PRIVACY CONCERN AND LIKELIHOOD OF PAYING A PRIVACY-FEE

Lori Baker-Eveleth, College of Business and Economics, University of Idaho, Moscow ID 83843, 208- 885-5940, leveleth@uidaho.edu
Daniel M. Eveleth, College of Business and Economics, University of Idaho, Moscow ID 83843, 208-885-4396, eveleth@uidaho.edu
Norman Pendegraft, College of Business and Economics, University of Idaho, Moscow ID 83843, 208- 885-7157, norman@uidaho.edu
Mark Rounds, College of Business and Economics, University of Idaho, Moscow ID 83843, 208-885- 4199, mrounds@uidaho.edu

ABSTRACT

This research examined the extent to which social-media users' privacy concerns affected the likelihood that they would pay a fee in exchange for a social-media company promising not to use or sell that user's data. Data to empirically test the theoretical model were collected by administering a survey to social-media users. The sample consisted of 173 usable responses. The results of the analyses, including the structural model show that users' knowledge of privacy issues, personal experience with invasions of privacy, and their levels of risk intolerance influenced the likelihood that they would pay a privacy fee, indirectly, through their concern for privacy. Furthermore, concern for privacy had a significant, positive effect on the magnitude of an expected privacy fee.

Keywords: Social media, SNS, privacy concern, rick tolerance, privacy fee

INTRODUCTION

A recent Pew Research report stated that the number of Americans who use some form of social media has risen from 5% in 2005 to nearly 70% in 2018, and over that time users have become increasingly "anxious about all the personal information that is collected and shared and the security of their data" [39]. In addition to calls for legislation requiring companies to provide opt-out options, disclose how they are protecting and using personal information, and notify users of data breaches, some have pushed for the use of financial incentives; either compensating users for their personal information or giving users the option to pay a fee in exchange for not using or selling their information [36]. However, in a recent interview Sheryl Sandberg, Chief Operating Officer of Facebook, noted that while giving users an option to opt out of data sharing by paying a fee is an alternative, the user base was thus far unwilling to pay for this option [21].

What makes this high-anxiety/low-willingness finding an interesting puzzle is that it is clear that users do assign value to the act of disclosing their private information and to a promise by organizations to protect the individual's private information [1]. Unfortunately, there is still little understanding about factors that affect these values or that affect users' willingness to pay for such value. Users' levels of concern for privacy, experience with privacy invasions, tolerance for risk, and familiarity with privacy issues may be some of those factors. In this manuscript we identify a set of hypothesized relationships between social-media users' willingness to pay an opt-out fee and factors that are likely to affect their willingness, and then describe a study that tested those hypotheses and the study results.

LITERATURE REVIEW

Individuals' concern for privacy has been widely documented across a wide array of settings as a meaningful construct of interest, including with respect to telemarketing and the use do-not-call-lists [9], e-commerce sites [29], bricks-and-mortar retailers using RFID tags [34], location identification [23], facial recognition technology to track shoppers [42], and activity on social media sites [35]. Across all of these settings, it is clear that organizations need a better understanding of the factors that affect users' concerns because their concerns likely affect their behaviors with respect to the organizations [15].

Smith, Dinev, and Xu [45] concluded, from an extensive review of privacy literature, that what is needed are empirical studies that "focus on antecedents to privacy concerns and on actual outcome" (p. 989). Laufer and Wolfe [27] postulated that individuals' concepts of privacy are affected by their experiences; and they described those experiences in terms of three dimensions: self-ego, environmental, and interpersonal. Hong, Chan and Thong [15] recently applied Laufer and Wolfe's [27] model to concerns for privacy in the online setting and concluded that three 'self-ego' or individual factors that have some effect on users' concerns for privacy are users' risk intolerance, experience with privacy invasion, knowledge or familiarity with privacy issues.

Further, a number of studies have confirmed that privacy concern does affect privacy-related intentions and behavior (e.g., [20] [25] [28]), and that the effect many antecedents to privacy concern have on intentions or behavior is fully mediated by concern for privacy [35]. It is for this reason that we propose the following hypotheses and the model displayed in Figure 1:

H1: A social-media user's knowledge of privacy issues positively influences their concern for privacy.

