UNDERSTANDING PERCEIVED PRIVACY: A PRIVACY BOUNDARY MANAGEMENT MODEL

Younghoon Chang, Department of Computing and Information Systems, Sunway University, Petaling Jaya, Malaysia, younghoonc@sunway.edu.my

Siew Fan Wong, Department of Computing and Information Systems, Sunway University, Petaling Jaya, Malaysia, siewfanw@sunway.edu.my

Hwansoo Lee, IT Law Program, Dankook University, Yongin-si, Republic of Korea, hanslee992@gmail.com

Abstract

Consumer data is asset to organizations. Analysis of consumers' transactional data helps organizations to understand customer behaviors and preferences. Before organizations could capitalize on these data, they ought to have effective plans to address consumers' privacy concerns because violation of consumer privacy brings long-term reputational damage to organizations. This paper proposes and tests a Privacy Boundary Management Model that explains how consumers formulate and manage their privacy boundary. Survey data was collected from 98 users of online banking websites who have used the system for a minimum of six months. The PLS results showed that the model accounts for high variance in perceived privacy. Three elements of the FIPs (notice, access, and enforcement) have significant impact on perceived effectiveness of privacy policy. Perceived effectiveness in turns significantly influences privacy control and privacy risks. Privacy control affects perceived privacy and trust while privacy risk influences privacy concern and perceived privacy. Privacy concern has a negative relationship with perceived privacy and trust has a positive relationship with perceived privacy. The findings have novel implications for organizations and policy makers.

Keywords: Perceived privacy, Perceived effectiveness, Privacy policy, Fair information practices, Privacy boundary management

1 INTRODUCTION

Every day, an unfathomable amount of data flows through the Internet. This data contains information ranging from simple every day conversation to complex and highly sensitive personal data and monetary transactions. Each piece of data leaves behind electronic trails of user activities. When properly collected, stored, and processed, the data allows organizations to understand customer behaviors and preferences. Such knowledge is valuable in customizing and personalizing products and services to meet consumer needs, thereby equipping companies with competitive advantage. In fact, consumer data is the backbone that supports the current trend of big data, analytics, and Internet of Things (IoT). Therefore, data is the propeller of knowledge economy that is built on a globalized ICT ecosystem.

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. Consumers who are the data owners are concerned about how companies collect, process, share, distribute, and use their private information. This concern is further elevated with the increasing cases of privacy invasion and online information leak. Data breach and violation of customer privacy have long-term damaging effect on companies as they risk substantial consumer backlash (Culnan 1993). Therefore, companies must devise effective privacy management plan to address privacy issues if they want to capitalize on customers' private data. This requires knowledge of how consumers perceive their information privacy and how they formulate and manage their privacy boundary.

This paper proposes and tests a Privacy Boundary Management Model (PBMM). It builds on Petronio's (2012) Communication Privacy Management (CPM) and Xu et al.'s (2011) application of the CPM in the context of information privacy to provide a wholesome view of consumers' privacy boundary management process. The model incorporates the existing Fair Information Practices (FIPs) into the boundary coordination and turbulence process to examine how consumers link the dimensions of FIPs to the effectiveness of privacy policy. It also studies perceived privacy as the dependent variable, thereby differentiating the concept from its proxies of privacy concern and trust.

2 PRIVARY BOUNDARY MANAGEMENT MODEL

2.1 Communication Privacy Management Theory

The overarching theory for this study is the Communication Privacy Management (CPM) theory. CPM theorizes the privacy management process where people make decisions about revealing and concealing their private information (Petronio 2012). It uses a boundary metaphor to suggest that individuals follow a rule-based system to constantly adjust, maintain, and coordinate their privacy boundaries based on the perceived benefits and costs of information disclosure.

CPM identifies three rule management elements: boundary rule formation, boundary coordination, and boundary turbulence. 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 thus want to maintain control of what, when, and with whom it is shared. When private information is kept with one owner, the boundary is considered thick because there is less possibility for information to make it out to the public. Once private information is shared with another party, the boundary becomes thin and more permeable.

Information within a personal boundary is considered private and thus not disclosed to others. When individuals share their private information, this information moves to the collective boundary where the data owners and the data recipients become co-owners with joint responsibility to keep the information private. Ownership conveys both rights and obligations. The co-ownership implies the beginning of collective data control and mutual boundary coordination by both the data owners and the data recipients. The coordination process is complex because each owner approaches the information from their distinct viewpoints and personal criteria. Hence, it requires understanding between the parties on how to coordinate the ownership of the information and knowledge. Nonetheless, 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, who it should be shared with, and when it should be shared.

At times, boundary coordination process fails which leads to turbulence (Petronio 2012). When turbulence happens, individuals may seek recourse from third party assurances such as government regulations or industrial standards (Xu et al. 2011).

2.2 A Cognitive Process Model of Privacy Boundary Management

An individual's privacy boundary management follows a three-phase procedure from institutional boundary identification to mutual boundary rule formation and finally to individual boundary decision (Figure 1). This process is recursive and iterative in nature where individuals constantly adjust their privacy boundary based on latest experience and information gathered. This means a decision to open up a boundary today could be replaced with an opposite choice to close the boundary.

