International Differences in Information Privacy Concerns: A Global Survey of Consumers

Steven Bellman

Graduate School of Management, University of Western Australia, Crawley, Western Australia, Australia

Eric J. Johnson

Department of Marketing, Columbia School of Business, Columbia University, New York, New York, USA

Stephen J. Kobrin

Joseph H. Lauder Institute of Management and International Studies, University of Pennsylvania, Philadelphia, Pennsylvania, USA

Gerald L. Lohse

Accenture, Philadelphia, Pennsylvania, USA

We examine three possible explanations for differences in Internet privacy concerns revealed by national regulation: (1) These differences reflect and are related to differences in cultural values described by other research; (2) these differences reflect differences in Internet experience; or (3) they reflect differences in the desires of political institutions without reflecting underlying differences in privacy preferences. Using a sample of Internet users from 38 countries matched against the Internet population of the United States, we find support for (1) and (2), suggesting the need for localized privacy policies. Privacy concerns decline with Internet experience. Controlling for experience, cultural values were associated with differences in privacy concerns. These cultural differences are mediated by regulatory differences, although new cultural differences emerge when differences in regulation are harmonized. Differences in regulation reflect but also shape country differences. Consumers in countries with sectoral regulation have less desire for more privacy regulation.

This research was funded by the Columbia Center for E-Business (cebiz.org) and the member companies of the Wharton Forum on Electronic Commerce.

Address correspondence to Steven Bellman, Senior Lecturer, Graduate School of Management, University of Western Australia, 35 Stirling Highway, Crawley, WA 6009, Australia. E-mail: sbellman@gsm.uwa.edu.au

Increasingly, companies are reaching out across borders to access international markets (Taylor & Fosler, 1994). Transborder information flows are the "lifeblood" of these markets, and the Internet has expedited these flows by enabling massive amounts of information about customers to be transferred instantly across borders (Nijhawan, 2003). However, differences in culture and national regulation create challenges for global information management strategies, sometimes limiting or even preventing the free flow of valuable information (Fjetland, 2002).

Differences in information privacy concerns in relation to the Internet have been found in national probability samples of consumers from the United States, the United Kingdom, and Germany (IBM, 1999). International differences in regulation of information privacy (e.g., the European Union's Data Privacy Directive vs. the industry self-regulation approach favored by the United States) are

supposed to reflect these concerns. However, some countries (notably Canada, Australia, and New Zealand) have adopted new privacy regulation expressly in order to continue trading with the European Union (EU) (Long & Quek, 2002), and this new regulation may have little relationship with the privacy preferences of consumers in those countries.

In this study, we examine three possible explanations for different forms of Internet privacy regulation: (1) These differences reflect and are related to differences in cultural values (Hofstede, 1980, 1991; Milberg et al., 1995); (2) these differences reflect differences in Internet experience and therefore familiarity with Web privacy practices; or (3) they reflect differences in the desires of political institutions without reflecting underlying differences in privacy preferences. In this study, we surveyed Internet-using consumers from 38 countries on concerns about information privacy on the Net, while controlling for differences in demographics (Poortinga & Malpass, 1986) to isolate the effects of cultural values, privacy regulation, and Internet experience. We find support for (1) and (2): that privacy regulation preferences reflect differences in cultural values and Internet experience, but are also shaped by the prevailing regulatory regime. This means that country differences in regulatory practices are not disconnected from, or imposed artificially on, the privacy preferences of consumers. It also means that companies collecting data from international consumers should adapt their data protection policies to local differences in the privacy preferences of consumers, and that readily observable differences in national regulation account for most of these differences.

CONCEPTUAL FRAMEWORK AND HYPOTHESES

Information Privacy and Fair Information Principles

Our study focuses on information privacy, defined by Westin (1967) as the amount of control that individuals can exert over the type of information, and the extent of that information, revealed to others. Marketing communications and data collection can be intrusive; marketers can appropriate consumer information surreptitiously or without giving consumers control over its use; and marketers can disclose embarrassing facts about consumers, or make use of false or inaccurate information (Nowak & Phelps, 1997). The ability of Web sites to collect information unobtrusively has heightened concern about the privacy of personal information. For example, in 2003, only a quarter (27%) of U.S. consumers had a "high level of trust" in how Web sites protect personal data (Consumer Internet Barometer, 2003). A multinational poll in 1999 found that 80% of consumers in the United States, 79% in Germany, and 68% in the United Kingdom agreed that "consumers have lost all control over how personal information is collected and used by companies" (IBM, 1999). In Canada too, concern about information privacy has been rising, with 92% of Canadians at least "moderately" concerned (Campbell, 1997).

This high level of concern about information privacy has been reflected in new privacy legislation in several countries. Differences between local information privacy regulation regimes could potentially disrupt international trade. However, *fair information principles* (FIPs) (U.S. Department of Health, Education, and Welfare, 1973) can provide an internationally agreed basis for balancing the concerns of consumers with the need for businesses to gather and use personal information about their customers. FIPs help reduce privacy concerns by giving people control over their personal information. The Organization for Economic Cooperation and Development's *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (OECD, 2002) list eight basic FIPs (collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability) that are reflected in the regulations of many countries, although there are differences in implementation. In the European Union (EU), the 1995 Data Protection Directive (EU, 1995), based on the OECD guidelines, has served to harmonize privacy regulation among its member countries. However, Articles 25 and 26 of the directive prohibit the transfer of personal data collected from EU citizens to countries that do not have privacy protection as adequate as what the directive provides. Some countries, such as Australia and Canada, have enacted omnibus data protection laws similar to the EU directive to allow such transfers (Long & Quek, 2002). In contrast, the United States has maintained a sectoral and self-regulatory approach to privacy legislation, and a "safe harbor" agreement between the United States and the EU was negotiated as an alternative to omnibus legislation (EU, 2000). Self-certifying that it will adhere to the "Safe Harbor" Privacy Principles (U.S. Department of Commerce, 2004) is one way that a U.S. company can enable the transfer of personal data from EU residents for subsequent processing (other alternatives include the use of model contracts for data transfer, or avoiding transborder transfer and processing data in Europe).

