

# ONLINE INFORMATION PRIVACY: MEASURING THE COST-BENEFIT TRADE-OFF

## **Il-Horn Hann**

Marshall School of Business  
University of Southern California  
Los Angeles, CA USA  
hann@marshall.usc.edu

## **Kai-Lung Hui**

Department of Information Systems  
National University of Singapore  
Singapore  
lung@comp.nus.edu.sg

## **Tom S. Lee**

Department of Information Systems  
National University of Singapore  
Singapore  
tlee@comp.nus.edu.sg

## **I. P. L. Png**

Department of Information Systems  
National University of Singapore  
Singapore  
ipng@comp.nus.edu.sg

## **Abstract**

*Concern over information privacy is widespread and rising. However, prior research is silent about the value of information privacy and the benefit of privacy protection. We conducted a conjoint analysis to explore individuals' trade-offs between the benefits and costs of providing personal information to Websites. We find that economic incentives (monetary reward and future convenience) do affect individuals' preferences over Websites with differing privacy policies. For instance, the disallowance of secondary use of personal information is worth between \$39.83 and \$49.78. Surprisingly, we find that cost-benefit trade-offs did not vary with personal characteristics including gender, contextual knowledge, individualism, and trust propensity.*

## **1 INTRODUCTION**

Privacy has been identified to be a major, if not the most critical, impediment to e-commerce:

In our view, the single, overwhelming barrier to rapid growth of e-commerce is a lack of consumer trust that consumer protection and privacy laws will apply in cyberspace. Consumers...worry, deservedly, that supposedly legitimate companies will take advantage of them by invading their privacy to capture information about them for marketing and other secondary purposes without their informed consent (U.S. Public Interest Research Group 2000).

Even before the advent of e-commerce, there was broad concern about the collection of personal information in various contexts, including employment, retailing and direct marketing, and government. These concerns prompted government action. In 1974, the U.S. Congress passed the Privacy Act to regulate government collection and use of personal information.<sup>1</sup> In 1980, the Organization for Economic Co-operation and Development (OECD) published its guidelines to harmonize the collection and use

---

<sup>1</sup>Specifically, the Privacy Act of 1974 prohibits unauthorized disclosures of records, gives individuals the right to review records about themselves, to check whether records have been disclosed, and to request corrections or amendments.

of personal information by government and private organizations (OECD 1980). Further, in 1995, the European Union adopted a data protection directive, which not only regulates information within the Union but also indirectly regulates information beyond the Union. The Directive disallows transfer of information to other countries that do not provide adequate protection.

Rapid improvements in computing technologies have accentuated concern about privacy: “There has been a well-documented transformation in consumer privacy attitudes over the past decade, moving concerns from a modest matter for a minority of consumers in the 1980s to an issue of high intensity expressed by more than three-fourth of American consumers in 2001” (Westin 2001).

The advent and growth of e-commerce has amplified public concern about privacy, and especially privacy on electronic networks. The widespread concern gave impetus to new legislation. In 1998, the U.S. Congress enacted the Children’s Online Privacy Protection Act to regulate the online collection and use of children’s personal information.

There continues to be public pressure for more legislation. Over 50 bills to regulate online privacy were introduced in the first session of the 107th Congress. However, resistance to more regulation has formed. The Online Privacy Alliance (OPA) claims that further legislation would diminish national competitiveness and weaken the new economy.<sup>2</sup> Hahn (2001) estimates the cost of complying with these legislative proposals to be \$9 billion and \$36 billion.

This leads to our research objective: Exactly how much do individuals perceive to be the cost of releasing personal information online? The real issue is not whether consumers value online privacy. It is obvious that people value online privacy. What is not known is how *much* people value their privacy online. Despite tremendous debate and policy interest, to date there has been little research into this question.

Businesses need this information to decide whether to invest in privacy seals and what incentives to offer consumers for their personal information. Governments need this information to decide on public policy toward information privacy. For instance, Laudon (1996) and Varian (1997) have proposed to regulate privacy through markets in personal information, but the economic viability of such markets depends on individuals’ perceived value of privacy.

