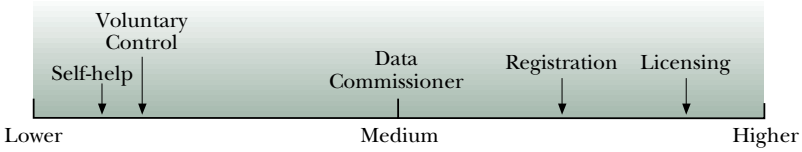
Values, Privacy, and Regulatory Approaches

Personal Information

The relationships among nationality, cultural values, personal information privacy concerns, and information privacy regulation are examined in this article.

Personal information privacy, "the ability of the individual to personally control information about oneself" [21], is fast becoming one of the most important ethical issues of our information age [4, 17]. Information technology developments—coupled with the increasing value of information to decision makers [13]—are causing a rising tide of concern about personal information privacy management practices. As such concerns continue to grow, businesses' ability to use personal information may be threatened, and decision makers will have to make trade-offs between the efficient, effective operation of businesses and the protection of personal information privacy [17].

Sandra J. Milberg, Sandra J. Burke, H. Jeff Smith, and Ernest A. Kallman



Level of Government Involvement in Corporate Privacy Management

Figure 1. Regulation Models. The models can be described as follows:

1)The "Self-Help" Model depends on data subjects' challenging inappropriate record-keeping practices. Rights of access and correction are provided for the subjects, but they are responsible for identifying problems and bringing them to the courts for resolution.

2) The Voluntary Control Model relies on self-regulation on the part of corporate players. The law defines specific rules and requires that a "responsible person" in each organization ensures compliance.

3) The Data Commissioner Model utilizes neither licensing nor registration, but relies on the ombudsman concept through a commissioner's office. The commissioner has no powers of regulation but relies on complaints from citizens, which are investigated. The commissioner also is viewed as an expert who should offer advice on data handling; monitor technology and make proposals; and perform some inspections of data processing operations. This model relies to a great degree on the commissioner's credibility with the legislature, the press, and the public.

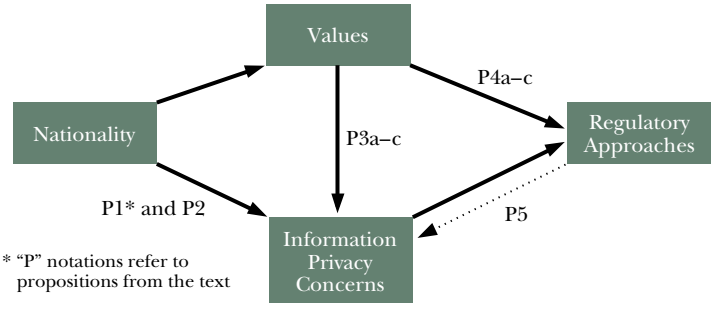
4) The Registration Model acts much like the Licensing Model, with one exception: the government institution has no right to block the creation of a particular information system. Only in a case where complaints are received and an investigation reveals a failure to adhere to data protection principles would a system be "deregistered." Thus, this model provides more remedial than anticipatory enforcement of principles.

5) The Licensing Model creates a requirement that each databank containing personal data be licensed (usually upon payment of a fee) by a separate government institution. This institution would stipulate specific conditions for the collection, storage, and use of personal data. This model anticipates potential problems and heads them off, by requiring prior approval for any use of data.

*Adapted from Smith [17]; categories based on Bennett [2].

This issue becomes even more complex given that interest in the globalization of information systems (IS) has emerged as organizations enter increasingly competitive international markets. Research has found that country-to-country differences must be considered when developing and implementing global IS applications [12]. Regulations and policies regarding the use of personal information differ from one country to another [2, 7, 14], as may the nature and level of information privacy concerns. Therefore, in a global marketplace dependent on transborder data flows, understanding the differences in information privacy concerns and regulatory approaches, and the relationships between them, may be a key to successfully managing those concerns.

Figure 2. Proposed model



Previous research has paid little attention to cross-cultural issues and the relationships among varying societal privacy concerns, cultural values, and information privacy regulatory policies. This empirical study addresses the complex relationships among these constructs through the following research questions:

1) What are the relationships among nationality, cultural values, and the nature and level of information privacy concerns?
2) Are cultural values and personal information privacy concerns associated with differing regulatory policy approaches?