The seven Safe Harbor Privacy Principles (see U.S. Department of Commerce, 2000) are another example of FIPs. They are: (1) open or readily available *notice* of the purpose of data collection and use; (2) the *choice* of being able to withdraw consent (opt-out, for an affordable cost) to transfer of data, or its use for an incompatible secondary purpose, and to give explicit consent (opt-in) before the transfer or incompatible use of sensitive data; (3) the application of the notice and choice principles before any *onward transfer* of the data, which is only possible

to organizations that subscribe to all the other Safe Harbor Principles; (4) individual participation in the form of *access* to their data by individuals whose data have been collected, "except where the burden or expense" of access would be out of proportion to the risks to that individual, or access would violate the rights of other individuals; (5) reasonable *security* precautions against "loss, misuse, unauthorized access, disclosure, alteration and destruction"; (6) *data integrity* in terms of compatible use, accuracy and quality; and (7) accountability of data controllers maintained by *enforcement* of the safe harbor regulations. A general recommendation would be that it is in a company's economic interest to apply FIPs to its data practices for two reasons: (1) Adhering to FIPs such as the Safe Harbor Principles will allow the transfer of valuable data from the EU to the United States (or any other country); and (2) FIPs build consumer trust and therefore greater willingness to disclose valuable data (Culnan & Bies, 1999; Smith, 2001). However, managers need guidance on exactly how to apply these principles in practice, when the importance or interpretation of these principles may differ across countries (Milberg et al., 2000). The cost of allowing, for example, access to information by consumers from all countries of the world (Walker, 2001) also suggests the need for research to understand whether companies should adopt these principles now, or continue to adopt a wait-and-see attitude, in the hope that these principles reflect temporary political solutions rather than the enduring privacy preferences of consumers. We investigate, in this research, whether the online privacy concerns of consumers around the world are associated with relatively unchanging cultural values or with more amenable differences in privacy regulation. Cultural differences in privacy preferences would be very stable and demand localized data collection practices, perhaps more restrictive than the Safe Harbor Principles. On the other hand, if consumers in highly regulated countries would be equally trusting of companies collecting their personal data under less restrictive privacy regulation, companies may eventually be able to adopt FIPs that are less restrictive than the EU Directive or the Safe Harbor Principles.

Cultural Values

Cultural values are a set of strongly held beliefs that guide attitudes and behavior and that tend to endure even when other differences between countries are eroded by changes in economics, politics, technology, and other external pressures (Hofstede, 1980; Long & Quek, 2002). Milberg et al. (2000) used a formative index to combine four of Hofstede's (1980, 1991) cultural values indices, *Power Distance Index* (PDI), *Individualism* (IND), *Masculinity* (MAS), and *Uncertainty Avoidance Index* (UAI), into an overall measure of cultural values, which they found had a significant and positive effect on information privacy concerns across countries. The regression weights for the four indicators demonstrated that concerns about information privacy were positively associated with PDI, IND, and MAS, and negatively associated with UAI. Milberg et al. (1995, 2000) explained these correlations in the following way. Although high Power Distance Index (PDI) cultures tolerate greater levels of inequality in power, higher scores are associated with greater mistrust of more powerful groups, such as companies. Low Individualism (IND), or collectivist, societies have a greater acceptance that groups, including organizations, can intrude on the private life of the individual. High Masculinity (MAS) cultures place greater emphasis on achievement and material success, and perhaps the economic benefits of using private information, over caring relationships and quality of life. Finally, societies with a high Uncertainty Avoidance Index (UAI) tend to reduce uncertainty by embracing clear written rules and regulations, and may be more likely to introduce higher levels of government regulation of privacy.

> H1: Cultural values will be associated with differences in concerns about information privacy.

Government Involvement in Regulation

There is a general consensus that government involvement in the regulation of information privacy is associated with the level of privacy concern in a country (Bennett, 1992; Smith, 1994). In the United States and, until recently, Canada and Australia, privacy regulation has tended to be targeted or sector specific, and to be aimed mainly at the public sector. This *sectoral* or voluntary approach contrasts with the *omnibus* approach, to both the public and private sectors, used by the European Union. Milberg et al. (1995, 2000) found a significant and positive relationship between concerns about information privacy and the level of government involvement in the regulation of privacy. If the level of regulation in different countries reflects the concerns of consumers in those countries, we should find that higher levels of government involvement in the regulation of corporate privacy management would be associated with higher levels of privacy concerns:

> H2: Consumers from countries with an omnibus privacy regulatory structure will have higher levels of privacy concerns compared to consumers from countries with sectoral privacy regulation or no privacy regulation.

Consumers with equal concerns about information privacy may prefer different levels of government regulation to solve these problems. Milberg et al. (2000) found a positive relationship between existing government involvement in regulation and preference for more government regulation. Their explanation was that status quo bias (e.g.,

Bellman et al., 2001; Johnson et al., 2002; Kahneman & Tversky, 1984; Samuelson & Zeckhauser, 1988) would favor further government regulation if that were the prevailing solution. Alternatively, government regulation may be a trailing indicator of privacy concerns.

> H3: Higher levels of current government involvement in the regulation of corporate privacy management will be associated with a greater preference for even stronger laws to regulate information privacy.

Internet Experience

Besides cultural values and government regulation, another influence on information privacy concern is likely to be familiarity with relationship marketing practices and ways of controlling the use of personal information. For example, Culnan (1995) found that consumers who were aware of name removal procedures for "opting out" of direct mailing lists were less concerned about information privacy. The need for more consumer education is a typical recommendation in the conclusion of academic studies (e.g., Culnan, 1995; Whitman et al., 2001). Recently, industry groups in the United States such as TRUSTe (Benassi, 1999) have been spending millions of dollars on education programs to try to reduce consumers' privacy concerns and demands for increased government regulation. Familiarity with online privacy practices should grow with experience at using the Internet.[1] Lohse et al. (2000), using a sample of U.S. consumers, found that sensitivity to privacy issues online decreased with Internet experience. We expect to find a similar relationship between Internet experience and privacy concerns around the world:

> H4: Participants with more Internet experience will exhibit lower levels of concern about the privacy of their personal information.