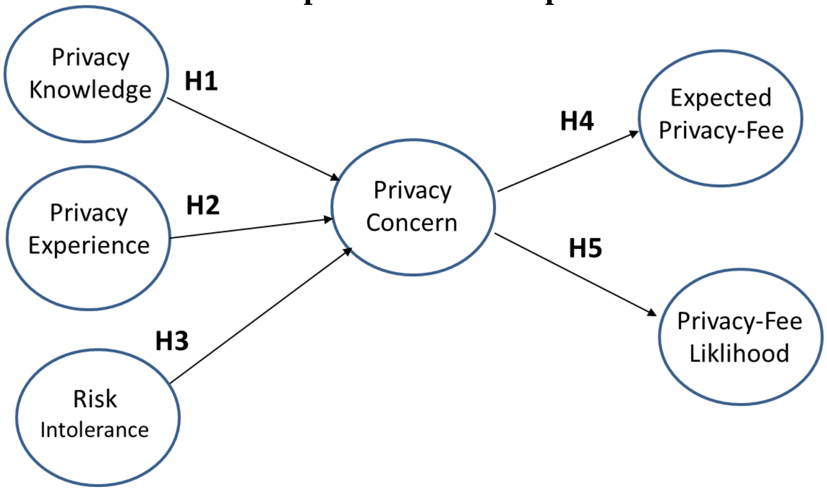
H2: A social-media user's experience with invasions of privacy positively influences their concern for privacy.

H3: A social-media user's risk intolerance positively influences their concern for privacy.

H4: A social-media user's concern for privacy positively influences the price that they believe someone would be expected to pay in exchange for a social-media company promising not to use or sell that subject's data.

H5: A social-media user's concern for privacy positively influences the likelihood that they would pay a fee in exchange for a social-media company promising not to use or sell that subject's data.

FIGURE 1
Proposed Relationships



METHOD

Participants

One hundred and seventy-three individuals participated in this study. Participants were students enrolled in one of four courses at a medium-sized university in western United States. Each course planned to have some discussion about social media privacy issues after students completed the survey, so in addition to earning extra credit for participation, the survey benefited students because the activity played a pedagogical role to stimulate awareness about the topic of privacy in social media. The average age of the participants was 21 years; 60% were female. Participants included freshmen (21.4%), sophomores (4.6%), juniors (25.4%), seniors (38.2%) and fifth-year seniors (10.4%). During a class session each instructor announced the opportunity to complete the online survey and then published a link to the survey on the class-management website.

Measures

The measures of the model's constructs were produced by collecting responses to questionnaire items that were adapted from previous research. Items for privacy knowledge, privacy experience, risk intolerance, and privacy concern were anchored by: (1) Disagree and (5) Agree. The measure for privacy knowledge was adapted from items reported by Singh and Hill [43]. The two items were: 1. I am knowledgeable about social media related privacy issues; and 2. I am familiar with current issues related to Internet privacy. The measure for privacy experience was adapted from items reported by Malhotra, Kim, and Agarwal [30]. The two items were: 1. I have personally experienced incidents whereby personal information I provided to a site was used without my authorization; and 2. I have personally been the victim of what I felt was an improper invasion of privacy on a website or social-media site. The measure for risk intolerance was adapted from items reported by Hong, Chan, and Thong [15]. The three items were: 1. Normally, I would rather be safe than sorry; 2. I am usually cautious in trying new or different things; and 3. I typically avoid risky things. The measure for privacy concern was adapted from items reported by Bright, Kleiser, and Grau [7] and Hong and Thong [16], and included eight items (e.g., I am concerned about my privacy on social-media sites; I am concerned that the personal information I give to sites is not protected from unauthorized access; I am concerned that sites are collecting too much personal information about me).