In the institutional boundary identification phase, the goal is to decide how effective an organization is in implementing and practicing the existing privacy policy. This phase is important as it serves as the foundation for the subsequent two phases. Since FIPs are commonly referenced in the literature (Culnan et al. 1999; Wu et al. 2012), we evaluate the policy here. The five core principles of FIPs are notice, choice, access, security, and enforcement. Notice refers to the disclosure of an organization's information policies to customers before any personal information is collected (Liu et al. 2005). Choice means giving consumers the option to select which personal information collected can be used and how it will be used (Liu et al. 2005). Access is the possibility of consumers accessing their stored personal information to view and check for data accuracy and completeness (Wu et al. 2012). Security refers to the assurances for keeping the data accurate and secure (Liu et al. 2005; Wu et al. 2012) to ensure data integrity. Enforcement is the administration and prosecution of the privacy policy by organizations.

We argue that three processes take place during the institutional boundary identification phase: boundary coordination, boundary turbulence, and boundary assurance. In boundary coordination, consumers evaluate the notice, choice, and access provided by organizations to determine how to organize their boundary. When undesirable incidents happen, boundary turbulence mode kicks in where consumers reference security measures of an organization and 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.

With perceived effectiveness of privacy policy on hand, consumers move to the second phase which is mutual boundary rule formation. We call it mutual boundary because here consumers need to compare the privacy boundary practiced in an organization with their own inherent need for privacy protection. They will perform 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 will move to the last phase which is the individual boundary decision phase. The boundary rule formed in the previous phase will serve as the foundation to which consumers reach a self-assessed state where others have limited access to information about him or her. Consumers will also balance the negative attitude of privacy concern with the positive attitude of trust to reach a finalized, self-assessed state of perceived privacy.

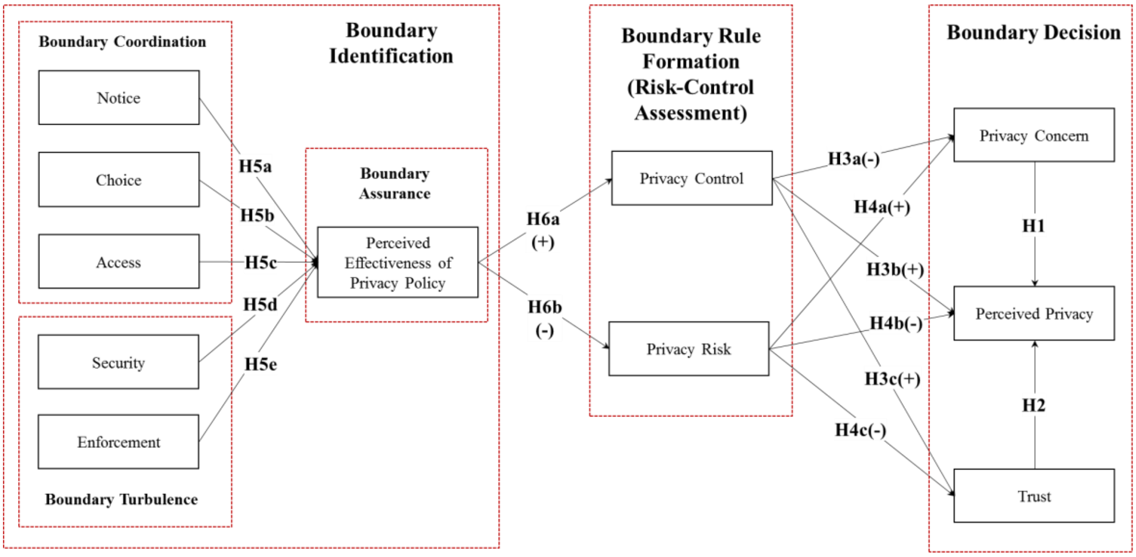

Figure 1. The proposed privacy boundary management model.

3 RESEARCH MODEL

3.1 Perceived Privacy

Perceived (state of) privacy refers to 'an individual's self-assessed state in which external agents have limited access to information about him or her' (Dinev et al. 2013). Most research treat privacy as a state whether it is implicitly or explicitly (Dinev et al. 2013). For example, Westin (1967) discusses 'states of privacy' and both Altman (1975; 1976) and Westin (1967) refer to 'state of control' and 'state of limited access'. When privacy is perceived as a state, it means an individual is found in a given situation at a given moment of time where decision related to their privacy matters has to be made.

Privacy concern and trust are two known proxies of perceived privacy (Dinev et al. 2013; Flavián et al. 2006). Privacy concern refers to individuals' level of anxiety regarding a third party's information practices (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 et al. 2008). Both privacy concern and trust are attitudinal factors indicating people's current mental state toward certain objectives (Vaske et al. 1999). 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 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; Smith et al. 2011).

H1: Privacy concern negatively influences perceived privacy.

H2: Trust positively influences perceived privacy.

3.2 Risk-Control Assessment

The calculus perspective of privacy which incorporates the interplay between risk and control (Dinev et al. 2006a; Dinev et al. 2013) is 'the most useful framework for analyzing contemporary consumer privacy concerns' (Culnan et al. 2003). 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 et al. 2002). This implies individuals will assess the associated risk as less serious and are therefore more willing to take risk (Brandimarte et al. 2013). The interplay between risk and control will influence individuals' perceived privacy.

In information disclosure, perceived information control is defined as individuals' beliefs of their ability to manage the release and dissemination of their private data (Westin 1967; Xu et al. 2011). Perceived information control explains high variance in privacy concerns (Dinev et al. 2004). When people have a sense of control over their private information, they tend to have a lower level of privacy concerns (Culnan et al. 1999; Malhotra et al. 2004; Xu et al. 2011). Hence, the relationship between privacy control and privacy concerns is a negative one. At the same time, the lack of perceived control will reduce customers' trust toward an organization (Joinson et al. 2010) and their perceived privacy (Dinev et al. 2006a; Dinev et al. 2013).