In this study, we apply conjoint analysis, which is the standard way of measuring consumer trade-offs (Green and Srinivasan 1990), to respondents’ rankings of alternative combinations of economic incentives and privacy policies in an online setting. Specifically, we construct a set of conjoint stimuli using two economic incentives (monetary reward and future convenience) and three privacy concerns (errors in storing or processing personal information, unauthorized secondary use of information, and improper access to information). We then assess the relative importance and contribution of these dimensions from the estimated part-worth patterns, and relate the respondents’ trade-offs to personal characteristics including gender, cultural trait, degree of trust propensity, and experience with privacy technologies.

## 2 LITERATURE REVIEW

Privacy is the ability to control the acquisition and use of one’s personal information (Westin 1967). That control over information is a key dimension of privacy has been stressed by researchers in diverse disciplines including law, information systems, marketing, organizational and social sciences, and psychology (Foddy and Finighan 1981; Goodwin 1991; Milne 2000; Nowak and Phelps 1997; P. Schwartz 2000; Simitis 1987; Smith et al. 1996; Stone and Stone 1990; Wang et al. 1998).

Opinion polls, surveys, and experiments have repeatedly shown information privacy to be of utmost concern (Cranor et al. 1999; Culnan and Milne 2001; Esrock and Ferre 1999; Fox 2000; Hoffman et al. 1999a; Katz and Tassone 1990; Phelps et al. 2000; Stone et al. 1983). However, Culnan (1993) finds that concern over privacy might not affect consumers’ attitudes toward secondary information use. Further, in unprompted surveys, individuals do not rate privacy to be a top priority (Harper and Singleton 2001).

Concern over privacy has been related to cultural values and trust. Specifically, people in more individualistic cultures as measured by Hofstede’s (1991) individualism-collectivism index are more concerned about privacy (Milberg et al. 2000; Smith 2001). In various organizational and marketing contexts, perceptions of privacy invasion have been shown to depend on

---

<sup>2</sup>The Online Privacy Alliance (OPA) is an advocacy group under the aegis of the U.S. Direct Marketing Association.

information control, outcomes arising from disclosures, information type and sensitivity, perceived relevancy of information use, and target of disclosures (Eddy et al. 1999; Fusilier and Hoyer 1980; Mael et al. 1996; Stone et al. 1983; Tolchinsky et al. 1981; Woodman et al. 1982).<sup>3</sup> Hoffman et al. (1999) find widespread lack of trust in Website privacy practices: nearly 63 percent of consumers would not provide information to Websites owing to lack of trust.

Concern over privacy has also been related to contextual knowledge (Stone and Stone 1990). Industrial and occupational psychologists and other professionals who are familiar with the use of bio-data systematically rated the collection of bio-data to be less invasive than respondents with less prior experience with bio-data (Mael et al. 1996). When assessing information privacy concerns, marketing and advertising professionals expressed less concern than other individuals (Esrock and Ferre 1999).

Finally, concern over privacy has been related to gender. Testifying before a Congressional subcommittee, privacy expert Alan Westin (2001) declared: “privacy now scores as one of the top consumer and social-policy issues in the U.S., especially intense among women.” However, the conclusions from previous research have been mixed: while women have a greater tendency to self-disclosure (Archer 1979; Cozby 1973) and have shown more openness during interviews (Fletcher and Spencer 1984), there is some evidence that they have stronger preference for privacy (Marshall 1974; Pedersen 1987).

A countervailing stream of research has focused on the benefits of releasing personal information and the cost of privacy regulation. Economists have emphasized that limits on the disclosure of information might render markets less efficient in allocation of scarce resources (Posner 1981; Stigler 1980).<sup>4</sup> As discussed earlier, the cost to industry of complying with various legislative proposals has been estimated to be substantial.

Anecdotal evidence shows that people are willing to disclose personal information for potential monetary savings (Russell 1989), and people do join Websites for free gifts and catalogs (Oberndorf 1999; S. Schwartz 2000). Further, compensation received the highest weight in a conjoint analysis of the factors influencing participation in direct mail (Milne and Gordon 1993).<sup>5</sup> The evidence supports the proposition that individuals respond to economic incentives in deciding whether to disclose information.