The measures for expected privacy-fee and likelihood of paying the fee were adapted from studies that have asked subjects about their willingness to pay a fee (e.g., [4] [6]). Each participant was asked to assume that the company that hosts the social-media site that the participant uses most frequently gives each user the option to pay a one-time fee in exchange for the company promising not to use or sell that user's data. Participants were then asked to select the price that a user would be expected to pay for such a service. In a previous study of U.S. consumers, Png [37] estimated that the value that households placed on protecting information was $3.22 at the lower bound with a best estimate of $8.25. Participants in this study were given the option of choosing any price between $1.00 and $100.00. Participants were then asked to report how likely they would be to pay the one-time fee. The item was anchored by: (1) Unlikely and (5) Likely.

RESULTS

Descriptive Statistics

Table 1 includes the descriptive statistics and correlations for each variable. The correlations between variables represented by the hypothesized relationships were positive and significant, offering preliminary support for our expectations.

TABLE 1
Correlations and Descriptive Statistics for all Variables

	Variables	Mean	s.d.	1	2	3	4	5	6	7
1	Age	21.05	3.63							
2	Gender	.60	.49	.03						
3	Privacy Knowledge	3.69	1.08	-.14	.01					
4	Privacy Experience	2.38	1.51	.20**	.09	.09				
5	Risk Intolerance	3.90	.90	.10	-.18*	.46**	.10			
6	Privacy Concern	3.86	.95	.08	-.08	.31**	.34**	.31**		
7	Expected Fee	20.71	24.29	.15*	.05	-.11	.10	.07	.17*	
8	Fee Likelihood	2.90	1.36	.10	.05	.10	.22**	.01	.23**	.07

Note: ***p<.001; **p<.01; *p<.05; gender is a dummy-coded variable that represents the percentage of females in the sample (0 = male, 1 =female).

The Measurement Model

The psychometric properties of each measure were evaluated with a confirmatory factor analysis using a structural equation modeling approach and maximum likelihood estimation in AMOS in SPSS version 22. All measures were reflective in their indicants and allowed to pairwise correlate. The goodness of fit index (GFI) and the adjusted goodness of fit index (AGFI) were 0.90 and 0.86, respectively. The root mean square error of approximation (RMSEA) was 0.06 with a 90% confidence interval of 0.04 to 0.08. The chi-square statistic was 156.49 with 98 degrees of freedom, which was statistically significant at a 1% level. Bentler’s [3]comparative fit (CFI) was 0.97 and the relative fit indices [i.e., Bentler & Bonett Normed Index (NFI), Bollen’s [5] Incremental Fit Index (IFI), & Tucker-Lewis Non-Normed Index (TLI)] were 0.92, 0.97, and 0.96, respectively. Taken together, as displayed in Table 2, these values indicate an acceptable fit between the model and the data [13] [17] [38].

TABLE 2
Fit Indices for the Measurement

	GFI	AGFI	X^2/df	CFI	RMSEA	NFI	TLI	IFI
Results	.90	.86	1.6	.97	.06	.92	.96	.97
Criteria	>.95	>.8	<2.0	<.95	<.07	>.9	>.9	>.9
Criteria Sources	[31]	[17]	[48]	[19]	[47]	[8]	[19]	[5]

The measures of the theoretical constructs in the model are shown in Table 3. The standardized path coefficients in the table were estimates from the confirmatory factor analysis. The items' standardized path coefficients ranged from 0.65 to 0.90, demonstrating satisfactory item reliability [38]. Similarly, the composite reliability estimates ranged from .74 to .99, and the Cronbach's Alpha estimates ranged from .78 to .94, thereby showing preferred levels since all exceeded the generally accepted cutoff level of 0.70 [33] [38]. Additionally, all the shared variance extracted percentages were above 50%. The combination of these results indicates that the measures satisfy convergent validity [11] [38].