Corporate and Public Policy Making

Corporate policy making regarding information privacy has been primarily reactive in nature, in that executives focus on information privacy issues only in response to a perceived external threat [17]. Calls for voluntary adherence to industry privacy principles are common, as are calls for additional regulation of many industry practices. However, voluntary adherence in many industries has been at best sporadic [3, 4], which given rising concerns, may result in broad regulation of information privacy issues in the private sector [17].

In most European countries, in Canada,

and in several other nations, legislative activity regarding information privacy restrictions has already snowballed [7, 14]. However, it is not clear how these accelerated reactions to information privacy are associated with cultural or national differences in privacy concerns. Indeed, nationality and cultural values may be moderating factors that affect individuals' concerns regarding information privacy, and thus have implications for both the study of privacy concerns and global information management practices.

. . .we postulate that there may be a reciprocal relationship, in which a country's regulatory approach **affects its inhabitants' levels of concern.**

Yet, while overall legislative activity regarding information privacy is flourishing internationally, no single, standard policy regarding privacy issues has emerged. An analysis of international regulatory models (see Figure 1) reveals a broad divergence in approaches [2, 17]. The models vary significantly in terms of governmental involvement in day-to-day corporate operations. At the low government involvement side (left end) of the continuum, the government assumes a "hands-off" role and allows corporations to monitor themselves, with reliance on injured individuals to pursue their own remedies in the court system. At the high government involvement side (right end) of the continuum, the government assumes authority to license and regulate all corporate uses of personal data, including the right to conduct inspections inside corporations and to examine all proposed applications of personal data before they are implemented.

Theoretical Development

Prior research into global information privacy issues has been limited primarily to considerations of various regulatory schemata [2, 7, 14]. But to date, little attention has been paid to the complex web of factors that influence—and may be influenced by—these regulatory options. As can be seen in Figure 2, different nationalities can be expected to exhibit different cultural values [9, 10, 22], which may in turn influence—along with other factors—the levels of information privacy concern among individuals in each country. These differing privacy concerns and values may, in turn, have an impact on the regulatory approach embraced by a particular country. Further, we postulate that there may be a reciprocal relationship, in which a country's regulatory approach affects its inhabitants' levels of concern. In the following sections, we briefly examine each of these relationships.

Nationality and Information Privacy Concerns

Westin [23] found that 1) every society values privacy in some form, but 2) the expressions of this privacy vary significantly across cultures. He also showed that all modern, democratic societies provide for solitude, intimacy, anonymity, and reserve—the four basic states of privacy [23]. Additionally, Westin noted that variations in privacy social balances, under which privacy's states are traded off against other societal values, are prominent even in societies that are rather homogeneous in many other respects. These variations in privacy patterns in interpersonal relations have been observed across countries by anthropologists, psychologists, and sociologists [23].

It might be expected, then, that individuals in different countries would exhibit different levels of concern regarding information privacy at a given point in time. This leads to:

PROPOSITION 1: *Levels of personal information privacy concern will differ across countries.*

It can also be inferred from Westin's [23] "social balance" arguments that different dimensions of information privacy may be perceived differently in different countries. Past research suggests that information privacy concerns are not unidimensional but instead consist of a number of underlying factors. Four underlying dimensions of personal information privacy concern have been identified by Smith et al. [19]: 1) Collection, a perception that "there's too much damn data collection going on" [15]; 2) Unauthorized secondary use, under which personal data collected for one purpose is used for another without permission; 3) Errors, which can be prevented by greater attention to the integrity of databases, and 4) Improper access, caused by looseness in management of "need to know" policies within an organization [17].

It can be argued that the nature of information privacy concerns—the hierarchy of levels of concern associated with various dimensions—may also be culturally affected. For example, Britain's "deferential democratic balance," which values reserve between English citizens and a high level of personal privacy in homes and private organizations, might be expected to produce concerns about the various dimensions of information privacy different from those produced by the United States's "egalitarian democratic balance," with a constant tension between individualism and social egalitarianism [23]. We thus state:

PROPOSITION 2: *The hierarchy of dimensions of information privacy concern will differ across countries.*

Nationality and Cultural Values

Values can be defined as shared beliefs or group norms that have been internalized by individuals [6]. Researchers have identified several major value dimensions in which national cultures can be distinguished [e.g., 9, 10, 22]. National differences with respect to cultural values result from a number of ecological factors, such as a country's history, economy, technology, geography, religiosity, and demographics, and remain relatively stable over time [9, 10, 22]. Furthermore, research has shown that values differ to some degree across countries and influence a society's responses to the environment [9, 10, 22].

