8-2020

Measuring privacy concerns with government surveillance and right-to-be-forgotten in nomological net of trust and willingness-to-share

Gaurav BANSAL

Fiona Fui-hoon NAH
Singapore Management University, fionanah@smu.edu.sg

Measuring Privacy Concerns with Government Surveillance and Right-to-be-Forgotten in Nomological Net of Trust and Willingness-to-Share

Completed Research Full Paper

Gaurav Bansal
University of Wisconsin – Green Bay
bansalg@uwgb.edu

Fiona Fui-Hoon Nah
Missouri Univ. of Science and Tech.
nahf@mst.edu

Abstract

In the post Snowden revelations era, concerns related to government surveillance and oversight have come to the forefront. The ability of the Internet to remember "everything" (or forget anything) also raises a privacy concern associated with the "right to be forgotten". Hence, in this paper, we propose and examine privacy concerns by extending the Hong and Thong's (2013) model with the addition of two dimensions: right to be forgotten as well as government surveillance and oversight. We tested two different measurement models using privacy concerns as a second-order and a third-order construct within a nomological net that includes trusting beliefs and willingness-to-share information for monetary gains, personalization, and national security. Data were collected from MTurk and analyzed using structural equation modeling. Findings provide support for the addition of the proposed dimensions.

Keywords

Privacy concern, right to be forgotten, government surveillance and oversight, willingness-to-share information.

Introduction

Privacy is a complex and variegated concept, interpreted differently by people as well as across cultures (Grossklags and Acquisti 2007). Citing Smith et al. (1996) and Culnan (1993), Stewart and Segars (2002) stated that the concept of privacy "evolves as computer-based information collection, storage, and retrieval become more pervasive" (p.46). The anxiety to be in control of one's information has increased in the age of social media, data breaches, Snowden revelations, among others (Rainie 2018). People want to be in control of their information (Stewart and Segars 2002). Although people are worried about the privacy of their information, they continue to trust technology giants, such as Facebook and Amazon, with even more sensitive and personal data despite repeated failures by these firms to protect their data (Molla 2019). People often share their information in the desire to enhance their perceived self-worth (Wilcox and Stephen 2013) and yet, are concerned about the privacy of their information and the degree of control they exercise over how their information is used or handled. Even though people are aware that the economy runs on information and hence, may have less resistance to sharing information, they are also more concerned about other aspects of information privacy that were less salient in the pre-Snowden era, such as government surveillance and oversight (Gao 2015). Specifically, a recent survey by Pew Research Center indicates that the Americans' perspective of privacy concerns (PC) has changed and 70% of them believe that the government is using surveillance data for purposes beyond anti-terror efforts (Geiger 2018). Another survey by the Pew Research Center has also indicated that the majority of Americans disapprove of the collection of citizens' data by the US government and that many of them have changed

their behavior because of the government surveillance program (Rainie and Madden 2015). Thus, the nature of PC has undergone a silent change to warrant a closer examination of the PC concept.

Although past research has conceptualized concerns for information privacy, none has examined it from the perspective of oversight or the possibility of constant government surveillance (Gao 2015). Smith et al. (1996) have conceptualized concerns for information privacy as comprising four dimensions: collection, secondary use, unauthorized access, and error. There have been several incremental modifications to the construct over the years. Stewart and Segars (2002) proposed conceptualizing concerns for information privacy as a second-order construct with control as the binding force that ties first-order factors – collection, secondary use, unauthorized access, and errors. Hong and Thong (2013) conceptualized PC as a third-order factor that comprises two second-order factors and one first-order factor, awareness. The two second-order factors are information management that comprises two first-order dimensions, i.e., unauthorized access and error, and interaction management that comprises three first-order dimensions, i.e., collection, secondary use, and control. In the post Snowden revelations era, concerns related to government surveillance and oversight have come to the forefront. Due to the typically low trust that Americans place on their government, government surveillance and oversight concerns are a significant factor impacting PC. Also, with the ability (or inability) of the Internet to remember "everything" (or forget anything), the "right to be forgotten" is also a concern to privacy (Steinbart et al. 2017). Hence, in this paper, we propose and examine PC by extending the PC model by Hong and Thong (2013) with two additional dimensions: right to be forgotten as well as government surveillance and oversight. We tested two different measurement models: in model 1 (see Figure 2), we factor all eight dimensions (collection, secondary use, unauthorized access, errors, control, awareness, right to be forgotten, and government surveillance and oversight) as first-order factors, and in model 2 (see Figure 3), we model PC as a third-order construct in a similar way as Hong and Thong (2013) by factoring right to be forgotten as part of interaction management (Steinbart et al. 2017) and government surveillance and oversight as part of information management. We examine the new PC construct within a nomological net that includes trusting beliefs and assess these two PC measurement models (i.e., a second-order model and a third-order model) with trusting beliefs and willingness-to-share information for (i) monetary gains, (ii) personalization, and (iii) national security.

