

# “Consumers’ online privacy concerns: causes and effects”

<b>AUTHORS</b>	Soumava Bandyopadhyay
<b>ARTICLE INFO</b>	Soumava Bandyopadhyay (2012). Consumers’ online privacy concerns: causes and effects. <i>Innovative Marketing</i> , 8(3)
<b>RELEASED ON</b>	Thursday, 08 November 2012
<b>JOURNAL</b>	"Innovative Marketing "
<b>FOUNDER</b>	LLC “Consulting Publishing Company “Business Perspectives”



NUMBER OF REFERENCES

0



NUMBER OF FIGURES

0



NUMBER OF TABLES

0

© The author(s) 2025. This publication is an open access article.

Soumava Bandyopadhyay (USA)

## Consumers' online privacy concerns: causes and effects

### Abstract

This article describes an empirical study that investigates the factors that influence American consumers' online privacy concerns and their outcomes. Consumers' online privacy concerns are found to be positively impacted by their perceived vulnerability to unauthorized gathering and use of personal information, and negatively impacted by their perceived ability to control the manner in which their personal information is collected and used online. The consumers' perceived vulnerability is negatively affected by their level of Internet literacy and their perceived ability to control the collection and use of information. In turn, the perceived ability to control information collection and use is positively influenced by both the Internet literacy level and the social awareness of the consumer. The privacy concerns of American consumers are found to negatively impact their willingness to provide personal information to web sites, their willingness to engage in e-commerce transactions, and even their willingness to surf the Internet. The implications of the findings for web site managers and designers are discussed.

**Keywords:** online privacy, information privacy, e-commerce, the United States.

### Introduction

Invasion of privacy on the Internet involves the unauthorized collection, disclosure, or other use of personal information (Wang, Lee, and Wang, 1998; Wills and Zeljkovic, 2011). As e-commerce continues to grow worldwide, companies are gathering an increasing amount of personal information from consumers on the Internet. Private information on consumers is now a commodity that is routinely bought, sold, and traded (Gillmor, 1998). Marketers across the board now collect detailed individual-level information to profile consumers, and increase the efficiency and effectiveness of their marketing strategies. It is now virtually impossible for consumers to transact business online without having to reveal personal information (Rust, Kannan and Peng, 2002). Personal information is also often asked for when consumers are required to register at web sites before being able to browse free content. In addition, consumers' personal information could be obtained involuntarily by the use of cookies that track people's online surfing behavior (Pierson and Heyman, 2011). Vast amounts of individual information can be very easily collected over the Internet, and digital networks can link all this private information in databases (Caruso, 1998). This information can then be bought, sold and traded, possibly without the consumers' permission, which increases consumers' concerns regarding having to reveal personal information online, and regarding the way in which such information might be used (Yao, Rice and Wallis, 2007; Ohm, 2010; Fletcher, 2003). Such concerns range from the intrusion of one's privacy and being targeted with unsolicited advertisements, to potential hassles resulting from online identity theft. Online privacy concerns are felt globally, as the Internet is a global medium, and

allows the transfer of massive amounts of consumer information instantly across national borders (Nijhawan, 2003). The fallout from such concerns about privacy could range from consumers declining to provide personal information online to the outright rejection of e-commerce, or even minimizing the use of the Internet (Nam et al., 2006; Dinev and Hart, 2006a; Wills and Zeljkovic, 2011).

Against this backdrop, we report a field study from the United States in this paper, which investigates a comprehensive set of factors that impact the online privacy concerns of consumers, and the possible outcomes of such concerns. A set of hypotheses is developed and tested. The managerial implications in terms of reducing consumers' online privacy concerns and encouraging e-commerce are also discussed.