Cultural Values and Concerns for Personal Information Privacy

Previous research has shown links between a number of individual traits or values and information privacy issues [20]. For example, Smith et al. [19] observed significant positive associations between individuals' information privacy concerns and their levels of trust, paranoia, and social criticism. But just as individuals have certain values, so do cultures. "Culture is to a human collectivity what personality is to an individual" [9]. Given that links have been observed between individual values and information privacy concerns, it seems likely that associations between cultural values and information privacy concerns may also exist. In particular, this should be true for three cultural values identified by Hofstede [9, 10]: uncertainty avoidance, power distance, and individualism versus collectivism.

The uncertainty avoidance index (UAI) measures the extent to which a society feels threatened by uncertain and ambiguous situations and tries to avoid these situations [9, 10]. Hofstede [9, 10] found that low scores on this index were associated with low levels of anxiety and stress and a willingness to take risks. High scores were associated with high levels of anxiety, stress, and concern for security. Further, respondents in high UAI countries had a pessimistic outlook regarding the motives of companies [9, 10]. Therefore, we expect:

PROPOSITION 3a: *Respondents in high "uncertainty avoidance" countries will exhibit higher levels of concern regarding information privacy.*

The power distance index (PDI) measures the degree of inequality in power between a less powerful individual and a more powerful other [9, 10]. Studies have shown that high PDI countries exhibit lower levels of interpersonal trust. Countries with high scores on this index feel that people are a potential threat and rarely can be trusted [9, 10]. In addition, Smith et al. [19] observed a positive relationship between interpersonal distrust and concerns for personal information privacy. Therefore, we postulate:

PROPOSITION 3b: *Respondents in high "power distance" countries will exhibit higher levels of concern regarding information privacy.*

The individualism (IDV) index measures an individual's independence from organizations [9, 10]. High scores on this index reflect an "I" mentality—an emphasis on individual initiative and achievement. Low scores reflect a "we" mentality, an emphasis on loyalty and belonging and an emotional dependence of individuals on organizations. Countries with high scores on this index tend to place more value on employees' personal lives. In addition, one general societal norm found to be associated with high IDV countries is the belief that everyone has the right to a private life; in low IDV countries there is more of an acceptance that organizations will invade one's private life [9, 10]. This leads us to:

Low levels of interpersonal trust among individuals in a society *may result in a desire for more government involvement to protect personal information privacy.*

PROPOSITION 3c: *Respondents in high "individualism" countries will exhibit higher levels of concern for information privacy.*

Cultural Values and Regulatory Approaches

Cultural values affect the development and maintenance of societal institutions, including political and legislative bodies [9, 10]. An analysis of political systems and legislation in various countries shows differences that can be interpreted as consequences of societal value differences. For example, Almond and Verba [1] observed that different "political cultures" are related to different cultural values.

Given that countries with high UAI scores exhibit higher levels of anxiety, stress, and concern for security, it is not surprising that they also exhibit preferences for clear written rules and regulations [9, 10]. Countries high in uncertainty avoidance have been shown to more aggressively embrace regulatory solutions than countries low in uncertainty avoidance [9, 10]. We therefore conjecture that:

PROPOSITION 4a: *Countries exhibiting high "uncertainty avoidance" will exhibit higher levels of government involvement in regulating information privacy.*

In a society in which high levels of inequality (high PDI) exist among citizens, the level of trust tends to be lower [9, 10]. Low levels of interpersonal trust among individuals in a society may result in a desire for more government involvement to protect personal information privacy. Further, Mulder [16] observed that individuals strive to reduce the power distance between themselves and more powerful people. Legislation may be one way to reduce the power inequalities that exist in such a country as well as the levels of interpersonal distrust that may result as a consequence of high levels of power inequalities. We therefore expect that:

PROPOSITION 4b: *Countries with higher levels of "power distance" will exhibit higher levels of government involvement in regulating information privacy.*

In countries with high IDV scores, individuals exhibit emotional independence from organizations and institutions. These societies value individual more than group decisions [9, 10, 22]. The level of individualism/collectivism in a society should also be associated with beliefs about organizational and governmental regulations or interventions. Inhabitants in high IDV countries tend to both desire fewer organizational and governmental rules and comply less with rules and regulations. Therefore, we expect:

PROPOSITION 4c: *Countries with higher levels of "individualism" will exhibit less government involvement and more individualistic approaches to regulating information privacy.*

Information Privacy Concerns and Regulatory Approaches

The relationship between levels of information privacy concern and regulatory approaches in various countries is expected to be a complex one. A number of authors have observed that regulatory responses usually occur in reaction to a growing level of discontent within the populace, which is transmitted to legislators in some form [2, 7, 17]. Smith [17] argues that higher levels of concern in the populace will generally be associated with higher levels of government involvement.