The paper proceeds as follows: first, we introduce the theoretical development and hypotheses. In the next section, we describe the field study and the data collected. Next, we present the data analysis and results. We then discuss the study's contributions and implications, and conclude the paper.

Theoretical Development and Hypotheses

Table 1 presents a summary of key empirical studies that have modeled PC. Drawing on the work by Hong and Thong (2013), we also adopt the multidimensional developmental theory (MDT) to conceptualize perceptions of PC (Laufer and Wolfe 1977). MDT views PC as a multidimensional construct that comprises self-development, environmental impact, and interpersonal interaction, as well as the ability to perceive choices (i.e., awareness). Self-development and environmental impact are associated with information management. Applying MDT, PC is conceptualized as a third-order construct comprising two second-order constructs – information management and interaction management – and a separate first-order construct, awareness (see Figure 3). Hong and Thong (2013) defined information management as a component of PC related to "how an individual manages his or her personal information", and interaction management as another component associated with the "ability of an individual to manage the collection and subsequent use of his or her personal information by websites" (p.277) or other parties. Table 2 provides the definitions for the eight PC dimensions.

Perceptions of risks are known to decrease trust (Bansal et al. 2010; Dinev and Hart 2006). PC shapes how much we trust an entity collecting or using our data (Bansal et al. 2010). In the post Snowden revelations era where there are heightened concerns about information privacy associated with government surveillance programs (Geiger 2018; Rainie 2016), people are more wary of trusting the government, online businesses, and the Internet in general. Hence, we propose the following hypothesis.

Hypothesis 1: Privacy concern is negatively associated with trust in (a) government, (b) online businesses, and (c) Internet.

Source	COL	SEC	UNA	ERR	AWA	CON	RTF	GSO	Key Findings
Hoehle et al. (2019)	X	X	X	X					Group unauthorized access and errors as information management, and collection and secondary use as interaction management
Hong and Thong (2013)	X	X	X	X	X	X			Divide PC dimensions into two groups – interaction management and information management
Smith et al. (1996)	X	X	X	X					Provide four dimensions of PC
Steinbart et al. (2017)	X	X	X	X	X	X	X		Introduce the right to be forgotten and associate it with concerns about the final stage of the information life cycle, i.e. disposal
Stewart and Segars (2002)	X	X	X	X					Privacy as a second-order construct, with *control* as a binding force
Current study	X	X	X	X	X	X	X	X	Propose government surveillance and oversight as a dimension of PC

Note: COL – collection, SEC – secondary use, UNA – unauthorized access, ERR – error, AWA – awareness, CON – control, RTF – right to be forgotten, GSO – government surveillance and oversight

Table 1. Summary of Literature Background

Collection	Degree to which an individual is worried about the amount of his/her personal information that is collected
Unauthorized access	Degree to which an individual is concerned about his/her personal information being made readily available to unauthorized parties
Secondary use	Degree to which an individual is concerned about the unjustified use of his/her information for purposes other than those for which they were initially gathered
Errors	Degree to which an individual is concerned about the deliberate or unintentional errors that might be made to his/her personal information
Right to be forgotten	Degree to which an individual is concerned that his/her past information in the post-use context would never be erased (Steinbart et al. 2017)
Control	Degree to which an individual has control over how his/her information is used
Awareness	Degree to which an individual is adequately aware that his/her information is being collected
Govt. surveillance and oversight	Degree to which an individual is concerned about constant surveillance by government