### 3 HYPOTHESES

Our first group of hypotheses investigates the value of online privacy in economic terms. Survey and experimental evidence has shown that privacy is of utmost concern (Esrock and Ferre 1999; Hoffman et al. 1999a; Phelps et al. 2000; Stone et al. 1983). However, economic theories suggest that individuals would disclose personal information for sufficient benefit. We operationalize the economic benefit in terms of two dimensions: monetary reward and future time saving. Many Websites offer coupons and discounts and customized shopping processes (for instance, Amazon’s one-click ordering) to consumers who register and provide personal information. Accordingly, we formulate the following null hypotheses:

- H1. An individual’s preferences over Websites are not affected by
- (a) monetary reward
  - (b) time saving

Our second group of hypotheses relates the perceived cost of online privacy to the individual’s personal characteristics. Given the prior literature, we formulate four hypotheses relating to gender, contextual knowledge, individualism-collectivism, and trust propensity.

---

<sup>3</sup>Control was commonly operationalized by allowing information to be disclosed only with the subjects’ permission.

<sup>4</sup>An often-cited example is the labor market. Job seekers have incentives to hide past criminal or bad test records, but employers need such information to make optimal employment decisions.

<sup>5</sup>Milne and Gordon’s conjoint analysis involved trade-offs among compensation, targeting, volume, and permission. These dimensions, however, do not clearly represent positive or negative consequences of revealing personal information. It is difficult to use their estimated part-worths to infer individuals’ willingness of trading privacy for positive reinforcements.

- H2. An individual's preferences over Websites with differing privacy policies and economic benefits do not depend on
- (a) gender
  - (b) prior contextual knowledge
  - (c) differences in individualism
  - (d) differences in trust propensity

## 4 EXPERIMENTAL DESIGN

Prior to the conjoint study, we conducted focus group discussions with upper-division undergraduate students to solicit their views on privacy practices and the economic rewards that they expected from Websites. The focus groups suggested that individuals value direct monetary savings, but they tended to measure the benefit from convenient access in terms of the frequency of visit rather than the explicit time saving per transaction. To reflect such a consideration, we operationalized convenience by "expected visit frequency" in our conjoint experiment.

Regarding the costs of privacy, we considered the four concern dimensions identified by Smith et al. (1996): collection, error, secondary use, and improper access.<sup>6</sup> Logically, collection is a necessary antecedent to the three other dimensions. Error, secondary use, and improper access of information can not happen without *ex ante* collection of personal information. Therefore, in our study, we controlled for the collection of information and focused only on the other three dimensions.

Taken together, our conjoint study assessed trade-offs among five dimensions—two economic rewards and three privacy concerns. The three concerns were manipulated by the presence (or absence) of proper information handling procedures. We created three treatment levels of monetary reward (\$5, \$10, and \$20) and visit frequency (monthly, weekly, and daily).<sup>7</sup> All of these are relevant levels of economic considerations that were reflected by subjects in the focus groups.

Based on these five dimensions and their manipulations, there are a maximum of  $3 \times 3 \times 2 \times 2 \times 2 = 72$  conjoint stimuli. To avoid asking subjects to rank too many alternatives, we selected 18 stimuli based on an optimal orthogonal design (Addelman 1962). An example of a stimulus is a Website that provides a \$5 reward, has no error correction procedure, no prevention of secondary use or improper access of information, and which the subject expects to visit only once a month.

To assess hypothesis 2, we included a demographic survey that captured subjects' gender, prior contextual knowledge, degree of individualism, and trust propensity. Contextual knowledge was operationalized by two measures: knowledge of cookies and anonymous Web surfing (exemplified by Anonymizer.com). The degree of individualism was measured with a set of previously validated instruments due to Triandis (1988). Trust propensity was measured using instruments adapted from Michael (1992).

We also controlled for the degree of information collection by telling the subjects that all 18 stimuli (that is, hypothetical Websites) requested the same set of personal information from the subjects.

The subjects were upper-division undergraduate students who were enrolled in an e-commerce course. The procedure of the experiment was as follows: first, all subjects completed the demographic survey. The experimental task and the meanings of the five dimensions were then explained. Finally, the subjects ranked the 18 stimuli based on their personal preferences. All subjects received course credits upon completing the experiment. After deleting incomplete rankings/surveys, we had a total of 184 usable responses.