H3a: Privacy control negatively influences privacy concern.

H3b: Privacy control positively influences perceived privacy.

H3c: Privacy control positively influences trust.

Perceived risk is 'the expectation of losses associated with the disclosure of personal information' (Xu et al. 2011). It introduces uncertainty resulting from the potential of negative outcomes (Havlena et al. 1991). The value chain of online transactions starting from information collection to processing, dissemination, and storing is embedded with 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 raise concerns on who will have access to their private information and how these information will be used (Dinev et al. 2006a; Dinev et al. 2006b; Xu et al. 2011). Higher sense of risk will also reduce consumer trust toward the ability of organizations to protect their information (Jarvenpaa et al. 2000; Kim et al. 2008; Malhotra et al. 2004). It will also increase their privacy concern (Dinev et al. 2006b; Malhotra et al. 2004; Van Slyke et al. 2006; Xu et al. 2011) and reduce their perceived privacy (Dinev et al. 2013; Petronio 2012).

H4a: Privacy risk positively influences privacy concern.

H4b: Privacy risk negatively influences perceived privacy.

H4c: Privacy risk negatively influences trust.

3.3 Privacy Policies and Its Perceived Effectiveness

Privacy policies can help to build customer trust and reduce privacy concern (Westin 1967; Wu et al. 2012). These policies inform customers 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 build consumer trust and reduce the fear that their personal information will be disclosed (Westin 1967). Current privacy policies are built around the US Federal Trade Commission's FIPs. FIPs are the prevailing global data protection principles which define guidelines for individual rights and organizational responsibilities (Bennett 1992; Culnan et al. 2009). While implementation of FIPs is voluntary, its adoption provides an evaluation tool for consumers to judge an organization's information practices and degree of responsiveness (Smith 1993).

Among the five core principles of FIPs, 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 important means to reduce consumers' privacy concerns (Wu et al. 2012) and improve their privacy perception (Faja et al. 2006). It helps consumers to decide whether or not they want to provide private data or choose not to engage with the particular website (Culnan et al. 1998). In an online environment, informativeness reduces perceived uncertainties (Pavlou et al. 2007). When customers see a website providing resourceful coverage of its privacy policies, consumer confidence toward the website increases (Earp et al. 2003).

This suggests that their perception toward the effectiveness of privacy policy in the website will also increase.

Besides notifying consumers on privacy practices, organizations should also give choices to consumers to select 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 to and 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), choice put the decision into the hands of the consumers to decide on their private information collection and use. Similar to the notification policy, when consumers are given choices, they will have better perception toward the privacy policy implementation in an organization as well as its level of effectiveness.

Consumers should also be given the option 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, their will have more favorable perception toward the effectiveness of privacy policy in an organization.

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 when store on physical properties. Consumers often measure the risk of online activities via the possibility of information privacy misuse or revelation (Milne et al. 2004). In fact, previous research has established the link between perceived security and trust in e-commerce transactions (Chellappa et al. 2002; Liu et al. 2005). Therefore, many websites try to fortify security perceptions by establishing relationships with third party assurance such as TRUSTe. TRUSTe 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 method, Hui et al. (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 FIPs which is ‘notice’. If consumers have a guarantee that the information they provide online is secured and will not be misused, there is higher likelihood that they will perceive the privacy practices in the organization as effective.

Enforcement ensures organizations are observant and obedient to the imposed regulations and policies. In this study, it is the FIPs. Enforcement can only be effective if there is a mechanism or instrument in place to enforce the principles (Wu et al. 2012). When FIPs are enforced in organizations by the law, consumers will have better perception toward the effectiveness of the privacy policy.

Based on the arguments above, we hypothesize that the presence of each of the five dimensions of privacy policy will help to improve consumer perception toward the effectiveness of the policy.

H5a: Notice positively influences perceived effectiveness of privacy policy.

H5b: Choice positively influences perceived effectiveness of privacy policy.

H5c: Access positively influences perceived effectiveness of privacy policy.

H5d: Security positively influences perceived effectiveness of privacy policy.

H5e: Enforcement positively influences perceived effectiveness of privacy policy.

Perceived effectiveness of privacy policy is ‘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). Previous literature found that an organization’s provision of privacy notice increases consumers’ perceived privacy control (Culnan et al. 2003; Milne et al. 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 et al. 1999; Xu et al. 2011).

H6a: Perceived effectiveness of privacy policy positively influences privacy control.

H6b: perceived effectiveness of privacy policy negatively influences perceived risk.

4 METHOD

4.1 Scale Development

To develop the measurement items, we adapted validated standard scales from the literature. Items for measuring perceived privacy were adopted from Dinev et al. (2013) while items for measuring trust came from Wu et al. (2012). We measured privacy concerns using four Likert-scale items from Dinev et al. (2006b). Perceived privacy risks were measured using four Likert-scale questions adapted from Dinev et al. (2006a) and Malhotra et al. (2004). Perceived privacy control and perceived effectiveness of privacy policy were measured using items taken from Xu et al. (2011). Items that measure the five dimensions of FIPs came from Wu et al. (2012). 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 the privacy practices of the particular website. This practice of specifying a research context is in-line with previous privacy research (Petronio 2012; Xu et al. 2011) that argue privacy concerns are domain-specific and must be studied in that context. Furthermore, sites utilizing more specific data types are associated with higher percentages of explained variance (Xu et al. 2011).