### 1. Factors affecting online privacy concerns

Two major factors that have been identified in the literature as major influencers of online privacy concerns are: (1) the consumers' *perceived vulnerability* to the unauthorized gathering and misuse of personal information; and (2) the consumers' *perceived ability to control* the manner in which personal information is collected and used (Dinev and Hart, 2004). *Perceived vulnerability* describes the perceived potential risk when personal information is revealed (Raab and Bennett, 1998). The revelation of private information could be caused by many factors, such as accidental disclosure, unauthorized access, hacking into networks, etc. (Rindfleish, 1997). The possible negative consequences for consumers include identity theft (Saunders and Zucker, 1999), undesirable consumer profiling (Budnitz, 1998), and being targeted by unwanted advertising messages on the Internet (i.e., 'spam' e-mails). These factors contribute to consumers feeling increasingly vulnerable to the risk of misuse of their

private information on the Internet and, therefore, experiencing increased online privacy concerns (Dinev and Hart, 2004). The *perceived ability to control* is the extent to which consumers think they can prevent personal information from being disclosed online (Culnan and Armstrong, 1999). Consumers tend to think that information disclosure is less invasive to their privacy, and less likely to lead to negative consequences when they believe that they can control when and how such information is disclosed and used in the future. Hence, consumers' online privacy concerns are likely to be reduced by their perceived ability to control information collection and dissemination.

There is also a likely relationship between the perceived ability to control personal information collection and usage, and the perceived vulnerability to information misuse. If consumers feel that they can actually control how their private information is collected and used by web sites, they will also feel less vulnerable to the potential negative outcomes of information misuse. Therefore, perceived ability to control private information flow on the part of consumers will reduce their perceived vulnerability and, in turn, will reduce their online privacy concerns.

The preceding discussion leads to our first three research hypotheses.

*H1: Consumers' perceived vulnerability to unauthorized online data collection and use of such data is positively related to their online privacy concerns.*

*H2: Consumers' perceived ability to control the manner in which their personal information is collected and used online is negatively related to their online privacy concerns.*

*H3: Consumers' perceived ability to control the manner in which their personal information is collected and used online is negatively related to their perceived vulnerability to unauthorized online personal data collection and use of such data.*

Dinev and Hart (2006a) examined the role of Internet literacy and social awareness in influencing consumers' online privacy concerns. *Internet literacy* refers to the level of skill and knowledge possessed by consumers in using the Internet, including establishing an Internet connection, navigating the web, completing e-commerce transactions, protecting the computer from viruses and spyware, setting the browser's privacy and security options appropriately, and protecting one's privacy by employing adequate measures before disclosing information online (Dinev and Hart, 2006a; Spiekermann, Grossklags, and Berendt, 2001). In the context of our research, *social awareness* is described as the extent to which

consumers are knowledgeable about the social issues involving Internet usage (Dinev and Hart, 2006a), such as trust, privacy, security, governance, censorship, and restrictions (Burn and Loch, 2001; Papazafeiropoulou and Pouloudi, 2001). Social awareness requires raised interest and passive involvement in these social issues, and is a key in increasing consumer consciousness (Bickford and Reynolds, 2002). Consumers who are socially aware will be interested in and follow community and government policies and initiatives related to technology and the Internet (Schwartz and Solove, 2011). Because of their interest in social issues and policy, consumers with a high degree of social awareness will closely follow Internet privacy issues and the development of privacy policies and regulations (Dinev and Hart, 2006a).

Based on the above observations, we propose the following four hypotheses.

*H4: Consumers' Internet literacy level is negatively related to their perceived vulnerability to unauthorized online personal data collection and use of such data.*

*H5: Consumers' social awareness level is positively related to their perceived vulnerability to unauthorized online personal data collection and use of such data.*

*H6: Consumers' Internet literacy level is positively related to their perceived ability to control the manner in which their personal information is collected and used online.*

*H7: Consumers' social awareness level is positively related to their perceived ability to control the manner in which their personal information is collected and used online.*

## 2. Outcomes of online privacy concerns

Increased consumer concerns about online information privacy is likely to affect all Internet-based activities that could result in the collection and subsequent use of personal data. When consumers perceive that negative consequences could result from submitting personal data online, they are less likely to do so. At the minimal level, consumers who are concerned about their online privacy will be unwilling to disclose personal information to web sites (Nam et al., 2006). This may result in browsing only those web sites where no personal data is captured (Rice, McCreadie, and Chang, 2001), or providing only limited and anonymous, or even false personal information to web sites (Dinev and Hart, 2006b) that require "registration" prior to using content. Consumers with elevated online privacy concerns could be unwilling to make e-commerce transac-