## 5 FINDINGS

Conjoint analysis assumes that an individual's ranking of each stimulus can be decomposed into the sum of contributions from the multiple dimensions. For each dimension, the contribution is the part-worth multiplied by the level of that dimension. Essentially, the part-worth of a dimension is the marginal utility of that dimension in ranking the conjoint stimuli.

---

<sup>6</sup>These dimensions were further validated by Stewart and Segars (2002).

<sup>7</sup>All rewards were framed in Singapore dollars. As of April 2002, one Singapore dollar = 54 U.S. cents.

**Table 1. Part-Worths and Relative Importance**

Instruments	Levels	Part-Worth	Relative Importance
Monetary Reward	\$5	0	11.69%
	\$10	0.2319 (0.1648)	
	\$20	1.3877*** (0.2808)	
Visit Frequency	Monthly	0	6.02%
	Weekly	0.4321*** (0.1533)	
	Daily	0.7147*** (0.2541)	
Error	No Review	0	15.06%
	Review	1.7867*** (0.1935)	
Improper Access	No restriction	0	28.43%
	Restriction	3.3736*** (0.3489)	
Secondary Use	Allowed	0	38.80%
	Not allowed	4.6046*** (0.2969)	

Standard errors in parentheses

\*\*\*Significant at 1% level

The estimated part-worths enable us to directly infer the individuals' trade-offs among the five dimensions. While past research can indicate the relative levels of privacy concerns, it cannot address managerial questions such as how much money Websites must offer to overcome individuals' concern over secondary use of information. Our conjoint analysis directly addresses such questions.

We use least-squares regression with dummy variables to estimate each subject's part-worths and then calculate the relative importance of the five dimensions. Table 1 reports the means of the part-worths and relative importance for the 184 subjects.

We test H1(a) as follows. Since our sample was relatively large, the central-limit theorem implies that the estimated part-worths for monetary reward should approximately follow a normal distribution. We then apply a t-test to determine whether the part-worth was statistically different from zero.

Referring to Table 1, the part-worth for a \$20 reward is 1.3877 and is statistically significant. This means that a Website offering a \$20 reward for personal information will raise its ranking by 1.3877 (out of 18) as compared to an otherwise identical Website offering the base level \$5 reward.

By contrast, the part-worth for a \$10 reward is 0.2319 but not significant. Therefore, H1(a) is rejected for a \$20 reward but not for a \$10 reward. These results suggest that, in individuals' decision on whether to provide information to Websites, a monetary reward has an effect only when it exceeds a threshold level. A sufficiently large monetary reward does increase the relative attractiveness of a Website. Equivalently, there are increasing returns to monetary rewards.

We can use these results to calculate the marginal utility of \$1 reward. Between the \$20 and \$5 rewards, the \$15 increase raises the ranking by 1.3877, hence the marginal utility was 0.0925 per dollar of reward. Alternatively, between the \$20 and \$10 rewards, the \$10 increase raises the ranking by  $1.3877 - 0.2319 = 1.1558$ , or 0.1156 per dollar of reward. These two estimates provide a range of 0.0925 – 0.1156 per dollar of reward.

**Table 2. Value of Privacy**

Website Privacy Policy	Value
Review for error	\$15.46 to \$19.32
Restriction against secondary access	\$29.18 to \$36.47
Secondary use not allowed	\$39.83 to \$49.78

We apply a similar procedure to test the part-worths for visit frequency. The part-worths at both monthly and daily frequencies are significant, and hence H1(b) is rejected at both levels. Time saving has a positive effect on individuals' preferences. However, the effect of weekly visits is not significantly different from the effect of daily visits.

The part-worths for all three privacy concerns are statistically significant. The part-worth for review (which enables an individual to correct errors in his/her personal information) is 1.7867 and significant. This indicates that a Website that has a policy of allowing review raises its ranking by 1.7867 (out of 18). The part-worth for restrictions against improper access is 3.3736 and significant, while the part-worth for disallowing secondary use is 4.6046 and significant. These results are consistent with the previous literature on privacy concerns.