METHODS

Sampling

We recruited participants to our privacy survey using email invitations and a banner ad campaign (heavily focused on European sites). We eliminated participants from countries for which Hofstede (1980, 1991) has not reported cultural values indices (e.g., Iceland, Luxembourg, Russia, Sri Lanka), or who had not completed an online panel signup survey, containing 88 demographics, Internet usage, and privacy concern items. Our final sample consisted of 534 valid responses from 38 countries. Less than half of the participants (37%) were females, the mean age was 32.7 years, the mean education level was 4.5 (between "some college" and "college graduate"), and the mean level of Internet experience was 27 months. Only 23% were full-time students. The U.S sample contained more men, and was slightly more educated, compared to U.S. panelists in general (who were representative of the U.S. Internet population), but had identical levels of privacy concern. U.S. panelists, both participants in the survey and nonparticipants, had the same level of concern about third parties monitoring their online transactions, and were equally likely to give their name, e-mail address, and telephone number to a Web site. Compared to the U.S. participants, International participants had identical Internet experience and demographics, with the exception of being slightly younger.

Survey Items

Concern for Information Privacy. Smith et al. (1996) reviewed the various aspects of information privacy concerns and found that four dimensions summarize these concerns. *Collection* reflects the growing impression, matched by increasing technological capabilities for surveillance, that companies are getting more intrusive and collecting unreasonable amounts of personal data. *Unauthorized secondary use* refers to the reuse of information collected for one purpose, without implied or explicit permission, either by the collecting company or another company. *Improper access* reflects lapses in the integrity and security of information systems that allow the disclosure of personal information to unauthorized individuals. Finally, the *Errors* dimension describes concerns about databases containing inaccurate personal information that portrays consumers in a false light, either by accident or design. These four dimensions, however, combine to form a single factor that reflects overall information privacy concerns, or *concern for information privacy* (CFIP; Stewart & Segars, 2002). The 15 items, based on the scale developed by Smith et al. (1996), were slightly modified to reflect online privacy rather than information privacy in general (Table 1). Seven-point Likert scales (1 = "strongly disagree" to 7 = "strongly agree") were used with a "no opinion" option so that responses were not forced.

A two-group confirmatory factor analysis comparing the U.S. sample with a sample of international consumers matched on demographics and Internet usage ($n = 140$) indicated that the CFIP items were interpreted equivalently in the United States and internationally (Meredith, 1993). A four-factor solution with a single higher order factor, concern for information privacy (Stewart & Segars, 2002), had fit indices above .90 (Bentler & Bonett, 1980) and root mean square residual (RMR) less than .09 (Bagozzi & Yi, 1989) in both samples. Construct reliability (CR) and average variance extracted (AVE) for all four factors and the higher order factor (CFIP) were close to, or above, their acceptable criteria, .70 for CR (Nunally, 1978) and .50 for AVE (Fornell & Larcker, 1981).

TABLE 1
Concern for information privacy scale items

Privacy scale factors and individual scale items (1 strongly disagree–7 strongly agree)	U.S. matched sample ($n = 195$) Factor loading	U.S. matched sample ($n = 195$) Mean (SD)	International matched sample ($n = 140$) Factor loading	International matched sample ($n = 140$) Mean (SD)
Collection	.55	5.22 (1.06)	.61	5.36 (1.06)
1. It usually bothers me when Web sites ask me for personal information.	.63	4.83 (1.32)	.70	4.87 (1.43)
2. When Web sites ask me for personal information, I sometimes think twice before providing it.	.53	5.93 (1.17)	.54	6.05 (1.01)
3. It bothers me to give personal information to so many Web sites.	.91	5.14 (1.39)	.86	5.36 (1.39)
4. I'm concerned that Web sites are collecting too much personal information about me.	.86	4.94 (1.37)	.85	5.12 (1.38)
Improper access	.95	5.95 (1.00)	.72	6.25 (.93)*
1. Web sites should devote more time and effort to preventing illegal access to personal information.	.62	5.87 (1.22)	.54	6.12 (1.28)
2. Databases that contain personal information should be protected from illegal access—no matter how much it costs.	.76	5.88 (1.36)	.60	6.17 (1.34)*
3. Web sites and other companies should take more steps to make sure that hackers cannot access the personal information in their computers.[a]	.72	6.04 (1.19)	.81	6.40 (1.07)**
Errors	.56	4.73 (1.10)	.61	5.10 (1.16)**
1. All the information received on Web sites should be double-checked for accuracy—no matter how much this costs.	.62	4.32 (1.54)	.70	4.76 (1.68)**
2. Web sites should take more steps to make sure that the personal information in their files is accurate.	.66	4.96 (1.20)	.84	5.29 (1.25)**
3. Web sites should have better procedures to correct errors in personal information.	.86	4.85 (1.37)	.81	5.24 (1.39)*
4. Web sites should devote more time and effort to verifying the accuracy of the personal information in their databases.	.89	4.79 (1.33)	.77	5.05 (1.28)
Unauthorized secondary use	.77	6.01 (1.16)	.66	6.50 (.75)***
1. Web sites should not use personal information for any purpose unless it has been authorized by the individuals who provide the information.	.74	6.30 (1.24)	.62	6.51 (1.07)
2. When people give personal information to a Web site for some reason, the Web site should never use the information for any other reason.	.73	5.81 (1.51)	.73	6.32 (1.16)***
3. Web sites should never sell the personal information they have collected to other Web sites.	.78	5.69 (1.68)	.62	6.37 (1.19)***
4. Web sites should never share personal information with other Web sites or companies unless it has been authorized by the individuals who provided the information.	.79	6.25 (1.25)	.75	6.63 (.72)**

Note. All items have been modified compared to the original scale items by the substitution of "Web site" for "company." Significance: $^{***}p < .001$; $^{**}p < .01$; $^{*}p < .05$.
[a] "Hackers" substituted for "unauthorized people."

The international sample tended to rate many of the scale items, and therefore the CFIP subscales, significantly higher than the U.S. sample (Table 1). However, the ranking of the subscales in descending order of concern was identical in both samples (secondary use ranked first, errors ranked last). Differences between our rankings and those in the Milberg et al. (1995) sample were insignificant.

Concern about Transaction Security on the Internet. The Smith et al. (1996) scale asks questions about the

security of personal data already stored in databases. However, data could also be stolen while in transit over the Internet. We asked our participants: "How concerned are you, in general, with the security of the transactions you do on the Net?" (1 = "not concerned at all" to 7 = "extremely concerned"). The lower correlation between this item and CFIP among international respondents (.30 vs. .51 for U.S. participants) suggested that this item measured concern about data security not tapped by the CFIP scale.