tions altogether, since almost all such transactions require the disclosure of sensitive personal information, such as credit card numbers, telephone numbers, e-mail and postal addresses, etc. (Dinev and Hart, 2006a). Graeff and Harmon (2002) reported a survey where nearly three-quarters of the respondents said that they did not feel comfortable using their credit cards for online purchases. A recent study by Tsai et al. (2011) revealed that consumers were more likely to purchase products from web sites that displayed their privacy practices prominently, and were even willing to pay a premium price to buy from such web sites. Consumers who are very highly concerned about protecting their privacy online may realize that even if they do not voluntarily submit any personal information to a web site, information is still exchanged between the consumers' client computers and the host server of the web site. The information exchanged includes the client machine's IP address (leading to the identification of the site user's location), and details of the specific areas of the web site that have been visited. Some web sites install software (known as "spyware") on client machines without the users' knowledge and consent. This software monitors the users' web surfing activities and provides the information to a specific server (Staples, 2004). While the planting of spyware without the user's awareness and consent is illegal, many legitimate web sites install small files called "cookies" on user's hard drives for relatively benign purposes, such as letting the user personalize the web site, identifying registered users of a web site, recall stored shopping cart information at e-commerce sites, etc. Although legitimate web sites install cookies only with the user's permission (typically stated in their privacy policy), and they can be configured to run on web browsers only under the user's own settings, the cookies are normally executed without any user action (Strauss and Frost, 2012). This feature is startling to Internet users who are extremely concerned about online privacy, and may feel that they could be unknowingly and involuntarily disclosing sensitive information online. To protect their privacy, these consumers may be unwilling to use the Internet altogether in extreme cases.

Considering these three possible outcomes depending on the consumers' degree of concern about online privacy, we propose our final three research hypotheses.

*H8: Consumers' online privacy concerns are negatively related to their willingness to provide personal information online.*

*H9: Consumers' online privacy concerns are negatively related to their participation in e-commerce transactions.*

*H10: Consumers' online privacy concerns are negatively related to their willingness to use the Internet.*

### 3. Research method

**3.1. Construct operationalization.** The measures used to operationalize the constructs were adapted from relevant prior studies that explored some of the individual factors influencing online privacy concerns (Dinev and Hart, 2004; Dinev and Hart, 2006a; Dinev and Hart, 2006b; Sheehan and Hoy, 2000; Bellman et al., 2004; Yao, Rice, and Wallis, 2007; Culnan and Armstrong, 1999). Multi-item measures were established for the following variables: online privacy concerns (PRIVCON, 4 items); perceived vulnerability to unauthorized online personal data collection and use of such data (VULNER, 6 items); perceived ability to control the manner in which personal information is collected and used online (CONTROL, 4 items); Internet literacy (INTLIT, 4 items); social awareness (SOCAWARE, 6 items); willingness to provide personal information online (WILINFO, 3 items), willingness to participate in e-commerce (WILECOM, 3 items); and the willingness to use the Internet (WILUSE, 2 items). For each scale item, survey respondents were asked to indicate, on a 7-point Likert scale, their perception regarding a statement describing the relevant variable. The items for all the measures are listed in the Appendix.

**3.2. Sampling frame.** Internet users across the United States were given an online survey that included the multi-item scales to measure the study variables described above. The respondents were randomly selected from the online consumer panel of a major market research company. Altogether, 264 completed surveys were received. Of the 264 respondents, 147 (55.7%) were female. The average age of the respondents was 41.7 years, and 210 (79.5%) respondents were college graduates or beyond. The average time spent online by the respondents was 20.4 hours per week.

### 4. Results

**4.1. Measurement of scale properties.** After the responses were compiled, the reliability of each multi-item measure was assessed via calculating Cronbach's coefficient alpha. The Cronbach's alphas and the descriptive statistics for the eight measures used in the study are presented in Table 1. The scale reliabilities were found to be satisfactory, considering the relatively small number of items for each measure (Churchill, 1979).