Interestingly, Table 1 shows that each of the two economic benefits (within the levels investigated) are relatively less important than any of the three privacy concerns. Using the marginal utilities and the part-worths for the concerns, we can estimate the value of each of the privacy concerns. For instance, taking the marginal utility of monetary reward to be 0.0925 per dollar, the value of disallowing secondary use is  $4.6046/0.0925 = \$49.78$ . With the marginal utility of monetary reward as 0.1156 per dollar, the value of disallowing secondary use is  $4.6046/0.1156 = \$39.83$ . In the same way, we can calculate the other values in Table 2.

Our results in Table 2 suggest that Websites need to offer quite substantial monetary incentives to overcome individual concerns over errors, improper access, and secondary use of information.

We tested hypotheses H2(a) through (d) by regressing the estimated part-worths on respondents' personal characteristics. Table 3 presents the results.

**Table 3. Personal Characteristics**

Hypothesis	Personal Characteristic	Effect on Part-Worth				
		Monetary Reward	Visit Frequency	Error	Improper Access	Secondary Use
H2(a)	Gender	No	Higher for females*	No	No	No
H2(b)	Cookie Knowledge	Increases**	No	No	No	No
	Knowledge of Anonymous Web Surfing	No	No	No	No	No
H2(c)	Individualism	No	No	No	No	No
H2(d)	Trust Propensity	No	No	No	No	No

\*Significant at 10%

\*\*Significant at 5%

Females have higher part-worths for visit frequency, but the coefficient is only marginally significant (at the 90 percent level). Gender has no significant effect on the other part-worths. We infer that individuals' preferences do not depend on gender, and H2(a) is not rejected.

With regard to contextual knowledge, only cookie knowledge has an effect, and the effect increases the part-worth of monetary reward. Contextual knowledge does not have a significant effect on the other dimensions. We infer that H2(b) is not rejected.

The degree of individualism also has no significant effect on any of the part-worths. Apparently, whether a person is individualistic or collectivistic does not affect his/her cost-benefit trade-off over information privacy. H2(c) is not rejected. Finally, trust propensity also has no significant effect on any of the part-worths, and hence, H2(d) is not rejected.

Overall, the part-worths of both economic benefits and privacy concerns do not appear to vary significantly with differences in personal characteristics.

## 6 LIMITATIONS

Our study is subject to several limitations. First, the subjects are undergraduate students who might have had limited experience of invasion of privacy and its possible consequences. Hence, they might not have a good understanding the implications of providing personal information to Websites. This limits the generalizability of the findings, especially those associated with the concern dimensions.

Our result with respect to monetary reward might be sensitive to the levels of rewards. In particular, we find that the effect of a reward was subject to a threshold: whereas a \$10 reward had no significant effect, a \$20 reward did. An important direction for further research is to investigate the effect of larger rewards such as \$30 and \$40, and to determine the marginal utility of rewards over these ranges. Any resulting changes in the estimated marginal utility of rewards might affect the estimated value of privacy as reported in Table 2.

The use of visit frequency may not truly reflect the time saving aspect of economic reward. For some individuals, the frequency of visits to a particular Website may depend on factors such as the inherent value of the Website or the formation of a long-term relationship. Further, subjects might have related the visit frequency to conventional retailing where information is not stored or shared with others. In that case, the subjects may feel that providing information to an infrequently visited store is not costly, as the retailer may have little opportunity to use/abuse the information. Future research should devise more complete measures of the convenience factor.

Methodologically, because we use an orthogonal array of stimuli, we cannot estimate any possible interaction between the dimensions under study. For instance, it is possible for economic rewards to be particularly salient when privacy protection procedures are present.

## 7 CONCLUDING REMARKS

Ours is the first study to estimate the dollar value of privacy concerns, and hence the first to estimate the value of privacy regulation. Recall that the cost to industry of complying with proposed privacy legislation has been estimated to be U.S. \$9 billion to \$36 billion (Hahn 2001). Referring to Table 2, our lower estimate of the value of the combination of review for error, restrictions against improper access, and no secondary use ranged from \$84.47 to \$105.57, or U.S. \$45.61 to \$57.01.

