European Journal of Information Systems, 24*(6), 624–644.

Bansal, G., & Zahedi, F. (2008). The moderating influence of privacy concern on the efficacy of privacy assurance mechanisms for building trust: A multiple-context investigation. *ICIS 2008 Proceedings*.

Bansal, G., Zahedi, F., & Gefen, D. (2010). The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decision Support Systems, 49*(2), 138–150.

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

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly, 35*(4), 1017–1042.

Bennett, C. J. (1992). *Regulating privacy: data protection and public policy in Europe and the United States.* Cornell University Press.

Boritz, E., & No, W. G. (2009). A gap in perceived importance of privacy policies between individuals and companies. *Paper presented at the Privacy, Security, Trust and the Management of e-Business*.

Brandimarte, L., Acquisti, A., & Loewenstein, G. (2013). Misplaced confidences privacy and the control paradox. *Social Psychological and Personality Science, 4*(3), 340–347.

Campbell, D. T., & Fiske, D. W. (1959). Convergent and discriminant validation by the multitrait-multimethod matrix. *Psychological Bulletin, 56*(2), 81–105.

Chellappa, R. K., & Pavlou, P. A. (2002). Perceived information security, financial liability and consumer trust in electronic commerce transactions. *Logistics Information Management, 15*(5/6), 358–368.

Chen, H., Chiang, R. H., & Storey, V. C. (2012). Business intelligence and analytics: From big data to big impact. *MIS Quarterly, 36*(4), 1165–1188.

Chin, W. W. (1998). The partial least squares approach to structural equation modeling. In G. A. Marcoulides (Ed.). *Modern methods for business research* (pp. 295–336). Hillsdale, NJ: Lawrence Erlbaum Associates.

Chua, H. N., Herbland, A., Wong, S. F., & Chang, Y. (2017). Compliance to personal data protection principles: A study of how organizations frame privacy policy notices. *Telematics and Informatics, 34*(4), 157–170.

Chua, H. N., Wong, S. F., Chang, Y., & Libaque-Saenz, C. F. (2017). Unveiling the coverage patterns of newspapers on the personal data protection act. *Government Information Quarterly, 34*(2), 296–306.

Cieh, E. L. Y. (2013). Personal data protection and privacy law in Malaysia. *Beyond data protection* (pp. 5–29). Springer.

Council of Europe (1987). Convention for the protection of individuals with regard to automatic processing of personal data. *From*https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108.

Culnan, M. J. (1993). " how did they get my name?": An exploratory investigation of consumer attitudes toward secondary information use. *MIS Quarterly, 17*(3), 341–363.

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science, 10*(1), 104–115.

Culnan, M. J., & Bies, R. J. (2003). Consumer privacy: Balancing economic and justice considerations. *Journal of Social Issues, 59*(2), 323–342.

Culnan, M. J., & Milberg, S. J. (1998). *The second exchange: Managing customer information in marketing relationships.* Unpublished manuscriptWashington, DC: Georgetown University.

Culnan, M. J., & Williams, C. C. (2009). How ethics can enhance organizational privacy: Lessons from the choicepoint and TJX data breaches. *MIS Quarterly, 33*(4), 673–687.

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

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

Dinev, T., & Hart, P. (2006b). Internet privacy concerns and social awareness as determinants of intention to transact. *International Journal of Electronic Commerce, 10*(2), 7–29.

Dinev, T., Xu, H., Smith, J. H., & Hart, P. (2013). Information privacy and correlates: An empirical attempt to bridge and distinguish privacy-related concepts. *European Journal of Information Systems, 22*(3), 295–316.

Dowling, G. R., & Staelin, R. (1994). A model of perceived risk and intended risk-handling activity. *Journal of Consumer Research, 21*(1), 119–134.

Drinkwater, D. (2016). Does a data breach really affect your firm's reputation. from http://www.csoonline.com/article/3019283/data-breach/does-a-data-breach-really-affect-your-firm-s-reputation.html.

Earp, J. B., & Baumer, D. (2003). Innovative web use to learn about consumer behavior and online privacy. *Communications of the ACM, 46*(4), 81–83.

Erevelles, S., Fukawa, N., & Swayne, L. (2016). Big data consumer analytics and the transformation of marketing. *Journal of Business Research, 69*(2), 897–904.

Faja, S., & Trimi, S. (2006). Influence of the web vendor's interventions on privacy-related behaviors in e-commerce. *Communications of the Association for Information Systems, 17*(1), 593–634.

Falk, R. F., & Miller, N. B. (1992). *A primer for soft modeling.* Akron, OH: University of Akron Press.