Table 2. Privacy Concern Dimensions

The privacy calculus theory suggests that PC is moderated by the benefits of sharing information (Dinev and Hart 2006; Sheng et al. 2008). As the benefits of sharing information increase, PC decreases, leading to an increase in trust. Even though online privacy assurance is associated with positive consumer valuations which increase users' willingness to share information, benefits such as financial gains and convenience (e.g., through personalization) further increase their willingness to share information (Grossklags and Acquisti 2007). Ozturk et al. (2017) found that while personalization may raise PC, it reduces users' perceived risk and increases trust. Similarly, Swire (2006) noted that people share information for national security reasons. The majority of Americans are concerned that anti-terrorism policies have not gone far enough to adequately protect them (Gao 2015). 49% of Americans indicated that it is acceptable for the government to collect data about all Americans to assess potential terrorist threats as compared to 31% who indicated that it is unacceptable to collect data from all Americans for the same purpose (Auxier et al. 2019). Thus, concerns about national security further enhance or moderate the positive relationship between trust and willingness to share information. Thus, we propose the following hypotheses:

Hypothesis 2: Willingness to share information for national security reasons is positively associated with trust in (a) government, (b) online businesses, and (c) the Internet.

Hypothesis 3: Willingness to share information for personalization reasons is positively associated with trust in (a) government, (b) online businesses, and (c) the Internet.

Hypothesis 4: Willingness to share information for monetary benefit reasons is positively associated with trust in (a) government, (b) online businesses, and (c) the Internet.

Figure 1 shows the research model based on the hypotheses.

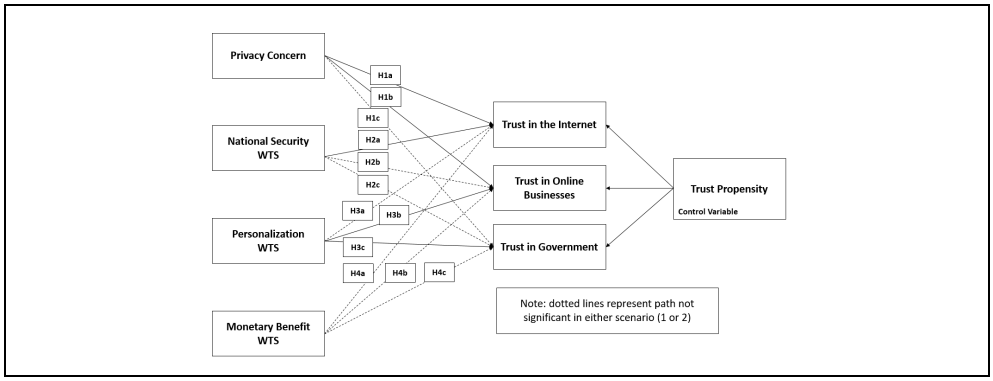

Figure 1. Nomological Model

Research Methodology

Data was collected using the Qualtrics survey from Amazon MTurk. 312 people completed the survey and 275 of them passed the attention check questions. The final sample had an average age of 34 years (standard deviation of 10 years). The age of the participants ranged from 18 to 69 years. There were 155 males and 119 females; one person chose 'other' for gender. 95% of the sample had college or higher education. 77% are employed full-time, 10% are employed part-time, and 10% are self-employed.

Measurement

We used preexisting scales where available and developed items for constructs that are not available in the literature, as shown in Table 3. The self-developed items are provided in Table 4.