TABLE 3
Construct Reliability and Convergent Validity

Construct	Item	Item reliability	Cronbach's alpha	Composite reliability	Average variance extracted
Privacy Knowledge	PK1	.89	.85	.81	.74
	PK2	.83			
Personal Experience	PE1	.86	.88	.74	.78
	PE2	.91			
Risk Intolerance	RI1	.65	.78	.88	.74
	RI2	.78			
	RI3	.80			
Privacy Concern	PC1	.70	.94	.99	.65
	PC2	.69			
	PC3	.87			
	PC4	.74			
	PC5	.90			
	PC6	.89			
	PC7	.77			
	PC8	.87			
	PC9	.80			

Discriminant validity was examined by evaluating the correlations between each measure of interest.

Acceptable discriminant validity is present when the square root of the average variance extracted (AVE) of each construct is greater than the correlations between it and other constructs [11]. As can be seen in Table 4, there is adequate discriminant validity; and since convergent and discriminant validity are satisfied for all the measures, it can be concluded that construct validity is also satisfied [13].

TABLE 4
Correlations Between Constructs with Reflective Measures

Variables	PK	PE	RI	PC
Privacy Knowledge	(.86)			
Privacy Experience	.10	(.75)		
Risk Intolerance	.55	.11	(.81)	
Privacy Concern	.34	.36	.34	(.88)

Note: Square roots of the average variance extracted are in parentheses.

The Estimation of the Model

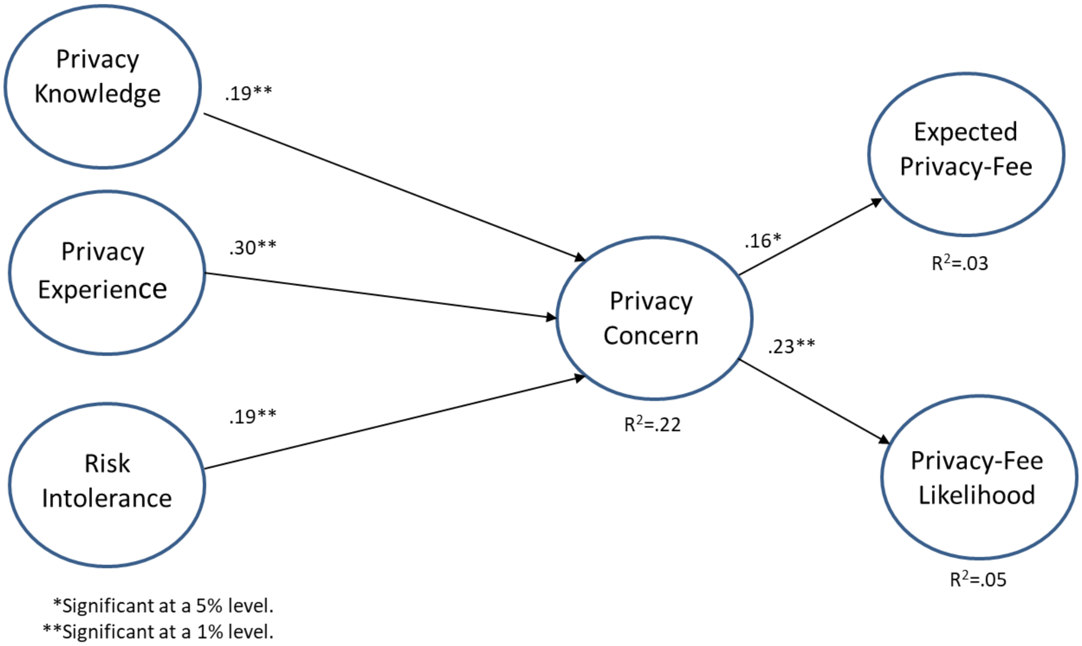
The model displayed in Figure 1 was estimated using a structural equations approach with AMOS in SPSS version 22 and maximum likelihood estimation. The summary statistics for the fit of the model to the data are displayed in Table 5. The goodness of fit index (GFI) was 0.98 and the adjusted goodness of fit index (AGFI) was 0.93. The normed chi-square statistic (X^2/df) was 1.9. The root mean square error of approximation (RMSEA) was estimated to be 0.07 with a 90% confidence interval of 0.00 to 0.13. Bentler's comparative fit index (CFI) was estimated to be 0.94 and the relative fit indices were 0.88 (NFI), 0.96 (IFI) and 0.86 (TLI). These summary statistics indicate a reasonable fit between the data and the model [13] [17].