Flavián, C., & Guinalíu, M. (2006). Consumer trust, perceived security and privacy policy: Three basic elements of loyalty to a web site. *Industrial Management & Data Systems, 106*(5), 601–620.

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

Gashami, J. P. G., Chang, Y., Rho, J. J., & Park, M.-C. (2016). Privacy concerns and benefits in SaaS adoption by individual users: A trade-off approach. *Information Development, 32*(4), 837–852.

Gefen, D., Straub, D., & Boudreau, M.-C. (2000). Structural equation modeling and regression: Guidelines for research practice. *Communications of the Association for Information Systems, 4*(7), 1–77.

Gellman, R. (2017). Fair information practices: A basic history. from https://ssrn.com/abstract=2415020.

Hair, J. F., Sarstedt, M., Ringle, C. M., & Mena, J. A. (2012). An assessment of the use of partial least squares structural equation modeling in marketing research. *Journal of the Academy of Marketing Science, 40*(3), 414–433.

Hair, J. F. J., Black, W. C., Babin, B. J., & Anderson, R. E. (2009). *Multivariate Data Analysis.* Upper Saddle River, New Jersey: Pearson Prentice Hall.

Harding, A. (2001). Comparative law and legal transplantation in South East Asia: Making sense of the 'Nomic din'. *Adapting legal cultures* (pp. 199–222). Portland, OR: Hart.

Harris, P. (1996). Sufficient grounds for optimism?: The relationship between perceived controllability and optimistic bias. *Journal of Social and Clinical Psychology, 15*(1), 9–52.

Havlena, W. J., & DeSarbo, W. S. (1991). On the measurement of perceived consumer risk. *Decision Sciences, 22*(4), 927–939.

Hazen, B. T., Cegielski, C., & Hanna, J. B. (2011). Diffusion of green supply chain management: Examining perceived quality of green reverse logistics. *The International Journal of Logistics Management, 22*(3), 373–389.

Henseler, J., Hubona, G., & Ray, P. A. (2016). Using PLS path modeling in new technology research: Updated guidelines. *Industrial Management & Data Systems, 116*(1), 2–20.

Higgins, E. T. (1997). Beyond pleasure and pain. *American Psychologist, 52*(12), 1280–1300.

Hong, W., & Thong, J. Y. (2013). Internet privacy concerns: An integrated conceptualization and four empirical studies. *MIS Quarterly, 37*(1), 275–298.

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

Janssen, M., & Kuk, G. (2016). The challenges and limits of big data algorithms in technocratic governance. *Government Information Quarterly, 33*(3), 371–377.

Janssen, M., & van den Hoven, J. (2015). Big and open linked data (BOLD) in government: A challenge to transparency and privacy? *Government Information Quarterly, 32*(4), 363–368.

Janssen, M., van der Voort, H., & Wahyudi, A. (2017). Factors influencing big data decision-making quality. *Journal of Business Research, 70*(1), 338–345.

Joinson, A. N., Reips, U.-D., Buchanan, T., & Schofield, C. B. P. (2010). Privacy, trust, and self-disclosure online. *Human–Computer Interaction, 25*(1), 1–24.

Karyda, M. (2009). The socioeconomic background of electronic crime. *Socioeconomic and Legal Implications of Electronic Intrusion* (pp. 1–24).

Kehr, F., Kowatsch, T., Wentzel, D., & Fleisch, E. (2015). Blissfully ignorant: The effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. *Information Systems Journal, 25*(6), 607–635.

King, W. R., & Teo, T. S. (1996). Key dimensions of facilitators and inhibitors for the strategic use of information technology. *Journal of Management Information Systems, 12*(4), 35–53.

Klein, C. T., & Helweg-Larsen, M. (2002). Perceived control and the optimistic bias: A meta-analytic review. *Psychology and Health, 17*(4), 437–446.