Construct	Items	Measurement Items
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:
	PRIV1	I feel I have enough privacy when I use this online banking service.
	PRIV2	I am comfortable with the amount of privacy I have when using this online banking service.
	PRIV3	I think my online privacy is preserved when I use this online banking service.
Privacy Concern	PCON1	I am concerned that the information I submit to this online banking service could be misused.
	PCON2	I am concerned that others can find private and personal information about me from this online banking service.
	PCON3	I am concerned about providing personal information to this online banking service because of what others might do with it.
	PCON4	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.
	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 Privacy Risk	RISK1	In general, it would be risky to give personal information to this online banking service.
	RISK2	There would be high potential for privacy loss associated with giving personal information to this online banking service.
	RISK3	Personal information could be inappropriately used by this online banking service.
	RISK4	Providing this online banking service with my personal information would involve many unexpected problems.
Perceived Control	PCTL1	I believe I have control over who can get access to my personal information collected by this online banking service.
	PCTL2	I think I have control over what personal information is released by this online banking service.

	PCTL3	I believe I have control over how personal information is used by this online banking service.
	PCTL4	I believe I can control my personal information provided to this online banking service.
Perceived Effectiveness of Privacy Policy		Some banks post privacy statements on their web sites to give information about their information practices, e.g., what information is collected, how your information is used, and with whom your information may be shared. Please indicate the extent to which you agree or disagree with each statement by ticking the appropriate number:
	POLY1	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.
	POLY2	With their privacy statements, I believe that my personal information will be kept private and confidential by the bank.
	POLY3	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.
	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.
	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.
	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.
	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.
Enforcement	ENF1	This online banking service discloses that there is a law sanctioning those who violate the privacy statements.
	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 1. Measurement Items.

4.2 Survey Administration

We approached potential participants at random in four largest shopping malls in Malaysia and asked for their willingness to participate in the study. Once 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 put in to ensure that the participants have sufficient experience with online banking services. A total of 98 participants who met the requirements answered our survey. In answering the questions, the participants were asked to recall their experiences in using one banking website that they most frequented in the past one month. Table 2 shows the demographic details of the participants.

5 RESULTS

We used Partial Least Squares (PLS) for the data analysis. PLS is a powerful second generation modeling technique that analyzes complex causal models involving multiple constructs with multiple observed items (Chin 1998). It assesses both measurement and structural models simultaneously in an optimal fashion. PLS places minimal restrictions on measurement scales, sample size, and residual distributions. It is suitable for testing theory in exploratory studies. The software utilized was SmartPLS 2.0 (Ringle et al. 2014). All constructs were modeled as reflective measures.

Respondents		**n=98**	
		Frequency	**Percent (%)**
Gender	Male	45	45.9
	Female	53	54.1
Age	Below 20	13	13.3
	20~29	17	17.3
	30~39	20	20.4
	40~49	20	20.4
	50~59	17	17.3
	60 and above	11	11.2
Time using Online Banking	6 month to 1 year	5	5.1
	1~2 years	19	19.4
	3~4 years	18	18.4
	5~7 years	25	25.5
	8~10 years	16	16.3
	More than 10 years	15	15.3

Table 2. Demographic information of the participants.

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 et al. 2000; Hair et al. 2009). Convergent validity is determined by item reliability, composite reliability, and average variance extracted (AVE). In Table 3, the composite reliabilities were also above the recommended 0.70 level (Nunnally 1978), whereas the AVEs were above 0.50 for all constructs (Fornell et al. 1981). Also, in Table 4, all item loadings were greater than 0.707, suggesting that more variance was shared between an item and its construct than there was error variance (Hair et al. 2012). Therefore, the measurement model in our study demonstrated good convergent validity.

Con-struct	**AVE**	**CR**	**CA**	**ACC**	**CHO**	**PCON**	**PCTL**	**POLY**	**ENF**	**NTC**	**PRIV**	**RISK**	**SEC**	**TRU**
ACC	0.91	0.97	0.95	**0.96**										
CHO	0.81	0.93	0.88	0.58	**0.90**									
PCON	0.80	0.94	0.92	-0.52	-0.45	**0.89**								
PCTL	0.88	0.97	0.95	0.83	0.51	-0.52	**0.94**							
POLY	0.93	0.98	0.96	0.83	0.55	-0.58	0.88	**0.96**						
ENF	0.95	0.98	0.97	0.79	0.61	-0.52	0.77	0.80	**0.97**					
NTC	0.79	0.92	0.87	0.71	0.70	-0.57	0.69	0.73	0.74	**0.89**				
PRIV	0.96	0.99	0.98	0.82	0.47	-0.62	0.82	0.83	0.76	0.65	**0.98**			
RISK	0.76	0.93	0.90	-0.66	-0.44	0.69	-0.69	-0.72	-0.61	-0.52	-0.71	**0.87**		
SEC	0.90	0.96	0.94	0.81	0.64	-0.57	0.75	0.77	0.86	0.77	0.76	-0.65	**0.95**	
TRU	0.86	0.97	0.97	0.80	0.46	-0.47	0.86	0.86	0.78	0.69	0.79	-0.61	0.73	**0.93**

Note: CR = Composite Reliability; CA = Cronbach's Alpha; AVE = Average Variance Extract; ACC = Access; CHO = Choice; PCON = Privacy Concerns; PCTL = Perceived Control; POLY = Effectiveness of the Policy; ENF = Enforcement, NTC = Notice; PRIV = Privacy; RISK = Perceived Privacy Risk; SEC = Security; TRU = Trust

Table 3. Reliability and validity.