Desire for More Regulation. Two scenarios compared privacy concerns in two contexts widely separated on a continuum of low versus high sensitivity of both information and collection environment. The first scenario described the use of a bonus card loyalty program that allowed a physical retail store to associate purchases with an individual consumer, to facilitate customized offers. Using a 7-point scale, panelists were then asked their level of agreement with the statement: "Bonus cards should be regulated by the government to ensure that my privacy is respected." In the second scenario, a life-insurance broker collected income and health information over the Web. After this scenario, panelists rated their agreement with the statement: "Government regulation is needed to ensure the confidentiality of medical and financial information on the Web." We averaged responses to these two questions to create an index of desire for more regulation of information privacy (U.S. Cronbach's $\alpha = .65$, international $\alpha = .64$). Order of presentation was counterbalanced across participants to control for possible order effects.

Information Privacy Regulatory Approaches. We consulted Privacy International's (1998) survey of privacy and human rights to update 19 country classifications by Milberg et al. (2000), and to classify 19 additional countries. We used just three levels of regulation instead of the six used by Milberg et al. (2000): *no regulation* (or *self help*), *sectoral*, and *omnibus*, compressing three categories of omnibus regulation defined by Milberg et al. (1995) into one category, as they are unlikely to appear different to consumers. The classifications for the 38 countries in our sample are listed in Table 2.

Cultural values: In our sample of 38 countries, PDI ranged from 11 in Austria to 104 in Malaysia, IND ranged from 6 in Guatemala to 91 in the United States, MAS ranged from 5 in Sweden to 95 in Japan, and UAI ranged from 8 in Singapore to 112 in Greece.

TABLE 2
Privacy regulation in 38 countries

Regulation	Countries
None or self-help	Argentina, Brazil, China, Guatemala, India, Malaysia, Mauritius, Mexico, Pakistan, Philippines, Singapore, Turkey, United Arab Emirates, Venezuela
Sectoral	Japan, United States
Omnibus	Australia, Austria, Belgium, Canada, Denmark, Finland, Germany, Greece, Hong Kong, Hungary, Ireland, Israel, Italy, Netherlands, New Zealand, Norway, Poland, Portugal, Spain, Sweden, Switzerland, United Kingdom

Note. From Privacy International (1998).

RESULTS

We used a multivariate analysis of covariance (MANCOVA) to test the significance of the independent variables—cultural values, regulatory structure (no regulation, sectoral, and omnibus), and Internet experience—on a set of dependent variables examining privacy and security concerns, and desire for more privacy regulation. The covariates controlled for demographics (age, gender, and level of education) and order of presentation (privacy scale items first or questions about the need for more regulation first) in every analysis. We found significant multivariate effects for regulatory structure and Internet experience, providing support for H3 and H4, but not for H2. We did not find consistent support for H1, the effect of cultural values.

We used three different methods to analyze the effects of cultural values: (1) analyzing each Hofstede index separately; (2) analyzing the simultaneous effects of four Hofstede indices; and (3) analyzing the discrete effects of being high or low on the four Hofstede indices. Analyzed separately, controlling for Internet experience, demographics, and order of presentation, there were significant multivariate effects of the cultural values indices for power distance (PDI) and individualism (IND).[2] However, in our data PDI and IND are very highly correlated ($r = -.54$, Table 3). The model including all four indices simultaneously isolated the unique effects of each index (Lynn et al., 1993). In this model, only IND has a significant multivariate effect (Wilk's $\Lambda = .95$, $F(6,441) = 3.48$, $p = .002$). All these models assumed that the Hofstede indices were continuous integer-level variables. To examine the ordinal-level effect of a culture being either high or low on a Hofstede index, we split our sample at the median country score for each index. For each index, the high group had significantly higher country scores than the low group (t-test p values all $<.001$), as is the case in experimental studies comparing culture across countries (e.g., Tan et al., 1998). When these dichotomized Hofstede

TABLE 3
Correlations between cultural values indices and privacy concerns

	PDI	IND	MAS	UAI	CFIP	Desire for more regulation	Security of online transactions
PDI	—				.02	.05	.08
IND	−.54***	—			−.03	−.16***	−.14**
MAS	.13**	.25***	—		.03	−.03	.03
UAI	.18***	−.43***	.13**	—	.03	.04	.06
Regulation	−.57***	.11**	−.32***	−.01	.10*	.18***	−.00

Note. PDI = Power Distance Index, IND = Individualism, MAS = Masculinity, UAI = Uncertainty Avoidance Index, CFIP = Concern for Information Privacy, Regulation = privacy regulation (0 = none, 1 = sectoral, 2 = omnibus). Significance: *** $p < .001$; ** $p < .01$; * $p < .05$.

indices were analyzed simultaneously, there were significant multivariate effects for three of the four indices: PDI (Wilk's $\Lambda = .94$, $F(6,441) = 4.39$, $p < .001$), IND (Wilk's $\Lambda = .96$, $F(6,441) = 2.77$, $p = .012$), and UAI (Wilk's $\Lambda = .97$, $F(6,441) = 2.50$, $p = .022$). Table 4 lists the least-squares means (and standard errors) from this dichotomized model. These least-squares means are the unique effect of each variable, controlling for all the other effects in the model.

Although these analyses indicated a zero-order effect of cultural values, supporting H1, when regulatory structure is added to any of these models the multivariate effects of cultural values are almost fully mediated and rendered insignificant.[3] Completing this test of mediation (Baron & Kenny, 1986), the zero-order correlations of three of the four Hofstede indices with privacy regulation are significant (Table 3), indicating that regulation summarizes variation in cultural values. In the model that included all four dichotomized Hofstede indices, the multivariate effect of regulatory structure was significant (Wilk's $\Lambda = .86$, $F(12,878) = 5.73$, $p < .001$), but only UAI was significant at the .05 level (Wilk's $\Lambda = .97$, $F(6,439) = 2.41$, $p = .026$), while IND was significant at the .10 level (Wilk's $\Lambda = .98$, $F(6,439) = 1.85$, $p = .087$).[4] Table 5 lists the least-squares means for different privacy regulation structures.