However, this earlier work rarely addresses the reciprocal relationship (denoted in Figure 2 by a dotted line) between regulatory structure and levels of information privacy concern. It could be conjectured (based loosely on Bennett [2]) that as a society embraces more strict regulation regarding personal information handling practices, levels of concern within the populace may be relaxed as a function of reduced numbers of privacy violations in the country. Smith and Kallman's work [18] provided some support for this relationship. This suggests that regulation will increase as concern increases to a point at which regulation is sufficient to dampen concerns; then concerns will relax as the regulation becomes more pronounced. Therefore, we expect:

PROPOSITION 5: *Lower levels of information privacy concern will be associated with both 1) countries with no privacy regulation and 2) countries with the highest levels of government involvement in corporate privacy management; higher levels of privacy concern will be associated with more moderate regulatory structures.*

Method and Procedures

To examine the links among nationality, information privacy concerns, cultural values, and regulatory approaches, an ex post facto quasi-experimental design was used. Although it takes the only practical approach to this type of research, this study can provide evidence only of association between constructs; it cannot establish causality.

To evaluate the propositions, a number of measures were required. First, measurements of personal information privacy concerns were collected from a sample that included respondents of various nationalities. Then, measures of predominant values were obtained for each of the nationalities. Finally, the existing information privacy regulatory approach in each of the relevant countries was coded according to the regulatory "model" (see Figure 1) that it matched most closely. These steps are elaborated on in the following sections.

Cross-Cultural Information Privacy Concerns

To gather measurements of personal information privacy concerns in various countries, an information privacy concern instrument developed and validated by Smith et al. [19] was used. This instrument, which contains 15 items on 7-point Likert scales, identifies four underlying dimensions of information privacy concern: 1) Collection, 2) Unauthorized secondary use, 3) Errors, and 4) Improper access. In addition to this instrument, the survey included some demographic items (see Appendix).

The survey was administered to a sample of

Table 1. Country classifications

Classification	Countries
No information privacy regulation	Thailand
Self-Help (Model 1)	France
Voluntary Control (Model 2)	Japan United States
Data Commissioner (Model 3)	Australia Canada New Zealand
Registration (Model 4)	Denmark United Kingdom
Licensing (Model 5)	None

approximately 900 members of the Information Systems Audit and Control Association (ISA & CA) in approximately 30 countries. The sample was comprised of 74% men and 36% women. The respondents were primarily IS auditors (64%) or financial auditors (10%) at various levels in their organizations (executives/directors, 13%; managers, 40%; lower-level subordinates, 47%), with an average of 16 years of industry experience. Surveys were distributed at selected chapter meetings, filled in by the respondents during the meetings, and collected by the chapter presidents.[1] Data from these surveys were used as measures of personal information privacy concern.

Table 2. Level of information privacy concern by dimension in countries

Country	Collection	Secondary Use	Errors	Improper Access
United States	5.4 (4)*	6.1 (1)	5.5 (3)	5.9 (2)
Canada	5.7 (3)	6.4 (1)	5.6 (4)	6.1 (2)
Australia	5.6 (3)	6.6 (1)	5.3 (4)	5.8 (2)
United Kingdom	5.2 (4)	6.0 (1)	5.6 (3)	5.8 (2)
New Zealand	5.3 (3)	6.4 (1)	5.2 (4)	5.9 (2)
France	5.0 (4)	6.6 (1)	5.5 (3)	6.2 (2)
Japan	4.9 (4)	6.3 (2)	5.6 (3)	6.5 (1)
Denmark	4.8 (4)	6.2 (1)	5.5 (3)	6.1 (2)
Thailand	4.7 (4)	5.8 (2)	5.2 (3)	6.0 (1)

*First number represents the mean (on a scale of 7), and number in parentheses represents the dimension's rank in the given country.