Table 1. Descriptive statistics of the measures ( $N = 264$ )

Measure	Number of items	Reliability (Cronbach's alpha)	Mean (value range 1-7)	Standard deviation
Online privacy concerns (PRIVCON)	4	.948	5.28	1.46
Perceived vulnerability (VULNER)	6	.949	5.12	1.49
Perceived ability to control (CONTROL)	4	.867	5.51	1.23
Internet literacy (INTLIT)	4	.808	5.22	1.40
Social awareness (SOCAWARE)	6	.870	4.33	1.41
Willingness to provide personal information (WILINFO)	3	.644	3.31	1.37
Willingness to participate in e-commerce (WILECOM)	3	.862	4.84	1.62
Willingness to use the Internet (WILUSE)	2	.898	4.97	1.80

**4.2. Tests of hypotheses.** To test hypotheses H1 and H2, a regression analysis was done, with consumers' online privacy concerns (PRIVCON) as the dependent variable, and perceived vulnerability (VULNER) and perceived ability to control (CONTROL) as the independent variables. The results are indicated in Table 2. The overall regression model with the two predictor variables was found to be statistically significant ( $F = 41.44$

with 2 degrees of freedom,  $p < .001$ ), with  $R^2 = .241$ . Both predictor variables were found to significantly affect the online privacy concerns as well. As hypothesized, perceived vulnerability was positively related (standardized beta-coefficient estimate = .406,  $t = 7.02$ ,  $p < .001$ ), and perceived ability to control was negatively related (standardized beta-coefficient estimate = -.166,  $t = -2.87$ ,  $p < .01$ ) to online privacy concerns.

Table 2. Regression predicting consumers' online privacy concerns (PRIVCON)

Number of observations = 264 $R^2 = .241$ Overall $F = 41.44$ , d.f. = 2, $p < .001$		
Predictor variable	Standardized coefficient estimate	t-value (probability of t)
Intercept	0.00	5.46 ( $p < .001$ )
Perceived vulnerability (VULNER)	.406	7.02 ( $p < .001$ )
Perceived ability to control (CONTROL)	-.166	-2.87 ( $p < .01$ )

Hypotheses H3, H4, and H5 were tested via a regression analysis, with perceived vulnerability (VULNER) as the dependent variable, and perceived ability to con-

trol (CONTROL), Internet literacy (INTLIT), and social awareness (SOCAWARE) as the independent variables. The results are reported in Table 3.

Table 3. Regression predicting consumers' perceived vulnerability (VULNER)

Number of observations = 264 $R^2 = .379$ Overall $F = 14.55$ , d.f. = 3, $p < .01$		
Predictor variable	Standardized coefficient estimate	t-value (probability of t)
Intercept	0.00	4.23 ( $p < .001$ )
Perceived ability to control (CONTROL)	-.349	-5.97 ( $p < .001$ )
Internet literacy (INTLIT)	-.208	-3.49 ( $p < .001$ )
Social awareness (SOCAWARE)	.102	2.00 ( $p < .05$ )

As seen from Table 3, the overall regression model was statistically significant at the  $p < .01$  level ( $F = 14.55$  with 3 degrees of freedom), with  $R^2 = .379$ . Perceived ability to control had a significant negative impact on perceived vulnerability (standardized beta-coefficient estimate = -.349,  $t = -5.97$ ) at the  $p < .001$  level. Internet literacy also had a significantly negative impact on perceived vulnerability (standardized beta-coefficient estimate = -.208,  $t = -3.49$ ), again at the  $p < .001$  level. Social awareness was found to have a significantly positive effect on perceived vulnerability (standardized beta-coefficient estimate = .102,  $t =$

2.00,  $p < .05$ ). Therefore, hypotheses H3, H4, and H5 were supported.

A regression analysis with perceived ability to control (CONTROL) as the dependent variable, and Internet literacy (INTLIT) and social awareness (SOCAWARE) as the independent variables was carried out to test hypotheses H6 and H7. The results are reported in Table 4. The overall regression model came out to be statistically significant at the  $p < .001$  level ( $F = 30.67$ , with 2 degrees of freedom). The  $R^2$  value obtained was .214. Internet literacy was found to positively impact the perceived ability to control (standardized beta-

coefficient estimate = .190,  $t = 3.18$ ,  $p < .001$ ). Social awareness was also found to positively impact the perceived ability to control (standardized

beta-coefficient estimate = .199,  $t = 3.31$ ,  $p < .001$ ). Therefore, both hypotheses H6 and H7 were supported.