Kock, N., & Hadaya, P. (2018). Minimum sample size estimation in PLS-SEM: The inverse square root and gamma-exponential methods. *Information Systems Journal, 28*(1), 227–261.
Lee, H., Lim, D., Kim, H., Zo, H., & Ciganek, A. P. (2015). Compensation paradox: The influence of monetary rewards on user behaviour. *Behaviour & Information Technology, 34*(1), 45–56.
Liang, H., Saraf, N., Hu, Q., & Xue, Y. (2007). Assimilation of enterprise systems: The effect of institutional pressures and the mediating role of top management. *MIS Quarterly, 31*(1), 59–87.
Libaque-Saenz, C. F., Chang, Y., Kim, J., Park, M.-C., & Rho, J. J. (2016). The role of perceived information practices on consumers' intention to authorise secondary use of personal data. *Behaviour & Information Technology, 35*(5), 339–356.
Libaque-Saenz, C. F., Chang, Y., Wong, S. F., & Lee, H. (2015). The power of fair information practices-A control agency approach. *Paper presented at the Australasian Conference on Information Systems, Australia*.
Libaque-Saenz, C. F., Wong, S. F., Chang, Y., Ha, Y. W., & Park, M.-C. (2016). Understanding antecedents to perceived information risks an empirical study of the Korean telecommunications market. *Information Development, 32*(1), 91–106.
Liu, C., Marchewka, J. T., Lu, J., & Yu, C.-S. (2005). Beyond concern—A privacy-trust-behavioral intention model of electronic commerce. *Information Management, 42*(2), 289–304.
Lowry, P. B., Cao, J., & Everard, A. (2011). Privacy concerns versus desire for interpersonal awareness in driving the use of self-disclosure technologies: The case of instant messaging in two cultures. *Journal of Management Information Systems, 27*(4), 163–200.
Lwin, M., Wirtz, J., & Williams, J. D. (2007). Consumer online privacy concerns and responses: A power–responsibility equilibrium perspective. *Journal of the Academy of Marketing Science, 35*(4), 572–585.
Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research, 15*(4), 336–355.
Manyika, J., Chui, M., Brown, B., Bughin, J., Dobbs, R., Roxburgh, C., et al. (2011). *Big data: The next frontier for innovation, competition and productivity.* McKinsey Global Institute.
Margulis, S. T. (2003). On the status and contribution of Westin's and Altman's theories of privacy. *Journal of Social Issues, 59*(2), 411–429.
Mattson, M., & Brann, M. (2002). Managed care and the paradox of patient confidentiality: A case study analysis from a communication boundary management perspective. *Communication Studies, 53*(4), 337–357.
Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review, 20*(3), 709–734.
Metzger, M. J. (2007). Communication privacy management in electronic commerce. *Journal of Computer-Mediated Communication, 12*(2), 335–361.
Milne, G. R., & Culnan, M. J. (2004). Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. *Journal of Interactive Marketing, 18*(3), 15–29.
Morey, T., Forbath, T., & Schoop, A. (2015). Customer data: Designing for transparency and trust. *Harvard Business Review, 93*(5), 96–105.
Nunnally, J. C. (1978). *Psychometric theory*. New York, NY: McGraw-Hill.
Organisation for Economic Cooperation and Development (OECD) (1980). OECD guidelines on the protection of privacy and transborder flows of personal data. from http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.
Pavlou, P. A. (2003). Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. *International Journal of Electronic Commerce, 7*(3), 101–134.
Pavlou, P. A., & Fygenson, M. (2006). Understanding and predicting electronic commerce adoption: An extension of the theory of planned behavior. *MIS Quarterly, 30*(1), 115–143.
Pavlou, P. A., Liang, H. G., & Xue, Y. J. (2007). Understanding and mitigating uncertainty in online exchange relationships: A principal–agent perspective. *MIS Quarterly, 31*(1), 105–136.
Petronio, S. (2002). *Boundaries of privacy*. Albany: State University of New York.
Petronio, S. (2012). *Boundaries of privacy: Dialectics of disclosure.* Suny Press.
Petronio, S. (2013). Brief status report on communication privacy management theory. *Journal of Family Communication, 13*(1), 6–14.
Pikkarainen, T., Pikkarainen, K., Karjaluoto, H., & Pahnila, S. (2004). Consumer acceptance of online banking: An extension of the technology acceptance model. *Internet Research, 14*(3), 224–235.
Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology, 88*(5), 879–903.
Prosser, W. L. (1960). Privacy. *California Law Review, 48*(3), 383–423.
Schwaig, K. S., Kane, G. C., & Storey, V. C. (2006). Compliance to the fair information practices: How are the fortune 500 handling online privacy disclosures? *Information Management, 43*(7), 805–820.
Sheehan, K. B. (1999). An investigation of gender differences in on-line privacy concerns and resultant behaviors. *Journal of Interactive Marketing, 13*(4), 24–38.
Smith, H. J. (1993). Privacy policies and practices: Inside the organizational maze. *Communications of the ACM, 36*(12), 104–122.
Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly, 20*(2), 167–196.
Smith, T. (2011). *Global Web Index Annual Report 2011: Welcome to social entertainment.* Global Web Index.
Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review, 154*(3), 477–564.
Solove, D. J. (2008). *Understanding privacy*. Cambridge, MA: Harvard University Press.
Sun, N., Morris, J., Xu, J., Zhu, X., & Xie, M. (2014). iCARE: A framework for big data-based banking customer analytics. *IBM Journal of Research and Development, 58*(5/6), 1–4.
Sutanto, J., Palme, E., Tan, C.-H., & Phang, C. W. (2013). Addressing the personalization-privacy paradox: An empirical assessment from a field experiment on smartphone users. *MIS Quarterly, 37*(4), 1141–1164.
Taddei, S., & Contena, B. (2013). Privacy, trust and control: Which relationships with online self-disclosure? *Computers in Human Behavior, 29*(3), 821–826.
Teo, T. S., Lim, V. K., & Lai, R. Y. (1999). Intrinsic and extrinsic motivation in internet usage. *Omega, 27*(1), 25–37.
TRUSTe (2011). Smart Privacy for Smartphones: Understanding and delivering the protection consumers want. from www.truste.com.
Tsai, J. Y., Egelman, S., Cranor, L., & Acquisti, A. (2011). The effect of online privacy information on purchasing behavior: An experimental study. *Information Systems Research, 22*(2), 254–268.
Van Slyke, C., Shim, J., Johnson, R., & Jiang, J. J. (2006). Concern for information privacy and online consumer purchasing. *Journal of the Association for Information Systems, 7*(6), 415–444.
Westin, A. F. (1967). *Privacy and freedom.* New York: Atheneum.
Wirtz, J., & Lwin, M. O. (2009). Regulatory focus theory, trust, and privacy concern. *Journal of Service Research, 12*(2), 190–207.
Wu, K.-W., Huang, S. Y., Yen, D. C., & Popova, I. (2012). The effect of online privacy policy on consumer privacy concern and trust. *Computers in Human Behavior, 28*(3), 889–897.
Xu, H. (2007). The effects of self-construal and perceived control on privacy concerns. *Paper presented at the proceedings of the 28th annual international conference on information systems (ICIS 2007), Montréal, Canada*.
Xu, H., Dinev, T., Smith, J., & Hart, P. (2011). Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems, 12*(12), 798–824.
Xu, H., Teo, H.-H., Tan, B. C., & Agarwal, R. (2012). Effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: A study of location-based services. *Information Systems Research, 23*(4), 1342–1363.
Yamaguchi, S. (2001). Culture and control orientations. *The handbook of culture and psychology* (pp. 223–243).
Yiu, C. S., Grant, K., & Edgar, D. (2007). Factors affecting the adoption of internet banking in Hong Kong—Implications for the banking sector. *International Journal of Information Management, 27*(5), 336–351.