Cross-Cultural Values

To operationalize measures of the predominant value systems of the various countries in the study, three cross-cultural value indices—power distance, uncertainty avoidance, and individualism—developed by Hofstede [9, 10] were utilized. Countries used in this study (Australia, Canada, Denmark, France, Japan, New Zealand, Thailand, the United Kingdom, and the United States)[2] were assigned measures of cultural values based on the Hofstede [10] indices. The value indices range from zero to 100, with 100 representing the highest level or strongest degree to which the value dimension is manifested in the culture. In the sample of countries included in this study, the power distance index scores ranged from 18 in Denmark to 68 in France; the uncertainty avoidance index scores ranged from 23 in Denmark to 92 in Japan; and the "individualism" index scores ranged from 20 in Thailand to 91 in the United States.

Information Privacy Regulatory Approaches/Models

To operationalize measures of government involvement in information privacy regulation in each of the countries, existing regulatory approaches were coded according to the regulatory "model" that they fit best. This coding was based on an assessment of the countries' regulatory approaches to information privacy as documented by Madsen [14].

Specifically, two judges, blind to the purposes of the study, were provided with extensive descriptions of information privacy regulatory models as shown in Figure 1. These regulatory model descriptions were used as the classification codes in the present study. In addition, the judges were provided with extensive descriptions of each country's existing information privacy regulations from Madsen [14]. The judges used these regulation descriptions to classify the information privacy policy of each country in the study according to which of the five regulatory models best reflected the elements of its existing policy. Furthermore, "no information privacy regulation" was available to the judges as a classification option. The inter-judge reliability of the coding was 0.81, with disagreements reconciled by a third independent judge. Results of the coding process can be seen in Table 1.

Analyses and Results

A number of analyses were performed to assess the associations in the proposed model, with the exception of the nationality/values link, which has been shown in previous studies [9, 10, 22].

Relationship Between Nationality and Information Privacy Concerns

Proposition 1 predicted that the level of personal information privacy concern would vary across countries. An ANOVA assessing group differences in the overall level of information privacy concern by country (determined by calculating each respondent's mean score across the 15 items on 7-point scales) showed that overall level of information privacy concern varied significantly ($p < 0.01$) across nationalities. The mean overall concern levels in the sampled countries ranged from a low of 5.36 in Thailand to a high of 6.01 in Canada.[3] These results provide support for Proposition 1.

[1] In some cases, meeting attendees took the surveys home and returned them to the researchers. We separated these surveys from those administered in the controlled environment and performed *t*-tests to ascertain any differences. There were no significant differences in response patterns; thus, all the responses were used.

[2] Only those countries from which 20 or more responses to the information privacy instrument were returned were used in this study ($n = 706$). The following countries were therefore eliminated: Argentina, Belgium, China, Finland, Germany, Holland, Hungary, India, Italy, Liechtenstein, Malaysia, Norway, Russia, and Switzerland. Nationality of respondents was self-reported (see item in Appendix).

Proposition 2 suggested that in addition to overall levels of information privacy concerns, the relative importance or hierarchy of the dimensions of those concerns should also vary across nationalities. To test this proposition, a chi-squared contingency test was used to assess the level of association between nationality and relative importance of the four dimensions of information privacy concerns (determined by calculating mean scores across the relevant items pertaining to the respective dimensions). The aggregate mean scores for each of the dimensions by country (see Table 2) were used to conduct the chi-square contingency analysis.

The results of the analysis showed no significant difference in the relative importance or hierarchy of concerns across nationalities. In fact, "secondary use" (overall mean = 6.16, SD = 0.98) was the highest concern dimension in seven of the nine countries sampled and second in the remaining two. "Improper access" (mean = 6.00, SD = 0.95) was the second most important dimension virtually across the board, with "collection" (mean = 5.31, SD = 1.13) and "errors" (mean = 5.55, SD = 1.04) being the two least important dimensions in every case. These results do not support Proposition 2.

Relationship Between Cultural Values and Information Privacy Concerns

Propositions 3a–3c suggest that cultural values should influence the level of personal information privacy concern in a society. To test these propositions, a regression analysis was performed to assess the association between each of the three relevant value dimensions (power distance, uncertainty avoidance, and individuality) and information privacy concerns. However, no significant relationships were found between the overall level of information privacy concern and any of the three value dimensions.

Relationship Between Cultural Values and Privacy Regulations

Propositions 4a–4c suggest that the amount of government involvement in information privacy regulation is affected by cultural values in the various countries. A polychotomous probit analysis was used to test these propositions.[4] In the analysis, regulatory structure (ranging from "no regulatory policy" to Model 4, which reflects high government involvement) was the dependent variable, and privacy concerns, along with the three cultural values, were the independent variables.[5]

Results of this analysis (see Table 3) showed signif-

[3] Responses within each country were relatively homogeneous, with standard deviations ranging from 0.86 (U.S.) to 0.46 (Thailand).