Discriminant validity is the degree to which items measuring different constructs are distinct (Campbell et al. 1959). The square roots of all AVEs were much larger than the corresponding cross-correlations

(Table 3), and each item loaded most strongly on its corresponding construct (Table 4). These results suggest adequate discriminant validity (Fornell et al. 1981).

Items	**ACC**	**CHO**	**PCON**	**ENF**	**NTC**	**PCTL**	**POLY**	**PRIV**	**RISK**	**SEC**	**TRU**
ACC1	**0.96**	0.60	0.80	0.75	0.66	-0.46	0.79	0.76	-0.61	0.75	0.75
ACC2	**0.96**	0.54	0.79	0.79	0.70	-0.48	0.80	0.78	-0.61	0.80	0.78
ACC3	**0.95**	0.51	0.79	0.72	0.67	-0.56	0.79	0.80	-0.66	0.79	0.77
CHO1	0.47	**0.86**	0.45	0.60	0.69	-0.43	0.46	0.43	-0.34	0.58	0.41
CHO2	0.55	**0.95**	0.51	0.55	0.65	-0.39	0.53	0.44	-0.44	0.60	0.44
CHO3	0.54	**0.89**	0.42	0.50	0.56	-0.41	0.48	0.39	-0.41	0.55	0.39
PCON1	0.74	0.40	**0.91**	0.68	0.59	-0.43	0.77	0.72	-0.60	0.64	0.78
PCON2	0.71	0.47	**0.93**	0.64	0.60	-0.50	0.75	0.72	-0.61	0.63	0.75
PCON3	0.79	0.51	**0.96**	0.75	0.66	-0.49	0.85	0.77	-0.66	0.74	0.83
PCON4	0.85	0.54	**0.95**	0.80	0.71	-0.52	0.89	0.85	-0.70	0.79	0.86
ENF1	0.77	0.62	0.76	**0.97**	0.73	-0.50	0.80	0.74	-0.58	0.85	0.76
ENF2	0.78	0.59	0.75	**0.98**	0.74	-0.53	0.78	0.75	-0.60	0.85	0.74
ENF3	0.75	0.57	0.74	**0.97**	0.69	-0.48	0.76	0.73	-0.60	0.82	0.76
NTC1	0.74	0.58	0.69	0.73	**0.88**	-0.58	0.73	0.67	-0.58	0.74	0.72
NTC2	0.66	0.64	0.66	0.69	**0.95**	-0.52	0.69	0.61	-0.48	0.74	0.63
NTC3	0.45	0.66	0.43	0.51	**0.84**	-0.40	0.47	0.40	-0.29	0.55	0.42
PCTL1	-0.53	-0.40	-0.47	-0.51	-0.56	**0.87**	-0.55	-0.54	0.57	-0.51	-0.49
PCTL2	-0.50	-0.34	-0.51	-0.51	-0.46	**0.90**	-0.53	-0.59	0.67	-0.54	-0.46
PCTL3	-0.45	-0.42	-0.44	-0.45	-0.51	**0.92**	-0.52	-0.58	0.64	-0.53	-0.39
PCTL4	-0.39	-0.48	-0.43	-0.37	-0.52	**0.89**	-0.46	-0.49	0.58	-0.47	-0.33
POLY1	0.81	0.55	0.84	0.78	0.71	-0.61	**0.96**	0.81	-0.72	0.77	0.81
POLY2	0.80	0.53	0.87	0.78	0.70	-0.55	**0.98**	0.81	-0.69	0.75	0.85
POLY3	0.78	0.50	0.82	0.76	0.69	-0.51	**0.96**	0.79	-0.67	0.72	0.84
PRIV1	0.82	0.47	0.80	0.76	0.65	-0.62	0.84	**0.98**	-0.71	0.76	0.80
PRIV2	0.79	0.45	0.79	0.73	0.64	-0.59	0.80	**0.98**	-0.67	0.75	0.74
PRIV3	0.80	0.44	0.81	0.75	0.62	-0.60	0.81	**0.98**	-0.70	0.74	0.78
RISK1	-0.53	-0.41	-0.54	-0.44	-0.51	0.64	-0.51	-0.54	**0.79**	-0.51	-0.43
RISK2	-0.57	-0.43	-0.60	-0.55	-0.47	0.59	-0.67	-0.60	**0.91**	-0.57	-0.53
RISK3	-0.59	-0.40	-0.61	-0.56	-0.47	0.65	-0.65	-0.68	**0.92**	-0.57	-0.55
RISK4	-0.60	-0.31	-0.67	-0.56	-0.39	0.53	-0.66	-0.65	**0.86**	-0.60	-0.59
SEC1	0.80	0.61	0.71	0.82	0.74	-0.56	0.75	0.73	-0.60	**0.95**	0.70
SEC2	0.76	0.59	0.72	0.78	0.75	-0.58	0.72	0.73	-0.66	**0.95**	0.67
SEC3	0.75	0.62	0.71	0.85	0.70	-0.49	0.73	0.71	-0.58	**0.94**	0.70
TRU1	0.69	0.44	0.76	0.72	0.62	-0.47	0.74	0.65	-0.51	0.64	**0.87**
TRU2	0.75	0.42	0.83	0.75	0.66	-0.47	0.83	0.73	-0.58	0.71	**0.94**
TRU3	0.77	0.46	0.84	0.73	0.65	-0.39	0.84	0.75	-0.53	0.67	**0.94**
TRU4	0.78	0.46	0.82	0.73	0.69	-0.45	0.84	0.76	-0.59	0.72	**0.96**
TRU5	0.74	0.38	0.77	0.66	0.59	-0.40	0.78	0.73	-0.58	0.63	**0.92**
TRU6	0.73	0.38	0.76	0.72	0.60	-0.42	0.78	0.74	-0.58	0.68	**0.92**

Note: ACC = Access; CHO = Choice; PCON = Privacy Concerns; PCTL = Perceived Control; POLY = Effectiveness of the Policy; ENF = Enforcement, NTC = Notice; PRIV = Privacy; RISK = Perceived Privacy Risk; SEC = Security; TRU = Trust

Table 4. Loadings and Cross-loadings.