Table 4. Regression predicting consumers' perceived ability to control (CONTROL)

Number of observations = 264 $R^2 = .214$ Overall $F = 30.67$ , d.f. = 2, $p < .001$		
Predictor variable	Standardized coefficient estimate	t-value (probability of $\dagger$ )
Intercept	0.00	7.92 ( $p < .001$ )
Internet literacy (INTLIT)	.190	3.18 ( $p < .001$ )
Social awareness (SOCAWARE)	.199	3.31 ( $p < .001$ )

The hypotheses regarding the outcomes of consumers' online privacy concerns (H8 through H10) were tested by correlating the consumers' privacy concerns (PRIVCON) with the three possible outcomes: willingness to provide personal information online (WILINFO), willingness to participate in e-commerce (WILECOM), and willingness to use the Internet (WILUSE). The Pearson correlation coefficient between online privacy concerns and willingness to provide personal information online was  $-.425$  (significant at the  $p < .001$  level), thus supporting the hypothesized negative relationship between the two variables (H8). The Pearson correlation coefficient between online privacy

concerns and the willingness to participate in e-commerce was also negative ( $-.387$ ) and significant at the  $p < .001$  level. This provided support for hypothesis H9. The Pearson correlation coefficient between online privacy concerns and the willingness to use the Internet came out to be  $-.325$ , which was statistically significant at the  $p < .001$  level. This negative relationship provided support for hypothesis H10.

### 5. Discussion and managerial implications

The results of the tests of hypotheses are summarized in Table 5 below. It is seen that the empirical data provided support for all ten hypotheses that were tested.

Table 5. Summary results of the tests of hypotheses

Hypotheses		Result
H1	Perceived vulnerability → + Online privacy concerns	Supported ( $p < .001$ )
H2	Perceived ability to control → - Online privacy concerns	Supported ( $p < .001$ )
H3	Perceived ability to control → - Perceived vulnerability	Supported ( $p < .01$ )
H4	Internet literacy → - Perceived vulnerability	Supported ( $p < .01$ )
H5	Social awareness → + Perceived vulnerability	Supported ( $p < .05$ )
H6	Internet literacy → + Perceived ability to control	Supported ( $p < .001$ )
H7	Social awareness → + Perceived ability to control	Supported ( $p < .001$ )
H8	Online privacy concerns → - Willingness to provide personal information online	Supported ( $p < .001$ )
H9	Online privacy concerns → - Willingness to participate in e-commerce	Supported ( $p < .001$ )
H10	Online privacy concerns → - Willingness to use the Internet	Supported ( $p < .001$ )

The study results suggest that online privacy concerns of American consumers could be reduced by reducing their perceived vulnerability to information misuse and its consequences, and by increasing their perceived ability to control the collection and use of sensitive personal information online (hypotheses H1 and H2). The perceived vulnerability itself could also be reduced (thus reducing the privacy concerns, in turn) by increasing the consumers' perceived ability to control information collection and usage (hypothesis H3), and by increasing their level of Internet literacy (hypothesis H4). The perceived ability to control can be positively impacted by the consumers' level of Internet literacy and their level of awareness of social issues involving Internet usage (hypotheses H6 and H7). Online marketers should, therefore,

make efforts to increase the consumers' Internet literacy by educating them about the options available for protecting private information. For example, they can post information on their web sites about specific software (e.g., firewalls, browser security fixes) or procedures (e.g., setting browser configurations to prevent tracking cookies being implanted without the user's permission) that may alleviate privacy concerns by increasing the perceived control and reducing the perceived vulnerability (Spiekermann, Grossklags, and Berendt, 2001). Given the relatively high educational achievements of Internet users (79.5% in our study sample were college graduates or beyond), such information should be easily understood by the majority of people using the Internet and, therefore, should be effective.