[4] A probit analysis was utilized instead of ordinary least squares (OLS) regression because the dependent variable was categorical rather than interval in nature.

[5] The information privacy concerns and cultural values were both included in the probit analysis because both have postulated relationships to the dependent variable (regulatory approach). Thus, exclusion of information privacy concerns might have led to 1) estimation bias in parameters and/or 2) insufficient explained variance of the model fit.

Table 3. Relationship between cultural values, privacy concerns, and regulatory models—probit analyses (n = 706)

Source of Variance	Probit Coefficient	Standard Error	p-value
"Power Distance" value	0.19	0.01	0.0001
"Uncertainty Avoidance" value	0.02	0.009	0.02
"Individuality" value	−0.02	0.006	0.02
Level of information privacy concern	−0.14	0.06	0.03

Lack-of-fit chi-square	p-value
982.2	>0.10

Table 4. Association between level of information privacy concern and regulatory approaches

Model	Mean Concern (7 = highest concern)	Comparisons	p-value
No regulation	5.36	vs. Models 1, 2, 3	0.02
		vs. Model 4	ND*
Self-Help (Model 1)	5.92		
Voluntary Control (Model 2)	5.72		
Data Commissioner (Model 3)	5.88		
Registration (Model 4)	5.63	vs. Models 1, 2, 3	0.02
		vs. "No regulation"	ND

*ND = No difference (p >0.10)

icant effects of each of the three cultural values on the model of privacy regulation existing in the various countries. As expected, the value dimensions of power distance and uncertainty avoidance each had statistically significant positive effects ($p < 0.03$ for each dimension) on existing privacy regulation. Further, the dimension of individuality had an expected significant negative effect ($p < 0.02$) on regulation.[6] A Chi-square lack-of-fit test performed on the probit analysis showed a non-significant chi-square, suggesting sufficient model fit. This analysis provides support for Propositions 4a–4c.[7]

Relationship Between Information Privacy Concerns and Privacy Regulations

Proposition 5 suggests that there will be differences in privacy concerns associated with different regulatory structures. Specifically, lower levels of information privacy concern will be associated with "no regulation" countries and with the highest levels of government involvement in corporate privacy management, while higher levels of privacy concern will be associated with more moderate regulatory structures. This proposition was tested using ANOVA and mean comparisons. An ANOVA was used to assess the significance of group differences in information privacy concerns among respondents grouped by their country's regulatory structure model (Figure 1). As expected, the level of information privacy concern varied significantly ($p < 0.005$) among the groups.

As shown in Table 4, countries with either "no privacy regulation" or the most strict model of privacy regulation observed in the study (registration model) were associated with significantly lower information privacy concerns ($p < 0.02$) than those using the other three models. Countries with more moderate regulatory structures were associated with higher aggregate levels of concern, and those levels of concern were not significantly different from one another ($p > 0.10$). These findings provide support for Proposition 5.

Discussion

As global approaches to IS management and transborder data flows become more commonplace, national differences in personal information privacy concerns and regulatory approaches to privacy protection stand as prominent challenges to both design and implementation of cohesive information systems. In an attempt to address some of the cross-cultural issues associated with personal information privacy, this study examined relationships among nationality, cultural values, personal information privacy concerns, and information privacy regulatory approaches.

Differences in overall levels of personal information privacy concern based on nationality were observed, as were associations among regulatory approaches, levels of information privacy concern, and cultural values. Contrary to expectations, the hierarchy of information privacy concerns appears consistent across nationalities, and a link between cultural values and levels of information privacy concern was not observed. Implications of these findings will be discussed, along with constraints of the study.

Limitations

This is one of the first cross-cultural, empirical studies related to personal information privacy. Therefore, certain limitations—imposed primarily by sampling issues—must be acknowledged.

First, the sample in this study may not be representative, given that it consisted of ISA & CA members and that the number of responses were too few in several countries to allow inclusion. But the fact that some differences across countries were observed in this somewhat homogeneous population may suggest that more dramatic differences could be expected in a sample drawn from the general populations of the countries.

Second, the lack of support for the association between cultural values and information privacy concerns may be explained by the use of 1) a limited set of cultural values and 2) aggregate rather than individual value scores—constraints imposed by the survey's length and the limitations of the surveyed organization. Even in light of these constraints, the present study provides some preliminary yet useful insights into the international information privacy domain.