Younghoon Chang is an Associate Professor in the School of Management and Economics at Beijing Institute of Technology, Beijing, China. He received his PhD degree in Business & Technology Management from Korea Advanced Institute of Science and Technology (KAIST), South Korea. His research interests include Information privacy, ICT4D, e-business, business analytics and HCI. His articles have appeared in the Government Information Quarterly, 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 editorial review board member of Journal of Computer Information Systems.

Siew Fan Wong is an Adjunct Associate Professor in the Department of Computing and Information Systems at Sunway University, Malaysia. She received her PhD degree in MIS from the University of Houston, Texas. Her research interests involve organizational IT strategy, digital inclusion, information privacy and business analytics. Her publications have appeared in journals such as the Government Information Quarterly, Journal of Global Information Management, International Journal of Information Management, Industrial Management & Data Systems, Information Development, and Telematics and Informatics as well as in the proceedings of international conferences. She is currently serving as an associate editor of International Journal of Business Intelligence Research.

Christian Fernando Libaque-Saenz is a Professor and Researcher at Universidad del Pacífico, Lima, Peru. He received his BS degree in Telecommunications Engineering from the Universidad Nacional de Ingeniería (Lima-Peru), and his MA and PhD 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, Behavior and Information Technology, Telematics and Informatics, as well as in international conferences.

Hwansoo Lee is an Assistant Professor in the Department of Convergence Security at Dankook University, South Korea. He received his PhD degree in Business & Technology Management from Korea Advanced Institute of Science and Technology (KAIST), South Korea. His research focuses on information security & privacy, electronic commerce, and enterprise information systems. His papers have appealed in journals such as Information & Management, Behaviour & Information Technology, Journal of Artificial Societies and Social Simulation, Journal of Global Information Management, Telematics & Informatics. He also received the Best Paper awards at various international and domestic conferences. Further, he has well-qualified experiences related to information systems as a developer and a system analyst. He is currently serving as an editorial review board member of Industrial Management and Data Systems.