Construct	Adapted From
Willingness to Share (WTS) for national security	Self-developed
Willingness to Share (WTS) for personalization	Self-developed
Willingness to Share (WTS) for monetary benefits	Self-developed
Concern with collection	Bansal et al. (2015)
Concern with secondary use	Bansal et al. (2015)
Concern with unauthorized access	Bansal et al. (2015)
Concern with errors	Bansal et al. (2015)
Awareness	Steinbart et al. (2017)
Right to be forgotten	Steinbart et al. (2017)
Control	Steinbart et al. (2017)
Government surveillance and oversight	Self-developed
Trust in the Internet	Bélanger and Carter (2008)
Trust in online businesses	Bélanger and Carter (2008); Teo et al. (2008)
Trust in government	Bélanger and Carter (2008); Teo et al. (2008)

Table 3. Measurement Instrument

Government surveillance and oversight	
OVER1	I am concerned that any information that I submit online could be used along with my other information to build an extensive profile on me.
OVER2	I am concerned that information that I submit online could be used to track my activities.
Willingness to share (WTS) for national security	
NSEC1	I do not mind online companies sharing my personal information in the interest of national security.
NSEC2	I do not mind having my personal information used in the interest of national security.
NSEC3	As long as my personal information is used for national security, I do not mind if it is shared.
Willingness to share (WTS) for personalization	
PERS1	I do not mind when companies use personal information that I provide online to personalize my experience.
PERS2	I do not mind sharing my personal information online in order to receive personalized advertisements and product recommendations.
Willingness to share (WTS) for monetary benefits	
MONB1	I always share my information when companies offer me a monetary reward for my personal information.
MONB2	I do not mind sharing my personal information online in order to receive a small monetary reward.
MONB3	I am willing to share my personal information with well-reputed companies for some monetary rewards.
Note: A scale of 1 (strongly disagree) to 7 (strongly agree) was used	

Table 4. Self-developed Items

Data Analysis

Data was analyzed using Mplus (Muthén and Muthén 1998-2012). We analyzed two measurement models. Model 1 conceptualized PC as a second-order construct with all eight dimensions (collection, secondary use, unauthorized access, error, control, right to be forgotten, awareness, and government surveillance and oversight) as first-order (as shown in Figure 2). Model 2 conceptualized PC as a third-order construct, which is in line with Hong and Thong (2013), using two second-order factors – interaction management (collection, secondary use, control, and right to be forgotten) and information management (unauthorized access, error, and oversight) – along with awareness as a first-order factor (see Figure 3). Steinbart (2017) argued that the right to be forgotten is a separate dimension of PC, and could be related to both information management and interaction management aspects of PC. Considering that the right to be forgotten is a part of information end-of-life cycle (Steinbart 2017) that begins with collection, we deem it to be associated with interaction management. We associate government surveillance and oversight with information management, along with unauthorized access and error. In the context of this research, oversight is primarily concerned with government surveillance and is closely related to unauthorized access of data but in a different way from unauthorized access by insiders or hackers.

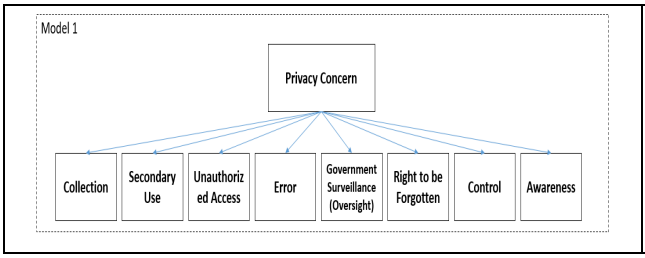

Figure 2. PC Model 1

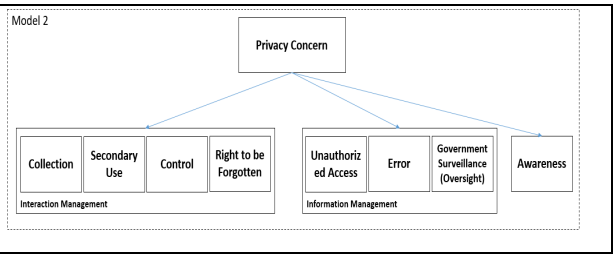

Figure 3. PC Model 2

We conducted reliability analysis as well as discriminant and convergent validity analysis. We also examined the measurement model. The constructs demonstrated adequate reliability with Cronbach's alpha coefficients that are greater than 0.7 for all of them. Construct correlations are less than the square root of AVE, demonstrating support for discriminant validity. AVE values are greater than .5, thus demonstrating support for convergent validity. We also found adequate support for discriminant and convergent validity through exploratory factor analysis. The loadings on the intended factors are all greater than .7, indicating good convergent validity, and the cross-loadings are less than .4, demonstrating good discriminant validity. Also, the fit indices for the confirmatory factor analysis model meet the generally accepted thresholds (see Table 4), further demonstrating adequate measurement fit. The fit indices for the estimation models also fall within recommended thresholds, indicating adequate model fit.