Implications for Managers

The overall level of information privacy concern among the ISA & CA members, across all countries, was high. Since these respondents are particularly well acquainted with information privacy policies and practices inside corporations, these high levels of concern should stand as a sobering reminder of potential problems that may lie ahead. In that high levels of information privacy concern were shown to be associated with increasing degrees of government involvement in corporate privacy management, IS executives should expect governmental responses if their own actions do not abate these concerns.

Most organizations have been reactive in their management of privacy issues, waiting for an external threat before crafting cohesive policies [17]. A more thoughtful managerial approach would include a proactive focus on privacy issues before an external threat forced a defensive corporate response or excessively restrictive regulation. The national differ-

[6] Interpretation of the probit coefficients is the same qualitatively as in OLS regression. The sign of the coefficient determines the direction of the effect; larger coefficients are associated with larger effects. However, the effect of size of the independent variable on the dependent variable is not directly comparable to that in OLS regression, in that the probit coefficient indicates the change in standard deviation of the normally distributed (transformed) dependent variable [8].

[7] Note that the effect of information privacy concern on privacy regulation was significantly negative. This can be attributed to the hypothesized reciprocal relationship between the two variables, which is examined with respect to Proposition 5.

ences observed in this study seem to suggest that IS managers in international organizations should embrace a multinational approach to the development of systems utilizing personal data, by crafting country-specific solutions [12]. Furthermore, it may be appropriate to pay even more attention to privacy controls in countries where levels of concern are highest and where the culture values regulatory solutions. Finally, special attention should be devoted to unauthorized secondary use and improper access in every country. These approaches should reduce the probability of consumer backlashes, of negative media exposure, and of onerous legislative solutions.

But this approach, while managerially prudent, may be flawed from some ethical perspectives. It can be reasonably argued that protection of personal information privacy is a "hypernorm"—a principle that is so "fundamental to human existence that [it serves] as a guide" across all cultures [5]. If this is so, then managers have an obligation to protect personal information privacy in every system and in every country, regardless of distinctions in national levels of concern or of regulatory approaches. The fact that concerns about privacy are higher in some places than others, or that certain managerial practices engender greater concern than do others, should not be used to develop managerial policies, according to some ethical perspectives [11]. While IS managers must draw their own conclusions regarding ethical responsibilities, some responses may make managers vulnerable to criticism from certain ethical camps.

Appendix. Items from privacy survey

Sample items from each subscale are shown here:

Subscale	# Items	Sample Item*
Collection	4	I'm concerned that companies are collecting too much personal information about me.
Secondary Use	4	Companies should not use personal information for any purpose unless it has been authorized by the individuals who provided the information.
Errors	4	Companies should take more steps than they currently take to make sure that the personal information in their files is accurate.
Improper Access	3	Computer databases that contain personal information should be protected from unauthorized access—no matter how much it costs.

In addition, the survey contained some demographic questions. These addressed the respondent's nationality; present job function (external or internal auditor, I/S or financial auditor); present job level (e.g., Executive, Supervisor); total number of years of business experience; gender.

*All items in this table were followed by a 7-point Likert scale anchored by 1 = "Strongly disagree" and 7 = "Strongly agree."

Implications for Public Policy

If IS executives do not choose to proactively confront the privacy management issues in their organizations, it is likely that levels of concern will continue to rise and that citizens will look to their governments for relief. The potential existence of reciprocal relationships between information privacy concerns and regulatory approaches may be useful information for countries grappling with their own public policies toward information privacy.

If levels of concern rise in a given country and if corporate policies and practices are not modified to dampen those concerns, lawmakers may then be forced to move away from the laissez-faire approaches represented by the Self-Help and Voluntary Control models. If future research supports the model tested in this study, it appears that the best path for such countries may be through the more restrictive Licensing and Registration models rather than through the more moderate Data Commissioner model. This should be a sobering finding for executives, as it suggests a threat of strong regulation should management efforts be insufficient. Executives may choose to reject the ethical "hypernorm" argument discussed previously. But the threat of negative impacts on the bottom line, driven by both market forces and the legislative agenda, should be sufficient to prod them toward a more enlightened view of the personal information privacy management domain.

Acknowledgments

The authors gratefully acknowledge the Information Systems Audit and Control Association (ISA & CA) and the Georgetown Center for International Business Education and Research (CIBER) for their support of this research. Dr. Leonardo Epstein offered invaluable assistance with the interpretation of statistical analyses. We also appreciate the very helpful comments of the reviewers and editors.