In our study, social awareness was found to directly impact the consumers' perceived vulnerability to unauthorized information gathering and use (hypothesis H5). In addition, a heightened level of social awareness positively affected the consumers' perceived ability to control the collection and use of personal information (hypothesis H7), and therefore, could be said to negatively influence online privacy concerns (following hypothesis H2) indirectly. Internet marketers can seek to increase the social awareness of consumers by posting a comprehensive privacy policy prominently on the home page of their web site (Hui, Teo, and Lee, 2007; Tsai et al., 2011). A key element is to convince the consumers regarding the procedural fairness in the collection and use of personal data, and increasing the consumers' trust in the web site (Culnan and Armstrong, 1999). Specific measures that marketers may implement include promoting the reputation and legitimacy of the company requesting information (Andrade, Kaltcheva, and Weitz, 2002), displaying third-party privacy seals such as VeriSign, TrustE, etc. on their web sites (Hui, Teo, and Lee, 2007). It is also prudent for online marketers not to ask for more information than is absolutely necessary for effecting e-commerce transactions.

Our study shows that when consumers are highly concerned with their online privacy, they are less willing to disclose personal information online, are less inclined to participate in e-commerce transactions, and are even prepared to minimize their Internet surfing (hypotheses H8, H9, and H10, respectively). These negative consequences of consumers' online privacy concerns are not acceptable to marketers who rely on enhancing their marketing strategies (consumer profiling, better targeting, etc.) by collecting and analyzing individual-level data, or who offer e-commerce

transactions on their web sites. To reduce the probability of these negative outcomes, marketers will need to address the antecedents of online privacy concerns and alleviate those concerns. The demographic information revealed that 68.9% of the respondents (182 out of 264) would read the "privacy policy" posted on a web site "sometimes, often, or always" before providing any personal information to the site, or before conducting any financial transaction at the site. Only 9.5% of the respondents (25 out of 264) indicated that they never read the "privacy policy," and 21.6% (57 out of 264) said they rarely read it. This suggests that if online marketers choose to offer comprehensive information about protecting the site visitors' privacy, consumers are more than likely to read that information and that would certainly help in reducing their privacy concerns and encouraging them to provide personal information online, and participate in e-commerce.

### Conclusion

We presented the results of an empirical test to investigate the influence of specific factors on the online privacy concerns of consumers in the United States, and the interrelationships among those factors. We also identified the undesirable outcomes of consumers' online privacy concerns on Internet marketers, e.g., reluctance to disclose personal information online, and reluctance to engage in e-commerce transactions. Online marketers need to understand the influencing factors and address them appropriately (as outlined in the managerial implications), so that consumers' online privacy concerns are reduced and they are willing to disclose personal information on the Internet, and participate in e-commerce.

### References

1. Andrade, E.B., Kaltcheva, V. & Weitz, B. (2002). Self-Disclosure on the Web: The Impact of Privacy Policy, Reward, and Company Reputation, *Advances in Consumer Research*, 29, pp. 350-353.
2. Bellman, S., Johnson, E.J., Kobrin, S.J. & Lohse, G.L. (2004). International Differences in Information Privacy Concerns: A Global Survey of Consumers, *The Information Society*, 20, pp. 313-324.
3. Budnitz, M. (1998). Privacy Protection for Consumer Transactions in Electronic Commerce: Why Self-Regulation is Inadequate, *South Carolina Law Review*, 49 (1), pp. 847-886.
4. Bickford, D.M. & Reynolds, M. (2002). Activism and Service-Learning: Reframing Volunteerism as an Act of Dissent, *Critical Approaches to Teaching, Literature, Language, Composition, and Culture*, 8 (2), pp. 229-252.
5. Burn, J. & Loch, K. (2001). The Societal Impact of the World Wide Web-Key Challenges for the 21<sup>st</sup> Century, *Information Resources Management Journal*, 14 (4), pp. 4-14.
6. Caruso, D. (1998). The Law and the Internet Beware, *Columbia Journalism Review*, 37 (1), pp. 57-61.
7. Churchill, G.A., Jr. (1979). A Paradigm for Developing Better Measures of Marketing Constructs, *Journal of Marketing Research*, 16 pp. 64-73.
8. Culnan, M. & Armstrong, P. (1999). Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation, *Organization Science*, 10 (1), pp. 104-115.
9. Dinev, T. & Hart, P. (2004). Internet Privacy Concerns and Their Antecedents—Measurement Validity and a Regression Model, *Behavior and Information Technology*, 23 (6), pp. 413-422.