We conducted additional multicollinearity test because several high correlations were found between the constructs (Table 3). We assessed the variance inflation factor (VIF) which quantifies the severity of multicollinearity. The results showed that that the VIFs were all lesser than 10. Based on guidelines provided in previous research (Lee, 2009), there is no serious concern of multicollinearity in our data.

5.2 Structural Model

After confirmation of acceptable psychometric properties for the measurement model, we examined the structural model (Figure 2). The predictive power of the structural model is assessed using R^2 in the endogenous constructs (Chin 1998; Gefen et al. 2000). Seventy-five percent of the variance in perceived privacy, 74 percent of the variance in trust, 48 percent of the variance in privacy concerns, 77 percent of the variance in privacy control, 52 percent of the variance in privacy risk, and 76 percent of the variance in perceived effectiveness of privacy policy were accounted for by the model. Since the percentages of variance explained were far greater than 10 percent, it indicates a satisfactory and substantive model (Falk et al. 1992).

The results show that perceived privacy is determined by privacy concerns, trust, privacy control, and privacy risk. Privacy control has the strongest effect, followed by trust, privacy concern, and privacy risk. Privacy control and privacy risk have interesting relationship with privacy concerns and trust. Privacy control exerts significant effect on trust but not privacy concerns. On the contrary, privacy risk exerts significant control on privacy concerns but not trust. The effectiveness of privacy policy has significant effect on both privacy control and privacy risk. Access has the strongest effect on effectiveness of privacy policy, followed by enforcement, and notice. Choice and security do not have significant effect on effectiveness of privacy policy.

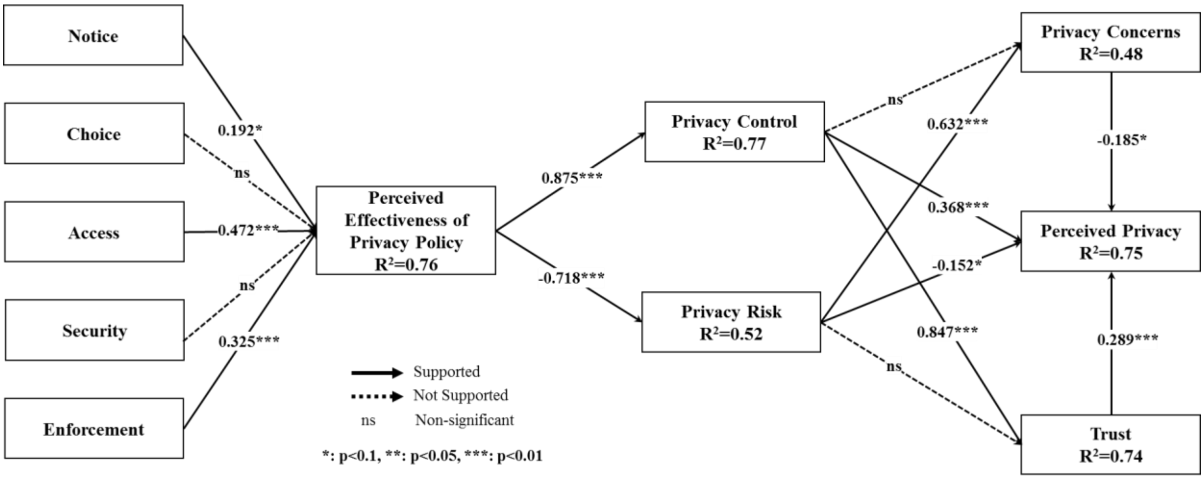

Figure 2. PLS results for the privacy boundary management model.

6 DISCUSSION AND IMPLCATIONS

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. The majority of the hypotheses are supported. The exceptions are the relationship between choice and perceived effectiveness, security and perceived effectiveness, privacy control and privacy concern, and privacy risk and trust.

Consumers have the options to choose whether to disclose their information. In fact, they can select the level of choice during the information disclosing process, and they can refuse to disclose information if they do not want to. Since it is a choice governed by themselves, it is not surprising to see consumers perceive 'choice' as a less important factor to link to the effectiveness of an organization's privacy policy. In the case of security, it is a fundamental condition for organizations to process any information, especially private information. Since it is a basic technological feature, consumers assume this to be in existence in all cases and therefore should not have any important impact on the effectiveness of privacy policy.

The strong effect of other antecedents nullify the relationship between privacy control and privacy concern, and privacy risk and trust. This can be explained from the perspectives of an individual or firm-specific measure. Trust has various modes such as process, characteristic, and institutional-based which can be of an individual disposition or firm-specific attribute (Bansal et al. 2010). In this study, trust measures consumers' faith toward a company's attribute, which is their privacy practices. Privacy control also measures indirectly the power given by organizations to consumers to manage the release and dissemination of their private data. If an organization is transparent about their privacy policy, consumers will feel stronger control over their data. Since privacy control and trust both measure the disposition toward an organization's privacy practice, it is natural that they correlate.