Tables 4 and 5 show that neither cultural values nor regulatory structure had a significant effect on overall privacy concerns (CFIP). However, participants from cultures with *lower* IND indicated *higher* levels of concern on the CFIP subscale errors in databases ($M = 5.11$ vs. 4.72, $p = .026$). Participants from cultures with low PDI and

TABLE 4
Effects of cultural values on information privacy concerns

	PDI		IND		MAS		UAI	
	Low ($n = 293$)	High ($n = 241$)	Low ($n = 272$)	High ($n = 262$)	Low ($n = 273$)	High ($n = 261$)	Low ($n = 273$)	High ($n = 261$)
Collection	5.06 (.08)	5.27 (.09)	5.04 (.10)	5.29 (.10)	5.30 (.11)	5.03 (.11)	5.03 (.10)	5.31 (.11)
Improper access	6.18 (.07)	6.04 (.08)	6.00 (.09)	6.21 (.09)	6.20 (.10)	6.02 (.10)	6.07 (.09)	6.14 (.10)
Errors	4.99 (.08)	4.84 (.09)	5.11 (.10)	4.72 (.10)*	4.92 (.11)	4.91 (.11)	5.08 (.10)	4.75 (.11)
Secondary use	6.42 (.07)	6.09 (.08)**	6.15 (.09)	6.37 (.09)	6.42 (.10)	6.09 (.10)*	6.27 (.09)	6.24 (.10)
Overall privacy concerns	5.66 (.06)	5.56 (.06)	5.58 (.07)	5.64 (.07)	5.71 (.08)	5.51 (.08)	5.61 (.07)	5.61 (.07)
Desire for more regulation	4.66 (.12)	4.15 (.14)*	4.51 (.15)	4.30 (.16)	4.40 (.17)	4.41 (.17)	4.25 (.15)	4.56 (.16)
Security of online transactions	4.45 (.14)	4.83 (.16)	4.49 (.18)	4.79 (.18)	5.04 (.19)	4.24 (.19)*	4.40 (.17)	4.88 (.19)

Note. Least-squares means adjust for all the other effects in the model (standard errors in brackets). Model included effects of order of presentation, cultural values (high vs. low PDI, IND, MAS, and UAI), Internet experience (in months), gender, age, and education. Significance: *** $p < .001$; ** $p < .01$; * $p < .05$.

TABLE 5
Effects of privacy regulation on information privacy concerns

	Regulation		
	None ($n = 25$)	Sectoral ($n = 199$)	Omnibus ($n = 310$)
Collection	5.01 (.28)	5.36 (.19)	5.04 (.16)
Improper access	6.25 (.25)	5.85 (.17)	6.29 (.14)
Errors	5.45 (.28)^{x}	4.55 (.19)^{x}	5.15 (.16)
Secondary use	6.30 (.25)	5.99 (.17)	6.45 (.14)
Overall privacy concerns	5.75 (.19)	5.44 (.13)	5.73 (.11)
Desire for more regulation	4.85 (.42)^{x}	3.36 (.29)^{xy}	5.17 (.23)^{y}
Security of online transactions	6.01 (.49)^{xy}	4.55 (.33)^{x}	4.59 (.27)^{y}

Note. Least-squares means adjust for all the other effects in the model (standard errors in brackets). Model included effects of order of presentation, regulation of information privacy, cultural values (high vs. low PDI, IND, MAS, and UAI), Internet experience (in months), gender, age, and education. Means with the same superscript letters are significantly different from each other at $p < .05$.

low MAS had higher levels of concern about unauthorized secondary use (PDI $M = 6.42$ vs. 6.09, $p = .007$; MAS $M = 6.42$ vs. 6.09, $p = .056$). Participants from cultures with low PDI also desired more privacy regulation ($M = 4.66$ vs. 4.15, $p = .014$), while participants from cultures with low MAS were more concerned about the security of online transactions ($M = 5.04$ vs. 4.24, $p = .020$). These results offer some limited support for H1.

Participants from countries with no privacy regulation were more concerned about errors in databases compared with participants from countries with sectoral privacy regulation ($M = 5.45$ vs. 4.55, $p = .002$). Participants from countries with no privacy regulation were also more concerned about the security of online transactions compared to participants from countries with either sectoral ($M = 6.01$ vs. 4.55, $p = .004$) or omnibus regulation ($M = 6.01$ vs. 4.59, $p = .025$). Both these results are inconsistent with H2.

In line with H3, participants from countries with omnibus privacy regulation had greater desire for more regulation than participants from countries with sectoral regulation ($M = 5.17$ vs. 3.36, $p < .001$). However, participants from countries with sectoral privacy regulation had less desire for more regulation than participants from countries with no privacy regulation ($M = 3.36$ vs. 4.85, $p = .001$).

Consistently across all eight models, and consistent with H4, the multivariate effect of Internet experience was significant (e.g., dichotomized Hofstede indices model: Wilk's $\Lambda = .97$, $F(6,439) = 2.12$, $p = .049$). To illustrate the effects of Internet experience, we split the sample at the median level of experience, 18 months, and estimated least-squares means for participants with high and low levels of Internet experience. Participants with more Internet experience were less concerned about online privacy overall (CFIP $M = 5.60$ vs. 5.70, $p = .026$), and in particular were less concerned about improper access ($M = 6.05$ vs. 6.23, $p = .019$) and secondary use ($M = 6.15$ vs. 6.38, $p = .002$).

The least-squares means listed in Table 5 also control for a significant multivariate order of presentation effect (Wilk's $\Lambda = .96$, $F(6,439) = 2.98$, $p = .007$). Participants who first answered the CFIP scale items indicated more concern about errors and secondary use, and consequently had higher levels of overall privacy concerns (CFIP $M = 5.72$ vs. 5.56, $p = .021$). There were also significant multivariate effects for demographics (age, Wilk's $\Lambda = .94$, $F(6,439) = 4.85$, $p < .001$; and gender, Wilk's $\Lambda = .97$, $F(6,439) = 1.89$, $p = .081$; education was not significant). These demographic effects, with the exception of education (cf. Culnan, 1995; Milne et al., 1996; Milne & Gordon, 1994; Sheehan, 2002; Wang & Petrison, 1993), were in line with previous research: Older participants were more concerned about privacy overall (CFIP $M = 5.76$ vs. 5.55, $p < .001$; cf. Campbell, 1997; Milne et al., 1994; Sheehan, 2002; Wang & Petrison, 1993), and females indicated more concern on one of the CFIP subscales, secondary use ($M = 6.35$ vs. 6.15, .034; cf. IBM, 1999; Westin, 1998).