TABLE 5
Fit Indices for the Estimation Model

	GFI	AGFI	X^2/df	CFI	RMSEA	NFI	TLI	IFI
Results	.98	.93	1.9	.94	.07	.88	.86	.94
Criteria	>.95	>.8	<2.0	<.95	<.07	>.9	>.9	>.9
Criteria Sources	[31]	[17]	[48]	[19]	[47]	[8]	[19]	[5]

The estimation also produced estimated path coefficients from the exogenous latent construct and among the endogenous latent constructs. These estimates are shown on Figure 2. The paths from privacy knowledge, privacy experience, and risk intolerance to concern for privacy were statistically significant (ß = .19, p < .01; ß = .30, p < .01, ß = .19, p < .01, respectively), offering support for Hypothesis 1, Hypothesis 2, and Hypothesis 3. In addition, the paths from concern for privacy to expected fee and likelihood of paying the fee were each significant (ß = .16, p < .05; ß = .23, p < .01, respectively), offering support for Hypothesis 4 and Hypothesis 5. The R-square values for concern for privacy, expected fee, and likelihood of paying the fee were .22, .03 and .05, respectively.

FIGURE 2
Estimated Model Using Standardized Path Coefficients



DISCUSSION

While this study contributes to a better understanding of the privacy concerns by social-media users, the unique aspects of this study must be acknowledged. First, it should be noted that subjects were students who may have different expectations about privacy than older people. The use of students seems to be a strength of this study and an opportunity for future research. As mentioned earlier, Pew Research reported that nearly 70% of Americans use some form of social media. That percentage is much higher for individuals in the 18 to 29-year-old range (i.e., 88%). However, studies about students' perceptions of privacy are relatively rare. For this reason, the present study is useful step that builds upon the work that has been done on students' concerns for privacy.

Henningsen, Valde, Entzminger, Dick, & Wilcher [14] studied privacy rules that emerge in student-educator interactions. Others, including Kyritsi, Zorkadis, Stavropoulos, & Verykios [26] and Rubel and Jones [41] have studied the ethics of big data analysis in dealing with student information, but did not deal with the students themselves. Moore & DeBruhl [32] surveyed students about their perceptions of Smartphone privacy and concluded that students are comfortable with sharing location data and contact data but are more concerned with the use of the smartphone to eavesdrop on specific conversations. Horton [18] surveyed students specifically on location data and found that male students had stronger privacy expectations than female students and that African American students had the highest expectation of privacy relative to other demographics with Asians having the lowest.

There have been some studies published on the perceptions of security within the populous as a whole, but few if any have been done on student populations [22, 24, 46]. Foltz, Cronan, and Jones [10] found that most students don’t read their University’s computer use handbooks. Adams and Sasse [2] report that most users don’t know a great deal about security. Siponen [44] add that most users are also unaware of the damage they can do through ill-considered responses to security situations.

Second, in this study the variance-explained in the likelihood that participants would pay a privacy fee was relatively small. While concern for privacy explained meaningful effects in users’ willingness to pay, further research is needed to better understand other outcomes of a user’s concern for privacy and other factors that might influence a user’s willingness to pay a fee. While it is clear that many users are concerned about privacy issues they “rarely make an effort to protect this data actively and often even give it away voluntarily” [12] (p. 226). Turow, Hennessy, and Draper [49] have argued that while social-media users may have concerns for privacy, one reason why they continue to share personal data is because they are “resigned to giving up their data” (p. 3). This seems to be supported by the Pew Research finding that “91% of consumers agreed that they have lost control of their personal information and data” [40].

REFERENCES

[1] Acquisti, A., L.K. John, and G. Loewenstein, *What is privacy worth?* The Journal of Legal Studies, 2013. 42(2): p. 249-274.