	Measurement Model		**Estimation Model**	
	Model 1	**Model 2**	**Model 1**	**Model 2**
Chi sq / df	1381.577/824	1355.515/822	1375.976/824	1355.730/822
CFI	.905	.909	.906	.909
TLI	.896	.900	.897	.900
RMSEA	.051	.050	.051	.050
SRMR	.062	.057	.055	.057

Table 4. Fit Indices

The results are summarized in Table 5. Across both models, we observed that PC lowers trust in government (p<.001), enhance trust in online businesses (p<.001), and has no significant impact on trust in the Internet. The control variable, trust propensity, significantly increases trust in the government (p<.001), trust in online businesses (p<.001), and trust in the Internet (p<.001). The structural model based on measurement model 2 explains 65% of the variation in trust in government (64% for model 1), 52% of the variation in online business (51% for model 1), and 63% of the variation in trust in Internet (62% for model 1). The results show that PC has a negative impact on trust in government, thus supporting H1a, but has a positive impact on trust in online businesses, which is a reverse relationship from H1b. PC has no impact on trust in Internet, thus H1c is not supported.

Hyp.	**Path**	**Model 1**		**Model 2**	
		Path Coeff.	**T-Stat**	**Path Coeff.**	**T-Stat**
H1a	PC to Trust in Government	-0.164***	-3.285	-0.163***	-3.390
H1b	PC to Trust in Online Businesses	0.147*	2.306	0.151**	2.425
H1c	PC to Trust in Internet	-0.068	-1.291	-0.069	-1.292
H2a	WTS for National Security to Trust in Government	0.314**	2.870	0.318**	2.897
H2b	WTS for National Security to Trust in Online Businesses	0.024	0.205	0.033	0.283
H2c	WTS for National Security to Trust in Internet	0.060	0.677	0.060	0.669
H3a	WTS for Personalization to Trust in Government	0.119	0.948	0.119	0.951
H3b	WTS for Personalization to Trust in Online Businesses	0.327**	2.359	0.321*	2.311
H3c	WTS for Personalization to Trust in Internet	0.364***	3.159	0.370***	3.213
H4a	WTS for Monetary Benefit to Trust in Government	-0.005	-0.047	-0.005	-0.046
H4b	WTS for Monetary Benefit to Trust in Online Businesses	0.162	1.318	0.169	1.366
H4c	WTS for Monetary Benefit to Trust in Internet	0.081	0.811	0.076	0.761
Control	Trust Propensity to Trust in Government	0.484***	5.983	0.480***	5.960
Control	Trust Propensity to Trust in Online Businesses	0.364***	3.988	0.363***	3.976
Control	Trust Propensity to Trust in Internet	0.434***	5.954	0.434***	5.966
Note: *** p<.001; ** p<.01; *p<.05; WTS: Willingness to Share					

Table 5. Summary of Results

Willingness to share information for national security is associated with trust in government, thus supporting H2a, but is not associated with trust in online businesses and trust in Internet, thus providing no support for H2b and H2c. Willingness to share information for personalization does not impact trust in government, but is positively associated with trust in online businesses and the Internet, thus supporting H3b and H3c but not H3a. Hypothesis H4 (all three parts) is not supported.