DISCUSSION

As far as we are aware, this is the first study to use a global sample of online consumers (as opposed to auditors: Milberg et al., 2000) to systematically investigate whether concerns about information privacy can be explained by differences in cultural values, privacy regulation, and Internet experience, by controlling for differences between samples in their demographics and Internet experience. We found that cultural values do have an influence on consumers' concerns about information privacy, largely confirming the findings of Milberg et al. (2000). However, in our sample, the influence of cultural values was only seen in two dimensions of information privacy concerns, errors in databases and unauthorized secondary use, rather than in overall concern for information privacy (CFIP). Three of the Hofstede indices (PDI, IND, and MAS) had an influence on privacy concerns in the opposite direction to that reported by Milberg et al. (2000). The influence of the fourth index (UAI) was not significant. One reason

for the difference between our results and those reported by Milberg et al. (2000) may be the method of analysis employed. Milberg et al. (2000) used partial least squares (PLS), which assigns weights to predictor variables that maximize the explained variance in the ultimate dependent variable (Chin, 1998). Like other forms of regression analysis, using predictors that are highly multicollinear, such as the four Hofstede indices, may produce unstable and biased PLS estimates of these weights. When we reproduced the relevant section of the Milberg et al. (2000) structural equation model, using PLS to predict CFIP or its dimensions from a formative index of cultural values defined by the four Hofstede indices, we also obtained results that differed from our MANOVA results. In particular, UAI is significant and negative, as Milberg et al. found.[5] The much simpler methods of analysis that we employed are less likely to generate biased estimates, and by employing multiple methods we cross-validated our findings. The negative association between IND and privacy concern found in our study contrasts with Milberg et al. (2000), but not with the majority of cross-cultural research, which has generally found that people from high IND cultures are comfortable with higher levels of disclosure of private information (e.g., Lewin, 1936; Ting-Toomey, 1991). For example, Maynard and Taylor (1996) found that students from Japan (IND = 46) were more concerned about privacy than students from the United States (IND = 91), and the IBM (1999) privacy survey, which used national probability samples from the United States and Germany (IND = 67), found that Americans were twice as likely to be classified as "low" in privacy concern compared to Germans.

We also found support for one of our hypotheses about the influence of national regulation on privacy concerns. Consumers from countries with a history of introducing government regulation of information privacy desired even stronger regulation of data collection, which was consistent with the Milberg et al. (2000) results. However, we found that consumers from countries with no privacy regulation were more concerned about one aspect of online privacy, errors in databases, than consumers from countries with sectoral privacy regulation. Consumers from countries without privacy regulation were also more concerned about the security of online transactions than consumers from countries with any form of privacy regulation, either sectoral or omnibus. This result contrasts with the findings of Milberg et al. (1995, 2000). One explanation for this difference may be the use of consumers instead of auditors. Unless they are legally obliged to have them, auditors may not have concerns about other people's privacy. Our findings seem more psychologically credible for consumers, who should feel more concerned about their information privacy in countries that offer no protection for their privacy.

An important finding in our study, and one that corroborates the Milberg et al. (1995, 2000) theoretical models, is that privacy regulation mediates cultural differences in information privacy concern. However, while including regulation in a model absorbs many of the effects of culture on privacy concerns, particularly those about errors in databases, other concerns surface that were previously obscured. These concerns about improper access and unauthorized secondary use (for cultures high in IND) and about the security of online transactions (for cultures high in UAI) are likely to persist, even if country differences in regulatory regimes were harmonized. (In our models, controlling for regulatory differences effectively equalized the effect of regulation across cultures.)

Finally, we found consistent evidence that online privacy concerns diminish with Internet experience. As more consumers use the Internet and the average level of experience rises, online privacy concerns should gradually fall, and the latest data from the United States suggests that this is already happening (Consumer Internet Barometer, 2003).

Limitations

We concentrated on minimizing differences between online consumers from the United States and other countries, rather than recruiting representative samples of consumers from each country. Furthermore, we ascribed country scores on Hofstede's cultural values indices to consumers from these countries, rather than measuring each consumer's cultural values individually. Future research should attempt to replicate our findings using national probability samples from various countries, and individual-level measures of cultural values. Future studies should also translate the Smith et al. (1996) CFIP scale into other languages to increase the coverage of countries. Finally, the Internet population is continually changing, and studies such as this one require frequent replication. However, recent U.S. polls (e.g., Harris Interactive, 2002) suggest that privacy concerns have generally remained at the levels indicated by our survey, even though our data were collected in 1998–1999.

Managerial Implications

U.S. companies that adopt the Safe Harbor Principles in order to transfer and process personally identifiable data collected from customers or employees who live in the EU may find that implementing these FIPs requires extensive changes to existing business practices or entirely new data protection practices (see Crutchfield George et al., 2001, for a discussion of the implications of the EU Directive for U.S. multinational employers). Different implementations of the EU Directive's FIPs in different countries

outside and even inside the EU may necessitate even more restrictive data protection practices to be applied on a country-by-country basis. U.S. companies have adopted different policies and practices to reflect these differences in legal regimes, ranging from refusing to collect data from international consumers to full cooperation with local enforcement authorities (which is only required for human resources data under the Safe Harbor Principles: FAQ 9; U.S. Department of Commerce, 2000).

Our results show very similar levels of concern across cultures and regulatory regimes on most dimensions of information privacy, which suggests that companies should be able to employ the same basic set of FIPs worldwide. However, we also found that countries with certain combinations of cultural values or privacy regulation will be more sensitive to some of these privacy dimensions. For example, although consumers from all the countries in our sample feel the same level of overall concern about information privacy, consumers from countries with no privacy regulation or with omnibus regulation desire more government involvement in the regulation of corporate privacy practices than consumers from countries with sectoral privacy regulation. Since regulatory structure largely mediates cultural influences, managers generally need only know the regulatory regime that applies in a country to adequately adjust their privacy policies to the privacy preferences of consumers in that country. The task of customizing privacy policies across countries and across customer segments is very expensive and labor-intensive, but software is available that at least ensures that privacy promises made are automatically kept (Whiting, 2002), for example, the Tivoli Privacy Manager from IBM (IBM, 2002). We offer the following basic guidelines where our research shows that cultural or regulatory differences affect perceptions of adherence to three of the Safe Harbor Principles:

1. *Data integrity.* Concerns about errors in databases are entirely mediated by differences in privacy regulation. Consumers from countries with no privacy regulation are more concerned about errors in databases than consumers from countries with sectoral regulation (e.g., the United States).
2. *Choice and onward transfer.* After controlling for differences in regulation, unauthorized secondary use is a greater concern in highly individualist cultures (e.g., the United States).
3. *Security.* Consumers from countries with no privacy regulation have significantly more concerns about the security of online transactions. If regulation were harmonized across countries, consumers from high UAI cultures (e.g., Greece) would still have more concerns about transaction security, and high IND cultures (e.g., the United States) would have more concerns about improper access to databases.