[2] Adams, A. and M.A. Sasse, *Users are not the enemy.* Communications of the ACM, 1999. 42(12): p. 41-46.

[3] Bentler, P.M., *Comparative fit indexes in structural models.* Psychological bulletin, 1990. 107(2): p. 238.

[4] Bobinac, A., et al., *Willingness to pay for a quality-adjusted life-year: the individual perspective.* Value in Health, 2010. 13(8): p. 1046-1055.

[5] Bollen, K.A., *Overall fit in covariance structure models: Two types of sample size effects.* Psychological bulletin, 1990. 107(2): p. 256.

[6] Brewer, A., et al., *Patient awareness, willingness, and barriers to point-of-care hepatitis C screening in community pharmacy.* Journal of the American Pharmacists Association, 2018. 58(4): p. S69-S72. e1.

[7] Bright, L.F., S.B. Kleiser, and S.L. Grau, *Too much Facebook? An exploratory examination of social media fatigue.* Computers in Human Behavior, 2015. 44: p. 148-155.

[8] Byrne, B.M., *Structural equation modeling with EQS and EQS/Windows: Basic concepts, applications, and programming*. 1994: Sage.

[9] Dommeyer, C.J. and B.L. Gross, *What consumers know and what they do: An investigation of consumer knowledge, awareness, and use of privacy protection strategies.* Journal of Interactive Marketing, 2003. 17(2): p. 34-51.

[10] Foltz, C.B., T. Paul Cronan, and T.W. Jones, *Have you met your organization's computer usage policy?* Industrial Management & Data Systems, 2005. 105(2): p. 137-146.

[11] Fornell, C. and D.F. Larcker, *Evaluating Structural Equation Models with Unobservable Variables and Measurement Error.* Journal of Marketing Research, 1981. 18(1): p. 39-50.

[12] Gerber, N., P. Gerber, and M. Volkamer, *Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior.* Computers & Security, 2018. 77: p. 226-261.

[13] Hair, J., Jr., et al., *Multivariate data analysis: with readings*. 1992, New York: MacMillan Publishing Company.

[14] Henningsen, M.L.M., et al., *Student Disclosures about Academic Information: Student Privacy Rules and Boundaries.* Communication Reports, 2019. 32(1): p. 29-42.

[15] Hong, W., F.K. Chan, and J.Y. Thong, *Drivers and Inhibitors of Internet Privacy Concern: A*