Discussions

Key Findings and Contributions

Prior research on privacy has established that people are concerned about collection of data, secondary use of data, unauthorized access to data, and erroneous data. They are also concerned about the degree to which they can control what organizations or governments can do with their information, oversight of their information by government surveillance, concerns about the ability to delete their information, and awareness about the security of their information. This study proposes and investigates government surveillance and oversight concerns as an information management factor of PC. The study also examines an alternate model that examines PC as a second-order factor comprising the eight dimensions (collection, secondary use, unauthorized access, errors, control, awareness, right to be forgotten, and government surveillance and oversight) as first-order factors. Additionally, the study examines if users' willingness to share their information (Grossklags and Acquisti 2007) could be extended to non-monetary benefits such as personalization and national security. We examine the role of PC and users' willingness to share information for national security, personalization, and monetary benefits on trust in three entities – government, online businesses, and the Internet.

The findings show that both models (1 and 2) provide similar results in terms of path coefficients (Table 5); however, model 2 is able to explain a slightly higher R square for all of the constructs except government surveillance and oversight, and the fit indices are also slightly better for model 2 (Table 4). The findings provide support for the hypothesized PC structures and suggest that willingness to share information for national security reasons and for personalization enhances people's trust in the government and in online businesses respectively. The results suggest that willingness to share information for monetary benefits did not lead to higher trust associations with any of the three entities – government, online businesses, and the Internet. Trust propensity was significantly associated with trust in the three entities.

Implications for Theory

The findings have several major theoretical implications. First, government surveillance and oversight will need to be included as an information management dimension of PC. Oversight is similar in nature to "unauthorized access", and hence, it is associated with information management. We provided empirical support for adding the oversight dimension to the PC scale, thus addressing the need and concern expressed in the literature (Campbell and Carlson 2002; Gao 2015). Findings also show support for adding right to be forgotten as an interaction management PC dimension. Second, the positive relationship between PC and trust in online businesses is an interesting finding. From hindsight, the finding is not surprising for businesses. Research has shown that even though web personalization by online businesses can increase users' concerns with privacy, it also helps to decrease risks to users through personalization, thus heightening users' trust (Ozturk et al. 2017). Hence, a positive correlation between PC and trust can arise. Similarly, an earlier study by (Bansal et al. 2010) have also reported that health information PC did not lower trust in health websites.

Third, our study assessed the relationship between willingness to share information (Grossklags and Acquisti 2007) and trust beliefs. As demonstrated in the study, willingness to share information for national security is associated with trust in government and willingness to share information for personalization is associated with trust in Internet and trust in online businesses. There is no relationship between willingness to share information for monetary benefits and trust in online businesses, Internet, or the government, suggesting that the trust factor may have been ignored because willingness to share information may have been predominately driven by monetary gains based on privacy calculus theory. Specifically, studies have shown that people are willing to share their information for as little as 25 cents (Grossklags and Acquisti 2007). However, in the context of e-commerce, people are willing to spend more

to purchase from trusted sources by paying a price premium (Bansal and Davenport 2010). In future research, it would be helpful to further investigate how monetary valuations are moderated by contextual factors.

Fourth, we observed that privacy concerns are not associated with trust in the Internet. It could be argued that the Internet is a joint venture between the public and private sectors (Goldsmith and Wu 2006). So, if people trust the private enterprise but not the public enterprise, there could be a tug-of-war between them that makes the impact of privacy concerns on trust in the Internet neutral or cancelled out.

Lastly, the definition of privacy is not about solitude, but about control. Privacy is the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others (Westin, 2015) and hence, users' right to control their information is key.

Implications for Practice

This study suggests that in the post Snowden revelations era, oversight concerns cannot be ignored and will need to be modeled as part of PC. This study has also demonstrated that the right to be forgotten is a key component of PC in the US today, even if it is not a legal requirement for businesses to comply with. The findings show that PC can not only lower trust in an entity (government), but it can also lead to higher trust in online businesses in general. It is probably this trust in online businesses that keeps e-commerce budding and social media flowering despite concerns about the data practices of several online companies. The paper provides guidance to business managers as they work with government entities on sharing data. Even though PC lowers trust in government, US citizens are more trusting of the government when it comes to national security. This observation is also supported by the Pew research survey (Maniam 2016) which shows that Americans in general value security concerns over civil liberties. The findings also provide support for personalization. According to a research survey, 58 percent of respondents indicated that they respond better to more personalized messages from brands (Businesswire.com 2018). In addition, organizations need to adequately address consumers' preferences and concerns about the right to be forgotten and government surveillance and oversight by incorporating their control preferences and limiting or seeking permissions to share their information.