On the other hand, privacy risk and privacy concern are both individual disposition. Privacy risk is the possibility of loss undertaken by an individual while privacy concern is the degree of anxiety an individual holds toward the loss of privacy. Since privacy concerns are a negative attitude or feeling about possible loss of privacy, and privacy risk is the expectation of losses, it makes sense for an expectation to lead to a negative attitude.

6.2 Contributions and Implications

This study makes several contributions. First, it builds a comprehensive model to explain individuals' privacy boundary management process. It complements Xu et al. (2011) by identifying the factors that affect privacy assurance. It also pairs privacy concern and trust to investigate their effect on perceived privacy. 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 will help organizations to develop effective privacy practices and governance strategy. The model proposed in this paper identifies how individuals process institutional level policy and compare that with their own inherent need for privacy protection 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.

Second, this study tested the dimensions of FIPs that will 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 contrary, a positive perception could elevate the status of an organization among its peers. The results clearly identify the elements organizations could manipulate to increase positive perception toward privacy policy implementation in organizations. The findings, being the premier in studying how FIPs link to perceived effectiveness, also enrich existing understanding of consumer privacy in the literature.

Third, the study evaluates the interplay effect between privacy concern and trust on perceived privacy. The results show that trust has stronger effect than privacy concern on perceived privacy. This underscores the value of creating a trusting environment. Previous research (Bansal et al. 2008; Milne et al. 2002) found that the quality of an organization's privacy-policy statements in terms of the content (adequacy) and format (understandability) is important in creating a trusting environment between an organization and its customers. Since privacy concern often arises from improper information practice by organizations (Wu et al. 2012), a trusting environment instils confidence into customers that their data will be safe and will not be misused.

Fourth, this study also has implications for policy makers. The FIPs have been in existence for sometimes. With changing business environment, there is a need to revisit and revise the policy accordingly to fit the existing business conditions. The results of this study show that in the banking and financial sector, choice and security are not significant factors influencing perceived effectiveness. Since privacy is context specific (Petronio 2012; Xu et al. 2011), policy makers may need to design industry-specific guidelines to fit different consumer privacy needs.

6.3 Limitations and Future Research

As with other empirical research, the current study has some limitations that should be taken into account. 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) supports our decision to focus on one sector and contends that privacy decision is context-specific. Therefore, privacy research should consider context differences. We believe that our model on a higher, more general level is extendable to other settings. Compared to many other online transactional data, the banking and financial sector contains sensitive private wealth information that many consumers would be reluctant to disclose to third parties. Therefore, we expect consumers to act more conservatively when it comes to the sharing and disclosure of their banking data. In future studies, we plan to compare consumer privacy boundary decision in different contexts. We are targeting the banking, e-commerce, and social network sectors as they carry information with different sensitivity level. Banks carry the most sensitive information, e-commerce contains data with medium level of sensitivity, and social network has data with low sensitivity. It will be interesting to identify how consumers' privacy boundary management differ based on the sensitivity level of their private data.

Second, the sample size for this study is only 98. While as an exploratory study, this size may be sufficient, in future studies, we plan to collect a larger sample using stratified sampling to categorize users into either age groups or experience with online transactions. As argue by Petronio (2012), age is an important factor in boundary management. Generation Z who are much younger grow up with technology. Their privacy boundary and tolerance level is different from generation X who only have accessed to technology when they become adults.

7 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, whilst exploratory, is novel in that the existing empirical research has not linked FIPs to perceived effectiveness, and has not evaluated the interplay effect between privacy concern and trust on perceived privacy. 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.

ACKNOWLEDGMENT

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

REFERENCES

Altman, I. (1975). The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding.

Altman, I. (1976). Privacy: A Conceptual Analysis. Environment and behavior, 8 (1), 7-29.

Bandura, A. (2001). Social Cognitive Theory: An Agentic Perspective. Annual review of psychology, 52 (1), 1-26.

Bansal, G., and 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.

Bansal, G., Zahedi, F., and Gefen, D. (2008). The Moderating Influence of Privacy Concern on the Efficacy of Privacy Assurance Mechanisms for Building Trust: A Multiple-Context Investigation. ICIS 2008 Proceedings, 7.

Bennett, C. J. (1992). Regulating Privacy: Data Protection and Public Policy in Europe and the United States, Cornell University Press.

Brandimarte, L., Acquisti, A., and Loewenstein, G. (2013). Misplaced Confidences Privacy and the Control Paradox. Social Psychological and Personality Science, 4 (3), 340-347.

Campbell, D. T., and Fiske, D. W. (1959). Convergent and Discriminant Validation by the Multitrait-Multimethod Matrix. Psychological Bulletin, 56 (2), 81-105.

Chellappa, R. K., and Pavlou, P. A. (2002). Perceived Information Security, Financial Liability and Consumer Trust in Electronic Commerce Transactions. Logistics Information Management, 15 (5/6), 358-368.

Chin, W. W. (1998). The Partial Least Squares Approach to Structural Equation Modeling. In Modern Methods for Business Research, G. A. Marcoulides (ed.), Lawrence Erlbaum Associates: Hillsdale, NJ, 295-336.

Culnan, M. J. (1993). " How Did They Get My Name?": An Exploratory Investigation of Consumer Attitudes toward Secondary Information Use. Mis Quarterly, 341-363.

Culnan, M. J., and Armstrong, P. K. (1999). Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. Organization science, 10 (1), 104-115.

Culnan, M. J., and Bies, R. J. (2003). Consumer Privacy: Balancing Economic and Justice Considerations. Journal of social issues, 59 (2), 323-342.