Multidimensional Development Theory Perspective. Journal of Business Ethics, 2019: p. 1-26.
[16] Hong, W. and J.Y. Thong, *Internet privacy concerns: An integrated conceptualization and four empirical studies.* Mis Quarterly, 2013: p. 275-298.
[17] Hooper, D., J. Coughlan, and M. Mullen, *Structural equation modelling: Guidelines for determining model fit.* Electronic Journal of Business Research Methods, 2008. 6(1): p. 53-60.
[18] Horton, J.E., *Privacy Under Pressure: A Survey of Privacy Expectations in the Modern Age*. 2018, Middle Tennessee State University.
[19] Hu, L.t. and P.M. Bentler, *Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives.* Structural equation modeling: a multidisciplinary journal, 1999. 6(1): p. 1-55.
[20] Jahangir, N. and N. Begum, *Effect of perceived usefulness, ease of use, security and privacy on customer attitude and adaptation in the context of e-banking.* Journal of Management Research (09725814), 2007. 7(3).
[21] Johnson, A. and E. Ortiz, *Without data-targeted ads, Facebook would look like a pay service, Sandberg says*, N. News, Editor. 2018.
[22] Kankanhalli, A., et al., *An integrative study of information systems security effectiveness.* International journal of information management, 2003. 23(2): p. 139-154.
[23] Katz, L., *Retailers are tracking where you shop—and where you sleep*, in *Bloomberg*. 2019.
[24] Khalfan, A.M., *Information security considerations in IS/IT outsourcing projects: a descriptive case study of two sectors.* International Journal of Information Management, 2004. 24(1): p. 29-42.
[25] Kumar, N., K. Mohan, and R. Holowczak, *Locking the door but leaving the computer vulnerable: Factors inhibiting home users' adoption of software firewalls.* Decision Support Systems, 2008. 46(1): p. 254-264.
[26] Kyritsi, K.H., et al., *The Pursuit of Patterns in Educational Data Mining as a Threat to Student Privacy.* Journal of Interactive Media in Education, 2019. 2019(1).
[27] Laufer, R.S. and M. Wolfe, *Privacy as a concept and a social issue: A multidimensional development theory.* Journal of Social Issues, 1977. 33(3): p. 22–42.
[28] Li, Y., *A multi-level model of individual information privacy beliefs.* Electronic Commerce Research and Applications, 2014. 13(1): p. 32-44.
[29] Liu, C., et al., *Beyond concern—a privacy-trust-behavioral intention model of electronic commerce.* Information & Management, 2005. 42(2): p. 289-304.
[30] Malhotra, N.K., S.S. Kim, and J. Agarwal, *Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model.* Information Systems Research, 2004. 15(4): p. 336-355.
[31] Miles, J. and M. Shevlin, *A time and a place for incremental fit indices.* Personality and Individual Differences, 2007. 42(5): p. 869-874.
[32] Moore, M. and B. DeBruhl, *Investigating University Student Desires and Use of Smartphone Privacy Settings.* The Journal of Computing Sciences in Colleges, 2019: p. 134.
[33] Nunnally, J., *Psychometric methods*. 1978, New York: McGraw-Hill.
[34] Ohkubo, M., K. Suzuki, and S. Kinoshita, *RFID privacy issues and technical challenges.* Communications of the ACM, 2005. 48(9): p. 66-71.
[35] Osatuyl, B., *Personality traits and information privacy concern on social media platforms.* Journal of Computer Information Systems, 2015. 55(4): p. 11-19.
[36] Piovesan, C., *How privacy laws are changing to protect personal information*, in *Forbes*. 2019.
[37] Png, I.P., *On the value of privacy from telemarketing: evidence from the'Do Not Call'registry.* Available at SSRN 1000533, 2007.
[38] Rainer, R.K. and A.W. Harrison, *Toward development of the end user computing construct in a university setting.* Decision Sciences, 1993. 24(6): p. 1187-1202.
[39] Rainie, L., *Americans' complicated feelings about social media in an era of privacy concerns.*, P.R.

Center, Editor. 2018.

[40] Rainie, L., *The state of privacy in post-Snowden America*, in *Pew Research Center FactTank*. 2016.

[41] Rubel, A. and K.M. Jones, *Student privacy in learning analytics: An information ethics perspective.* The Information Society, 2016. 32(2): p. 143-159.

[42] Ryski, M., *Do the benefits of using facial recognition in retail outweigh the risks?*, in *Real Wire*. 2019.

[43] Singh, T. and M.E. Hill, *Consumer privacy and the Internet in Europe: a view from Germany*. Journal of consumer marketing, 2003. 20(7): p. 634-651.

[44] Siponen, M.T., *Five dimensions of information security awareness.* ACM SIGCAS Computers and Society, 2001. 31(2): p. 24-29.

[45] Smith, H.J., T. Dinev, and H. Xu, *Information privacy research: an interdisciplinary review.* MIS quarterly, 2011. 35(4): p. 989-1016.

[46] Stanton, J.M., et al., *Analysis of end user security behaviors.* Computers & security, 2005. 24(2): p. 124-133.

[47] Steiger, J.H., *Understanding the limitations of global fit assessment in structural equation modeling.* Personality and Individual differences, 2007. 42(5): p. 893-898.

[48] Tabachnick, B.G., L.S. Fidell, and J.B. Ullman, *Using multivariate statistics*. Vol. 5. 2007: Pearson Boston, MA.

[49] Turow, J., M. Hennessy, and N. Draper, *The tradeoff fallacy: How marketers are misrepresenting American consumers and opening them up to exploitation.* Available at SSRN 2820060, 2015.