In March 2001, an estimated 58 million Americans made a purchase over the Internet, while 100 million used e-mail (Horrigan and Rainie 2002). Based on the number of purchasers, we conservatively estimate the benefit from privacy legislation to be U.S. \$2.65 billion to \$3.31 billion, which falls quite far short of Hahn's (2001) cost estimates.<sup>8</sup> Of course, with growing consumer

---

<sup>8</sup>If each person values privacy at U.S. \$45.61, then 58 million people would value privacy at a total of  $58 \times 45.61 =$  U.S. \$2,645 million or approximately U.S. \$ 2.65 billion. Similarly, if we use the higher estimate of the value of privacy (U.S. \$57.01), the value of privacy to the entire population is U.S.\$3.31 billion.

A limitation of these calculations is that we assume the value of privacy to be the same among the Singapore subjects and American consumers.

participation in Internet commerce, the benefit of privacy legislation increases proportionately. Based on the number of e-mail users, a more aggressive estimate of benefit would be U.S. \$4.56 billion to \$5.70 billion, which is still less than Hahn's cost estimates.

Our results show that that individuals' concern for privacy is not absolute, but rather that they are willing to trade off privacy concerns for economic benefits. These results imply that proposals (Laudon 1996; Varian 1997) to regulate privacy through markets are viable.

Among the concern dimensions, we find that the respondents value improper access and secondary use to be more important than possible errors. These results are consistent with previous research that did not use conjoint analysis, but are based purely on comparing numerical ratings (Esrock and Ferre 1999; Milberg et al. 1995). Using the conjoint method, we not only confirm the relative significance of the three concern dimensions, but also identify the possible managerial devices to overcome such concerns. These results complement those of Culnan and Armstrong (1999), who suggested that privacy concerns can be mitigated through fair information procedures.

The outstanding puzzle is why differences in personal characteristics—gender, prior contextual knowledge, degree of individualism, and trust propensity—appear to have no significant effect on the respondents' part-worths for both economic and concern dimensions. One possible explanation is that there is not sufficient variation in personal characteristics among our respondents, being all undergraduate students in an e-commerce course studying in an Asian culture. In particular, the limited sample variation might have obscured the influences of culture and trust propensity. Future work should apply the conjoint approach to a more varied pool of subjects.

In any event, our results suggest that Websites collecting personal information may not be able to segment markets based on demographics. This observation applies especially to economic incentives (monetary reward and convenience) that Websites can manipulate most directly.

## 8 REFERENCES

- Addelman, S. "Orthogonal Main-Effect Plans for Asymmetrical Factorial Experiments," *Technometrics* (4:1), February 1962, pp. 21-46.
- Archer, R. L. "Role of Personality and the Social Situation," in G. J. Chelune and Associates (eds.), *Self-Disclosure: Origins, Patterns, and Implications of Openness in Interpersonal Relations*. San Francisco: Jossey Bass, 1979.
- Cozby, P. C. "Self-Disclosure: A Literature Review," *Psychological Bulletin* (79:2), February 1973, pp. 73-91.
- Cranor, L. F., Reagle, J., and Ackerman, M. S. "Beyond Concern: Understanding Net Users' Attitudes About Online Privacy," *AT&T Labs-Research Technical Report TR 99.4.3*, 1999 (<http://www.research.att.com/library/trs/TRs/99/99.4/>).
- Culnan, M. J. "How Did They Get My Name? An Exploratory Investigation of Consumer Attitudes Toward Secondary Information Use," *MIS Quarterly* (17:3), September 1993, pp. 341-363.
- Culnan, M. J., and Armstrong, P. K. "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation," *Organization Science* (10:1), January-February 1999, pp. 104-115.
- Culnan, M. J., and Milne, G. R. "The Culnan-Milne Survey on Consumers and Online Privacy Notices: Summary of Responses," December 2001 (<http://www.ftc.gov/bcp/workshops/glb/supporting/culnan-milne.pdf>).
- Eddy, E. R., Stone, D. L., and Stone-Romero, E. F. "The Effects of Information Management Policies on Reactions to Human Resource Information Systems: An Integration of Privacy and Procedural Justice Perspectives," *Personnel Psychology* (52:2), 1999, pp. 335-358.
- Esrock, S. L., and Ferre, J. P. "A Dichotomy of Privacy: Personal and Professional Attitudes of Marketers," *Business and Society Review* (104:1), Spring 1999, pp. 107-120.
- Fletcher, C., and Spencer, A. "Sex of Candidate and Sex of Interviewer as Determinants of Self-Preservation Orientation in Interviews: An Experimental Study," *International Review of Applied Psychology* (33), 1984, pp. 305-313.
- Foddy, W. H., and Finighan, W. R. "The Concept of Privacy from a Symbolic Interaction Perspective," *Journal for the Theory of Social Behavior* (10), 1981, pp. 1-17.
- Fox, S. "Trust and Privacy Online: Why Americans Want to Rewrite the Rules," August 2000.
- Fusilier, M. R., and Hoyer, W. D. "Variables Affecting Perceptions of Invasion of Privacy in a Personnel Selection Situation," *Journal of Applied Psychology* (65:5), 1980, pp. 623-626.
- Goodwin, C. "Privacy: Recognition of a Consumer Right," *Journal of Public Policy and Marketing* (10:1), Spring 1991, pp. 149-166.