10. Dinev, T. & Hart, P. (2006a). Internet Privacy Concerns and Social Awareness as Determinants of Intention to Transact, *International Journal of Electronic Commerce*, 10 (2), pp. 7-29.
11. Dinev, T. & Hart, P. (2006b). Privacy Concerns and Levels of Information Exchange: An Empirical Investigation of Intended E-Service Use, *E-Service Journal*, 6 (1), pp. 25-59.
12. Fletcher, K. (2003). Consumer Power and Privacy: The Changing Nature of CRM, *International Journal of Advertising*, 22, pp. 249-272.
13. Gillmor, D. (1998). Violating Privacy is Bad Business, *Computerworld*, 32 (12), pp. 38-39.
14. Graeff, T.R. & Harmon, S. (2002). Collecting and Using Personal Data: Consumers' Awareness and Concerns, *The Journal of Consumer Marketing*, 19, pp. 302-318.
15. Hui, K., Teo, H. & Lee, S.T. (2007). The Value of Privacy Assurance: An Exploratory Field Experiment, *MIS Quarterly*, 31 (1), pp. 19-33.
16. Nam, C., Song, C., Lee, E. & Park, C. (2006). Consumers' Privacy Concerns and Willingness to Provide Marketing-Related Personal Information Online, *Advances in Consumer Research*, 33, pp. 212-217.
17. Nijhawan, D.R. (2003). The Emperor Has No Clothes: A Critique of Applying the European Union Approach to Privacy Regulation in the United States, *Vanderbilt Law Review*, 56 (3), pp. 939-976.
18. Ohm, P. (2010). Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, *UCLA Law Review*, 57, pp. 1701-1777.
19. Papazafeiropoulou, A. & Pouloudi, A. (2001). Social Issues in Electronic Commerce: Implications for Policy Makers, *Information Resources Management Journal*, 14 (4), pp. 24-32.
20. Pierson, J. & Heyman, R. (2011). Social Media and Cookies: Challenges for Online Privacy. *Info: The Journal of Policy, Regulation, and Strategy for Telecommunications, Information, and Media*, 13 (6), pp. 30-42.
21. Raab, C.D. & Bennet, C.J. (1998). The Distribution of Privacy Risks: Who Needs Protection? *The Information Society*, 14 (4), pp. 253-262.
22. Rice, R.E., McCreddie, M. & Chang, S.L. (2001). *Accessing and Browsing Information and Communication*, Cambridge, MA: The MIT Press.
23. Rindfleish, T.C. (1997). Privacy, Information Technology, and Healthcare, *Communications of the ACM*, 40, pp. 92-100.
24. Rust, R.T., Kannan, P.K. & Peng, N. (2002). The Customer Economics of Internet Privacy, *Journal of the Academy of Marketing Science*, 30, pp. 455-464.
25. Saunders, K. & Zucker, B. (1999). Contracting Identity Fraud in the Information Age: The Identity Theft and Assumption Deterrence Act, *International Review of Law, Computers, and Technology*, 13 (2), pp. 183-192.
26. Schwartz, P.M. & Solove, D.J. (2011). The PII Problem: Privacy and a New Concept of Personally Identifiable Information, *New York University Law Review*, 86, pp. 1815-1894.
27. Sheehan, K.B. & Hoy, M.G. (2000). Dimensions of Privacy Concern Among Online Consumers, *Journal of Public Policy and Marketing*, 19 (1), pp. 62-73.
28. Spiekermann, S., Grossklags, J. & Berendt, B. (2001). E-Privacy in 2<sup>nd</sup> Generation E-Commerce. Privacy Preferences versus Actual Behavior. In *Proceedings of EC'01: Third ACM Conference on Electronic Commerce*. New York: Association for Computing Machinery, pp. 38-47.
29. Staples, B. (2004). The Battle Against Junk Mail and Spyware on the Web, *The New York Times*, January 3.
30. Strauss, J. & Frost, R. (2012). *E-Marketing*, 6<sup>th</sup> ed. Upper Saddle River, NJ: Pearson Prentice Hall.
31. Tsai, J.Y., Egelman, S., Cranor, L. & Acquisti, A. (2011). The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study, *Information Systems Research*, 22 (2), pp. 254-268.
32. Wang, H., Lee, M.K.O. & Wang, C. (1998). Consumer Privacy Concerns about Internet Marketing, *Communications of the ACM*, 41, pp. 63-70.
33. Wills, C.E. & Zeljkovic, M. (2011). A Personalized Approach to Web Privacy: Awareness, Attitudes, and Actions, *Information Management & Computer Science*, 19 (1), pp. 53-73.
34. Yao, M.Z., Rice, R.E. & Wallis, K. (2007). Predicting User Concerns About Online Privacy, *Journal of the American Society for Information Science and Technology*, 58 (5), pp. 710-722.