Conclusion

As with any research, it is important to acknowledge the limitations of our study. This study was carried out in the Mechanical Turk crowdsourcing platform and hence, future research should test the model with a more diverse and representative sample of the US population as well as examine the model longitudinally. As noted earlier, PC is a "dynamic" construct that will need to be examined over time to capture the "essence" of the construct in order to reflect on its evolving multi-tiered structure – single factor, to second-order, to now third-order, and beyond. Privacy concerns may still evolve as home security cameras, appliances, health fitness indicators get connected through IoT to local businesses, medical providers and other local and federal government agencies. As users and citizens get more educated about how online businesses aid in government intrusion through unpublicized channels such as third-party doctrine (Bedi 2013), privacy concerns related to government surveillance and oversight will become even more salient. This study extends the interaction management and information management dimensions of PC as proposed by Hong and Thong (2013), and provides empirical support to incorporate the right to be forgotten and government surveillance and oversight concerns respectively. The study also provides competing models for PC and discusses the relative merits of them. We measured and assessed the fit of a more enhanced and comprehensive set of PC dimensions that includes oversight and the right to be forgotten, and verified that they fit well in the nomological network of PC.

Acknowledgement

The research was made possible in part due to Frederick E. Baer Professorship in Business at Austin E. Cofrin School of Business at the University of Wisconsin–Green Bay.

References

Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M., and Turner, E. 2019. "Americans and Privacy: Concerned, Confused and Feeling Lack of Control over Their Personal Information," from https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/ (last accessed Jan 28, 2020).

Bansal, G., and Davenport, R. 2010. "Moderating Role of Perceived Health Status on Privacy Concern Factors and Intentions to Transact with High Versus Low Trustworthy Health Websites," *Fifth Midwest Association for Information Systems Conference*, Moorhead, MN.

Bansal, G., Zahedi, F., and 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), pp. 624-644.

Bansal, G., Zahedi, F. M., 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), pp. 138-150.

Bedi, M. 2013. "Facebook and Interpersonal Privacy: Why the Third Party Doctrine Should Not Apply," *Boston College Law Review* (54), pp. 1-71.

Bélanger, F., and Carter, L. 2008. "Trust and Risk in E-Government Adoption," *Journal of Strategic Information Systems* (17:2), pp. 165-176.

Businesswire.com. 2018. "New Research from Vision Critical Reveals Two-Thirds of Consumers Would Comfortably Share Personal Information If Brands Were Open About Its Use," from https://www.businesswire.com/news/home/20180411005385/en/New-Research-Vision-Critical-Reveals-Two-Thirds-Consumers/ (last accessed Jan 28, 2020).

Campbell, J. E., and Carlson, M. 2002. "Panopticon.Com: Online Surveillance and the Commodification of Privacy," *Journal of Broadcasting & Electronic Media* (46:4), pp. 586-606.

Culnan, M. J. 1993. "How Did They Get My Name: An Exploratory Investigation of Customer Attitudes toward Secondary Information Use," *MIS Quarterly* (17:3), pp. 341-361.

Dinev, T., and Hart, P. 2006. "An Extended Privacy Calculus Model for E-Commerce Transaction," *Information Systems Research* (17:1), pp. 61-80.

Gao, G. 2015. "What Americans Think About Nsa Surveillance, National Security and Privacy," from https://www.pewresearch.org/fact-tank/2015/05/29/what-americans-think-about-nsa-surveillance-national-security-and-privacy/ (last accessed Jan 28 2020).

Geiger, A. W. 2018. "How Americans Have Viewed Government Surveillance and Privacy since Snowden Leaks," from https://www.pewresearch.org/fact-tank/2018/06/04/how-americans-have-viewed-government-surveillance-and-privacy-since-snowden-leaks/ (last accessed Feb 28, 2020).