Conclusion

Only when consumers around the world trust online companies with their data will those companies be able to make the most of the possibilities offered by global database marketing. To provide this level of trust, companies will increasingly have to customize their information collection and management strategies to match the privacy concerns of consumers in different regions. Our research shows that most of these concerns are highly related to the privacy regulatory framework prevailing in a particular country, which tends to reflect as well as shape the privacy preferences of individual consumers. Another influence on online privacy concerns is lack of experience with the Internet, but this influence is likely to diminish as the average level of experience grows. However, some of these differences in concern reflect differences in cultural values that are likely to persist or, more accurately, would only become apparent if privacy regulation across countries were harmonized.

NOTES

1. There was a significant correlation ($r = .18$, $p < .001$) in our sample between Internet experience and knowledge of Web privacy issues, as measured by six items: whether ("yes" or "no") the participant had ever examined a Web site's privacy policy; how knowledgeable participants were (0 = "I really don't know," 1 = "I have a faint idea," or 2 = "I am pretty knowledgeable") about five concepts related to online privacy: "putting a cookie on a machine," "SET" (Secure Electronic Transaction, adopted by very few Web sites at the time of our survey), "Privacy Policy," "TRUSTe" (the largest privacy policy certifier), and "Clickstreams and Log Files." We multiplied responses to the privacy policy item by two and then summed responses to all six items to create an index of Web privacy knowledge (U.S. $\alpha = .71$, international $\alpha = .73$).

2. PDI, Wilk's $\Lambda = .96$, $F(6,444) = 3.23$, $p = .004$; IND, Wilk's $\Lambda = .94$, $F(6,444) = 4.71$, $p < .001$.

3. If the cultural values indices are analyzed individually, with regulatory structure included in the model, UAI has a significant multivariate effect at the .10 level of significance (Wilk's $\Lambda = .97$, $F(6,442) = 1.90$, $p = .079$).

4. Consumers with high UAI were more concerned about the security of online transactions ($M = 5.37$ vs. 4.73, $p = .04$). Consumers with high IND were more concerned about improper access ($M = 6.29$ vs. 5.97, $p = .06$) and unauthorized secondary use ($M = 6.41$ vs. 6.09, $p = .06$).

5. Only two of these models had a significant path from cultural values to the dependent variable: errors ($\beta = .17$, $t = 3.73$) and collection ($\beta = -.16$, $t = 2.10$). In the errors model, three of the four Hofstede indices had significant weights, of which two were negative, and one was positive: IND ($-.84$, $t = 3.25$), UAI ($-.73$, $t = 3.65$), MAS (.63, $t = 2.65$). In the collection model, UAI is the only index with a significant weight (at the .10 level), and it is negative ($-.50$, $t = 1.79$).

REFERENCES

Bagozzi, Richard P., and Yi, Youjae. 1989. On the use of structural equation models in experimental designs. *Journal of Marketing Research* 26(3):271–284.

Baron, Reuben M., and Kenny, David A. 1986. The moderator–mediator variable distinction in social psychological research: Conceptual, strategic and statistical considerations. *Journal of Personality and Social Psychology* 51(6):1173–1182.

Bellman, Steven, Johnson, Eric J., and Lohse, Gerald L. 2001. To opt-in or opt-out? It depends on the question. *Communications of the ACM* 42(12):32–38.

Benassi, Paola. 1999. TRUSTe: An online privacy seal program. *Communications of the ACM* 42(2):56–59.

Bennett, Colin J. 1992. *Regulating privacy: Data protection and public policy in europe and the United States*. Ithaca, NY: Cornell University Press.

Bentler, P. M., and Bonett, Douglas G. 1980. Significance tests and goodness-of-fit in the analysis of covariance structures. *Psychological Bulletin* 88(3):588–606.

Campbell, Alexandra J. 1997. Relationship marketing in consumer markets: A comparison of managerial and consumer attitudes about information privacy. *Journal of Direct Marketing* 11(3):44–57.

Chin, Wynne. 1998. Issues and opinion on structural equation modeling. *MIS Quarterly* 22(1):vii–xvi.

Consumer Internet Barometer. 2003. Consumers continue flocking to the internet: Usage, satisfaction and trust continue to improve. Press release, April 3. http://www.consumerinternetbarometer.us/press.htm

Crutchfield George, Barbara, Lynch, Patricia, and Marsnick, Susan J. 2001. U.S. multinational employers: Navigating through the "Safe Harbor" Principles to comply with the EU Data Privacy Directive. *American Business Law Journal* 38(4):735–783.

Culnan, Mary J. 1995. Consumer awareness of name removal procedures: Implications for direct marketing. *Journal of Direct Marketing* 9(2):10–19.

Culnan, Mary J., and Bies, Robert J. 1999. Managing privacy concerns strategically: The implications of fair information practices for marketing in the twenty-first century. In *Visions of privacy: Policy choices for the digital age*, eds. Colin J. Bennett and Rebecca Grant, pp. 149–167. Toronto: University of Toronto Press.

European Union. 1995. *Directive 95/46/EC of the European Parliament and of the Council of 24 October, 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data*. Online document, European Union. http://europa.eu.int/eur-lex/en/lif/reg/en_register_1940.html

European Union. 2000. *Report on the Draft Commission Decision on the Adequacy of the Protection Provided by the Safe Harbour Privacy Principles, June 22*. http://europa.eu.int/comm/internal_market/en/dataprot/adequacy/0177-2000en.pdf

Fjetland, Michael. 2002. Global commerce and the privacy clash. *Information Management Journal* 36(1):54–57.

Fornell, Claes, and Larcker, David F. 1981. Evaluating structural equation models with unobservable measurement error. *Journal of Marketing Research* 18(1):39–50.

Harris Interactive. 2002. *The Harris Poll #46, September 10, 2002*. http://www.harrisinteractive.com/harris_poll/index.asp?PID=325.

Hofstede, Geert. 1980. *Culture's consequences: International differences in work-related values*. Beverly Hills, CA: Sage.