## Appendix. Survey items

**Online privacy concerns (PRIVCON).** To what extent (on a scale from 1 to 7) do you agree with the following?

1. I am concerned that the information I submit on the Internet could be misused.
2. When I shop online, I am concerned that the credit card information can be stolen while being transferred on the Internet.
3. I am concerned about submitting information on the Internet because of what others might do with it.
4. I am concerned about submitting information on the Internet because it can be used in a way I have not foreseen.

**Perceived vulnerability (VULNER).** To what extent (on a scale from 1 to 7) do you think the following could happen to you when you use the Internet?

1. Records of online transactions could be sold to third parties.
2. Personal information submitted could be misused.



3. Personal information could be made available to individuals or companies without my knowledge.
4. Personal information could be made available to government agencies.
5. Personal information could be inappropriately used.
6. Unauthorized charges could be made against credit card information submitted.

**Perceived ability to control (CONTROL).** To what extent (on a scale from 1 to 7) do you agree with the following?

1. I would only submit accurate and personal information at a web site if the site allowed me to control the information I volunteer.
2. I would only provide accurate and personal information at a web site if the site allowed me to control the information they can use.
3. Being able to control the personal information I provide to a web site is important to me.
4. I would only provide accurate and personal information at a web site if their control policy is verified/monitored by a reputable third party.

**Internet literacy (INTLIT).** Rate (on a scale from 1 to 7) the extent to which you are able to do the following tasks:

1. Identify and delete a program which you consider intrusive (spyware) and which was installed through the Internet without your knowledge and permission.
2. Manage virus attacks by using antivirus software.
3. Communicate through instant messaging or discussion boards.
4. Download files/audio/video/executables from the Internet.

**Social awareness (SOCAWARE).** To what extent (on a scale from 1 to 7) do you agree with the following?

1. I am interested in reading political commentaries or watching them on TV.
2. I closely follow developments in my community.
3. I enjoy discussing important social issues with others.
4. I watch news and other television programs/channels that address current issues.
5. I closely follow government regulation of high-tech businesses.
6. I read at least one newspaper every day or watch news on TV.

**Willingness to provide personal information (WILINFO).** To what extent (on a scale from 1 to 7) do you agree with the following?

1. I am generally unwilling to disclose personal information at a web site.
2. I avoid using web sites that require personal information about myself before letting me use the content.
3. If a web site requires registration with personal information before letting me use the content, I generally provide false information.

**Willingness to participate in e-commerce (WILECOM).** To what extent (on a scale from 1 to 7) are you willing to use the Internet to do the following?

1. Purchase goods (e.g., books) or services (e.g., airline tickets) from web sites that require me to submit accurate and identifiable information (e.g., credit card information).
2. Conduct sales transactions at e-commerce sites that require me to provide credit card information.
3. Retrieve highly personal and password-protected financial information from the Internet (e.g., using web sites that allow me to access my bank account or credit card account).

**Willingness to use the Internet (WILUSE).** To what extent (on a scale from 1 to 7) do you agree with the following?

1. I avoid using the Internet altogether because I am afraid that my personal information can be automatically collected by web sites without my knowledge or permission.
2. I use the Internet only in very limited circumstances because I am scared of giving away my personal information to strangers.