- Green, P. E., and Srinivasan, V. "Conjoint Analysis in Marketing: New Developments with Implications for Research and Practice," *Journal of Marketing* (54:4), October 1990, pp. 3-19.
- Hahn, R. "An Assessment of the Costs of Proposed Online Privacy Legislation," Working Paper, AEI-Brookings Joint Center for Regulatory Studies, May 2001.
- Harper, J., and Singleton, S. "With a Grain of Salt: What Consumer Privacy Surveys Don't Tell Us," Competitive Enterprise Institute, June 2001.
- Hoffman, D. L., Novak, T. P., and Peralta, M. A. "Building Consumer Trust Online," *Communications of the ACM* (42:4), April 1999, pp. 80-85.
- Hofstede, G. H. *Cultures and Organizations: Software of the Mind*. New York: McGraw-Hill, 1991.
- Horrigan, J. B., and Rainie, L. "Getting Serious Online," Pew Internet & American Life Project, Washington, DC, March 2002.
- Katz, J. E., and Tassone, A. R. "Public Opinion Trends: Privacy and Information Technology," *Public Opinion Quarterly* (54), 1990, pp. 125-143.
- Laudon, K. C. "Markets and Privacy," *Communications of the ACM* (39:9), 1996, pp. 92-104.
- Mael, F. A., Connerley, M., and Morath, R. A. "None of Your Business: Parameters of Biodata Invasiveness," *Personnel Psychology* (49:3), Autumn 1996, pp. 613-650.
- Marshall, N. J. "Dimensions of Privacy Preferences," *Multivariate Behavioral Research* (9), 1974, pp. 255-272.
- Michael, G. B. "Trust, Distrust, and Interpersonal Problems: A Circumplex Analysis," *Journal of Personality and Social Psychology* (62:6), 1992, pp. 989-1002.
- Milberg, S. J., Smith, H. J., and Burke, S. J. "Information Privacy: Corporate Management and National Regulation," *Organization Science* (11:1), January-February 2000, pp. 35-57.
- Milne, G. R. "Privacy and Ethical Issues in Database/Interactive Marketing and Public Policy: A Research Framework and Overview of the Special Issue," *Journal of Public Policy and Marketing* (19:1), Spring 2000, pp. 1-6.
- Milne, G. R., and Gordon, M. E. "Direct Mail Privacy-Efficiency Trade-offs Within an Implied Social Contract," *Journal of Public Policy and Marketing* (12:2), Fall 1993, pp. 206-215.
- Nowak, G. J., and Phelps, J. "Direct Marketing and the Use of Individual-Level Consumer Information: Determining how and when Privacy Matters," *Journal of Direct Marketing* (11:4), Fall 1997, pp. 94-109.
- Oberndorf, S. "Registering for Success," *Catalog Age* (16:13), December 1999, pp. 47-48.
- OECD. *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (Privacy Guidelines), September 23, 1980 (<http://www1.oecd.org/dsti/sti/it/secur/prod/privacyguide.htm>).
- Pedersen, D. M. "Sex Differences in Privacy Preferences," *Perceptual and Motor Skills* (48), 1987, pp. 1239-1242.
- Phelps, J., Nowak, G., and Ferrell, E. "Privacy Concerns and Consumer Willingness to Provide Personal Information," *Journal of Public Policy and Marketing* (19:1), Spring 2000, pp. 27-41.
- Posner, R. A. "The Economics of Privacy," *American Economic Review: Papers and Proceedings* (71:2), May 1981, pp. 405-409.