Hofstede, Geert. 1991. *Cultures and organizations: Software of the mind*. New York: McGraw-Hill.

IBM. 1999. *IBM multi-national consumer privacy survey*. Somers, NY: IBM Global Services, October. http://www.ibm.com/services/files/privacy_survey_oct991.pdf

IBM. 2002. *Enable your applications for privacy with IBM Tivoli Privacy Manager for E-Business*. Somers, NY: IBM Corporation Software Group. http://www.tivoli.com/products/documents/whitepapers/privacy-mgr-e-bus.pdf

Johnson, Eric J., Bellman, Steven, and Lohse, Gerald L. 2002. Defaults, framing, and privacy: Why opting in $\neq$ opting out. *Marketing Letters* 13(1):5–15.

Kahneman, Daniel, and Tversky, Amos. 1984. Choices, values, and frames. *American Psychologist* 39(4):341–350.

Lewin, Kurt. 1936. Some social-psychological differences between the United States and Germany. *Character and Personality* 4:265–293.

Lohse, Gerald L., Bellman, Steven, and Johnson, Eric J. 2000. Consumer buying behavior on the internet: Findings from panel data. *Journal of Interactive Marketing* 14(1):15–29.

Long, William J., and Quek, Marc Pang. 2002. Personal data privacy protection in an age of globalization: The US—EU Safe Harbor compromise. *Journal of European Public Policy* 9(3):325–344.

Lynn, Michael, Zinkhan, George M., and Harris, Judy. 1993. Consumer tipping: A cross-country study. *Journal of Consumer Research* 20(3):478–488.

Maynard, Michael L., and Taylor, Charles R. 1996. A comparative analysis of Japanese and U.S. attitudes toward direct marketing. *Journal of Direct Marketing* 10(1):34–44.

Meredith, William. 1993. Measurement invariance, factor analysis and factorial invariance. *Psychometrika* 58(4):525–543.

Milberg, Sandra J., Burke, Sandra J., Smith, H. Jeff, and Kallman, Ernest A. 1995. Values, personal information privacy, and regulatory approaches. *Communications of the ACM* 38(12):65–74.

Milberg, Sandra J., Smith, H. Jeff, and Burke, Sandra J. 2000. Information privacy: Corporate management and national regulation. *Organization Science* 11(1):35–57.

Milne, George R., and Gordon, Mary Ellen. 1994. A segmentation study of consumers' attitudes toward direct mail. *Journal of Direct Marketing* 8(2):45–52.

Milne, George R., Beckman, James, and Taubman, Marc L. 1996. Consumer attitudes toward privacy and direct marketing in Argentina. *Journal of Direct Marketing* 10(1):22–29.

Nijhawan, David Raj. 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):939–976.

Nowak, Glen J., and Phelps, Joseph. 1997. Direct marketing and the use of individual-level consumer information: Determining how and when "privacy" matters. *Journal of Direct Marketing* 11(4):94–108.

Nunally, Jum C. 1978. *Psychometric theory*, 2nd ed. New York: McGraw-Hill.

Organization for Economic Cooperation and Development. 2002. *OECD guidelines on the protection of privacy and transborder flows of personal data*. Paris: OECD.

Poortinga, Ype H., and Malpass, Roy S. 1986. Making inferences from cross-cultural data. In *field methods in cross-cultural research*, eds. Walter J. Lonner and John W. Berry, pp. 17–46. Beverly Hills, CA: Sage.

Privacy International. 1998. *Privacy and human rights: An International survey of privacy laws and practice*. Online document, London/ Washington, DC: Privacy International, in cooperation with the Global Internet Liberty Campaign. http://www.privacyinternational.org/survey/phr98/

Samuelson, William, and Zeckhauser, Richard. 1988. Status quo bias in decision making. *Journal of Risk & Uncertainty* 1(1):7–59.

Sheehan, Kim Bartel. 2002. Toward a typology of Internet users and online privacy concerns. *The Information Society* 18(1):21–32.

Smith, H. Jeff. 1994. *Managing privacy: Information technology and corporate America*. Chapel Hill, University of North Carolina Press.

Smith, H. Jeff. 2001. Information privacy and marketing: What the U.S. should (and shouldn't) learn from Europe. *California Management Review* 43(2):8–33.

Smith, H. Jeff, Milberg, Sandra J., and Burke, Sandra J. 1996. Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly* 20(2):167–196.

Stewart, Kathy A., and Segars, Albert H. 2002. An empirical examination of the concern for information privacy instrument. *Information Systems Research* 13(1):36–49.

Tan, Bernard C. Y., Wei, Kwok-Kee, Watson, Richard T., Clapper, Danial L., and McLean, Ephraim R. 1998. Computer-mediated communication and majority influence: Assessing the impact in an individualistic and a collectivistic culture. *Management Science* 44(9):1263–1278.

Taylor, Charles, and Fosler, Gail D. 1994. The necessity of being global. *Across the Board* 31(2):40–43.

Ting-Toomey, Stella. 1991. Intimacy expressions in three cultures: France, Japan, and the United States. *International Journal of Intercultural Relations* 15(1):29–46.

U.S. Department of Commerce. 2000. *Safe Harbor Privacy Principles, July 21*. http://www.export.gov/safeharbor/sh_overview.html

U.S. Department of Commerce. 2004. *Safe Harbor List*. http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list

U.S. Department of Health, Education, and Welfare. 1973. *Records, computers and the rights of citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems*. Washington, DC: U.S. Government Printing Office.

Walker, Kent. 2001. The costs of privacy. *Harvard Journal of Law & Public Policy* 25(1):87–128.

Wang, Paul, and Petrison, Lisa A. 1993. Direct marketing activities and personal privacy: A consumer survey. *Journal of Direct Marketing* 7(1):7–19.

Westin, Alan F. 1967. *Privacy and freedom*. New York: Athenaeum.

Westin, Alan F. 1998. *E-commerce & privacy: What Net users want*. Hackensack, NJ: Center for Social and Legal Research/Privacy and American Business, June Summary of findings available at http://www.pandab.org/E-Commercer%20Exec.%20Summary.html

Whitman, Michael E., Perez, Jorge, and Beise, Catherine. 2001. A study of user attitudes toward persistent cookies. *Journal of Computer Information Systems* 41(3):1–7.

Whiting, Rick. 2002. Making [privacy] work. *InformationWeek* 902 (August 19):30–36.