Culnan, M. J., and Milberg, S. J. (1998). The Second Exchange: Managing Customer Information in Marketing Relationships. Unpublished manuscript, Georgetown University, Washington, DC.

Culnan, M. J., and Williams, C. C. (2009). How Ethics Can Enhance Organizational Privacy: Lessons from the Choicepoint and Tjx Data Breaches. Mis Quarterly, 673-687.

Dinev, T., and Hart, P. (2004). Internet Privacy Concerns and Their Antecedents-Measurement Validity and a Regression Model. Behaviour & Information Technology, 23 (6), 413-422.

Dinev, T., and Hart, P. (2006a). An Extended Privacy Calculus Model for E-Commerce Transactions. Information Systems Research, 17 (1), 61-80.

Dinev, T., and 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., and 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.

Earp, J. B., and Baumer, D. (2003). Innovative Web Use to Learn About Consumer Behavior and Online Privacy. Communications of the ACM, 46 (4), 81-83.

Faja, S., and 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), 27.

Falk, R. F., and Miller, N. B. (1992). A Primer for Soft Modeling, University of Akron Press, OH.

Flavián, C., Guinalíu, M., and Gurrea, R. (2006). The Role Played by Perceived Usability, Satisfaction and Consumer Trust on Website Loyalty. Information & Management, 43 (1), 1-14.

Fornell, C., and Larcker, D. F. (1981). Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. Journal of Marketing Research, 18 (1), 39–50.

Gefen, D., Straub, D., and Boudreau, M.-C. (2000). Structural Equation Modeling and Regression: Guidelines for Research Practice. Communications of the association for information systems, 4 (Article 7).

Hair, J. F., Sarstedt, M., Ringle, C. M., and 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., and Anderson, R. E. (2009). Multivariate Data Analysis, Pearson Prentice Hall, Upper Saddle River, New Jersey.

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., and DeSarbo, W. S. (1991). On the Measurement of Perceived Consumer Risk. Decision Sciences, 22 (4), 927-939.

Hui, K.-L., Teo, H. H., and Lee, S.-Y. T. (2007). The Value of Privacy Assurance: An Exploratory Field Experiment. Mis Quarterly, 19-33.

Jarvenpaa, S. L., Tractinsky , N., and Vitale, M. (2000). Consumer Trust in an Internet Store. Information Technology and Management, 1 (1-2), 45-71.

Joinson, A. N., Reips, U.-D., Buchanan, T., and Schofield, C. B. P. (2010). Privacy, Trust, and Self-Disclosure Online. Human–Computer Interaction, 25 (1), 1-24.

Kim, D. J., Ferrin, D. L., and Rao, H. R. (2008). A Trust-Based Consumer Decision-Making Model in Electronic Commerce: The Role of Trust, Perceived Risk, and Their Antecedents. Decision support systems, 44 (2), 544-564.

Klein, C. T., and Helweg-Larsen, M. (2002). Perceived Control and the Optimistic Bias: A Meta-Analytic Review. Psychology and Health, 17 (4), 437-446.

Liu, C., Marchewka, J. T., Lu, J., and Yu, C.-S. (2005). Beyond Concern—a Privacy-Trust-Behavioral Intention Model of Electronic Commerce. Information & Management, 42 (2), 289-304.

Malhotra, N. K., Kim, S. S., and Agarwal, J. (2004). Internet Users' Information Privacy Concerns (Iuipc): The Construct, the Scale, and a Causal Model. Information Systems Research, 15 (4), 336-355.

Milne, G. R., and Culnan, M. J. (2002). Using the Content of Online Privacy Notices to Inform Public Policy: A Longitudinal Analysis of the 1998-2001 Us Web Surveys. The Information Society, 18 (5), 345-359.

Milne, G. R., and 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.

Nunnally, J. C. (1978). Psychometric Theory, McGraw-Hill, New York, NY.

Pavlou, P. A., Liang, H. G., and Xue, Y. J. (2007). Understanding and Mitigating Uncertainty in Online Exchange Relationships: A Principal–Agent Perspective. MIS Quarterly, 31 (1), 105-136.

Petronio, S. (2012). Boundaries of Privacy: Dialectics of Disclosure, Suny Press.

Ringle, C. M., Wende, S., and Becker, J.-M. 2014. "Smartpls 3," SmartPLS: Hamburg.

Smith, H. J. (1993). Privacy Policies and Practices: Inside the Organizational Maze. Communications of the ACM, 36 (12), 104-122.

Smith, H. J., Dinev, T., and Xu, H. (2011). Information Privacy Research: An Interdisciplinary Review. MIS quarterly, 35 (4), 989-1016.

Smith, H. J., Milberg, S. J., and Burke, S. J. (1996). Information Privacy: Measuring Individuals' Concerns About Organizational Practices. MIS quarterly, 167-196.

Van Slyke, C., Shim, J., Johnson, R., and Jiang, J. J. (2006). Concern for Information Privacy and Online Consumer Purchasing. Journal of the Association for Information Systems, 7 (1), 16.

Vaske, J. J., and Donnelly, M. P. (1999). A Value-Attitude-Behavior Model Predicting Wildland Preservation Voting Intentions. Society & Natural Resources, 12 (6), 523-537.

Westin, A. F. (1967). Privacy and Freedom.

Wu, K.-W., Huang, S. Y., Yen, D. C., and 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., Dinev, T., Smith, J., and Hart, P. (2011). Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances. Journal of the Association for Information Systems, 12 (12), 798-824.

Yamaguchi, S. (2001). Culture and Control Orientations. The handbook of culture and psychology, 223-243.