- Russell, C. "Kiss and Tell," *American Demographics* (11:12), December 1989, p. 2.
- Schwartz, P. M. "Beyond Lessig's CODE for Internet Privacy: Cyberspace Filters, Privacy-Control, and Fair Information Practices," *Wisconsin Law Review* (4), 2000, pp. 743-788.
- Schwartz, S. "It's Privacy, Stupid," *Intelligent Enterprise* (3:6), April 2000, pp. 10-12.
- Simitis, S. "Reviewing Privacy in an Information Society," *University of Pennsylvania Law Review* (135), 1987, pp. 707-746.
- Smith, H. J. "Information Privacy and Marketing: What the U.S. Should (and Shouldn't) Learn from Europe," *California Management Review* (43:2), Winter 2001, pp. 8-33.
- Smith, H. J., Milberg, S. J., and Burke, S. J. "Information Privacy: Measuring Individuals' Concerns About Organizational Practices," *MIS Quarterly* (20:2), June 1996, pp. 167-196.
- Stewart, K. A., and Segars, A. H. "An Empirical Examination of the Concern for Information Privacy Instrument," *Information Systems Research* (13:1), March 2002, pp. 36-49.
- Stigler, G. J. "An Introduction to Privacy in Economics and Politics," *Journal of Legal Studies* (9:4), 1980, pp. 623-644.
- Stone, E. F., Gueutal, H. G., Gardner, D. G., and McClure, S. "A Field Experiment Comparing Information-Privacy Values, Beliefs, and Attitudes Across Several Types of Organizations," *Journal of Applied Psychology* (68:3), 1983, pp. 459-468.
- Stone, E. F., and Stone, D. L. "Privacy in Organizations: Theoretical Issues, Research Findings, and Protection Mechanisms," *Research in Personnel and Human Resources Management* (8), 1990, pp. 349-411.
- Tolchinsky, P. D., McCuddy, M. K., Adams, J., Ganster, D. C., Woodman, R. W., and Fromkin, H. L. "Employee Perceptions of Invasion of Privacy: A Field Simulation Experiment," *Journal of Applied Psychology* (66:3), 1981, pp. 308-313.
- Triandis, H.C. "Individualism and Collectivism: Cross-Cultural Perspectives on Self-ingroup Relationships," *Journal of Personality and Social Psychology* (54), 1988, pp. 323-338.
- U.S. Public Interest Research Group. "Public Comment on Barriers to Electronic Commerce," Response to call by U.S. Department of Commerce (65 Federal Register 15898), April 25, 2000.

- Varian, H. "Economic Aspects of Personal Privacy," in U.S. Department of Commerce, *Privacy and Self-Regulation in the Information Age*, June 1997.
- Wang, H., Lee, M. K. O., and Wang, C. "Consumer Privacy Concerns about Internet Marketing," *Communications of the ACM* (41:3), March 1998, pp. 63-70.
- Westin, A. "Opinion Surveys: What Consumers Have To Say About Information Privacy," Testimony before U.S. House of Representatives, Committee on Energy and Commerce, Subcommittee on Commerce, Trade, and Consumer Protection, May 8, 2001.
- Westin, A. F. *Privacy and Freedom*. New York: Atheneum, 1967.
- Woodman, R. W., Ganster, D. C., Adams, J., McCuddy, M. K., Tolchinsky, P. D., and Fromkin, H. "A Survey of Employee Perceptions of Information Privacy in Organizations," *Academy of Management Journal* (25:3), 1982, pp. 647-663.