Goldsmith, J., and Wu, T. 2006. *Who Controls the Internet?: Illusions of a Borderless World*. Oxford University Press, NY.

Grossklags, J., and Acquisti, A. 2007. "When 25 Cents Is Too Much: An Experiment on Willingness-to-Sell and Willingness-to-Protect Personal Information," *Sixth Workshop on the Economics of Information Security (WEIS 2007), Pittsburgh, PA*.

Hoehle, H., Aloysius, J. A., Goodarzi, S., and Venkatesh, V. 2019. "A Nomological Network of Customers' Privacy Perceptions: Linking Artifact Design to Shopping Efficiency," *European Journal of Information Systems* (28:1), pp. 91-113.

Hong, W., and Thong, J. Y. 2013. "Internet Privacy Concerns: An Integrated Conceptualization and Four Empirical Studies," *MIS Quarterly* (37:1), pp. 275-298.

Laufer, R. S., and Wolfe, M. 1977. "Privacy as a Concept and a Social Issue: A Multidimensional Development Theory," *Journal of Social Issues* (33:3), pp. 22-42.

Maniam, S. 2016. "Americans Feel the Tensions between Privacy and Security Concerns," from https://www.pewresearch.org/fact-tank/2016/02/19/americans-feel-the-tensions-between-privacy-and-security-concerns/ (last accessed Jan 28, 2020).

Molla, R. 2019. "People Say They Care About Privacy but They Continue to Buy Devices That Can Spy on Them," from https://www.vox.com/recode/2019/5/13/18547235/trust-smart-devices-privacy-security (last accessed Feb 9, 2020).

Muthén, L. K., and Muthén, B. O. 1998-2012. *Mplus User's Guide (Seventh Edition)*. Los Angeles, CA: Muthén & Muthén.

Ozturk, A. B., Nusair, K., Okumus, F., and Singh, D. 2017. "Understanding Mobile Hotel Booking Loyalty: An Integration of Privacy Calculus Theory and Trust-Risk Framework," *Information Systems Frontiers* (19:4), pp. 753-767.

Rainie, L. 2016. "The State of Privacy in Post-Snowden America," from http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/ (last accessed July 3, 2019).

Rainie, L. 2018. "Americans' Complicated Feelings About Social Media in an Era of Privacy Concerns," from https://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns (last accessed Mar 12, 2020).

Rainie, L., and Madden, M. 2015. "How People Are Changing Their Own Behavior," from https://www.pewresearch.org/internet/2015/03/16/how-people-are-changing-their-own-behavior/ (last accessed April 22, 2020).

Sheng, H., Nah, F. F.-H., and Siau, K. 2008. "An Experimental Study on Ubiquitous Commerce Adoption: Impact of Personalization and Privacy Concerns," *Journal of the Association for Information Systems* (9:6), pp. 344-376.

Smith, H. J., Milberg, S. J., and Burke, S. J. 1996. "Information Privacy: Measuring Individuals' Concerns About Organizational Practices," *MIS Quarterly* (20:2), pp. 167-196.

Steinbart, P., Keith, M., and Babb, J. 2017. "Measuring Privacy Concern and the Right to Be Forgotten," *Proceedings of the 50th Hawaii International Conference on System Sciences*.

Stewart, K. A., and Segars, A. H. 2002. "An Empirical Examination of the Concern for Information Privacy Instrument," *Information Systems Research* (13:1), pp. 36-49.

Swire, P. P. 2006. "Privacy and Information Sharing in the War on Terrorism," *Vill. L. Rev.* (51:4), pp. 951-980.

Teo, T. S., Srivastava, S. C., and Jiang, L. 2008. "Trust and Electronic Government Success: An Empirical Study," *Journal of Management Information Systems* (25:3), pp. 99-132.

Wilcox, K., and Stephen, A. T. 2013. "Are Close Friends the Enemy? Online Social Networks, Self-Esteem, and Self-Control," *Journal of Consumer Research* (40:1), pp. 90-103.