References

1. Almond, G.A., and Verba, S. *The Civic Culture: Political Attitudes and Democracy in Five Nations.* Princeton University Press, Princeton, NJ, 1963.
2. Bennett, C.J. *Regulating Privacy.* Cornell University Press, Ithaca, NY, 1992.
3. Cespedes, F.V. and Smith, H.J. Database marketing: New rules for policy and practice. *Sloan Management Rev.* (Summer 1993), 7–22.
4. Culnan, M.J. How did they get my name?: An exploratory investigation of consumer attitudes toward secondary information use. *MIS Q.* (Sept. 1993), 341–363.

5. Donaldson, T. and Dunfee, T.W. Toward a unified conception of business ethics: Integrative Social Contracts Theory. *Acad. Manage. Rev. 19*, 2 (1994), 252–284.
6. Engel, J.F., Blackwell, R.D., and Miniard, P.W. *Consumer Behavior.* Dryden, Hinsdale, Ill., 1986.
7. Flaherty, D.H. *Protecting Privacy in Surveillance Societies.* University of North Carolina Press, Chapel Hill, NC, 1989.
8. Hanushek, E.A. and Jackson, J.E. *Statistical Methods for Social Scientists.* Academic Press, Orlando, Fla., 1977.
9. Hofstede, G. *Culture's Consequences: International Differences in Work-Related Values.* Sage, Beverly Hills, Calif., 1980.
10. Hofstede, G. *Cultures and Organizations.* McGraw-Hill, Berkshire, England, 1991.
11. Hume, D. *A Treatise of Human Nature.* Oxford University Press, Oxford, 1888/1978.
12. Ives, B. and Jarvenpaa, S.L. Applications of global information technology: Key issues for management. *MIS Q.* (Mar. 1991), 33–48.
13. Mason, R.O. Four ethical issues of the information age. *MIS Q.* (Mar. 1986), 4–12.
14. Madsen, W. *Handbook of Personal Data Protection.* Macmillan, New York, 1992.
15. Miller, A. Computers and privacy. In W. Hoffman and J.M. Moore, Eds., *Ethics and the Management of Computer Technology.* Oelgeschlager, Gunn and Hain, Cambridge, Mass., 1982, 93–108.
16. Mulder, M. *The Daily Power Game.* Martinus Nijhoff, Leyden, 1977.
17. Smith, H.J. *Managing Privacy: Information Technology and Corporate America.* University of North Carolina Press, Chapel Hill, NC, 1994.
18. Smith, H.J. and Kallman, E.A. *International privacy policies and practices: An exploratory study from an organizational perspective.* Working paper, Georgetown University and Bentley College (1994).
19. Smith, H.J., Milberg, S.J., and Burke, S.J. *Information privacy: Measuring individuals' concerns about corporate practices.* Working paper, Georgetown University (1994).
20. Stone, E.F. and Stone, D.L. Privacy in organizations: Theoretical issues, research findings, and protection mechanisms. *Res. Pers. Hum. Resource Manage. 8* (1990), 349-411.
21. Stone, E.F., Gardner, D.G., Gueutal, H.G., and McClure, S. A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations. *J. Applied Psychol. 68,* 3 (1983), 459–468.
22. Trompenaars, F. *Riding the Waves of Culture: Understanding Diversity in Global Business.* Irwin, New York, 1994.
23. Westin, A. *Privacy and Freedom.* Atheneum, New York, 1967.

About the Authors:
SANDRA J. MILBERG is an assistant professor at Georgetown University. Current research interests include consumer privacy, brand equity, and the roles of affect and cognition in attitude formation and choice behavior. email: milbergs@gunet.georgetown.edu

SANDRA J. BURKE is an assistant professor at Georgetown University. Current research interests include ethical/privacy issues in marketing, consumer information processing and decision-making, and consumer inference use and formation.

H. JEFF SMITH is an assistant professor at Georgetown University. Current research interests include social issues created by the use of emerging technologies, especially information privacy. email: jsmith@guvax.georgetown.edu

Authors' Present Address: Georgetown School of Business, Georgetown University, Old North Hall, Washington, DC 20057.

ERNEST A. KALLMAN is a professor of Computer Information Systems at Bentley College and a research associate at the Bentley College Center for Business Ethics. Current research interests include information privacy, computer ethics, and the management of the information center function. **Author's Present Address:** Bentley College, 175 Forest Street, Waltham, MA 02154; email: ekallman@bentley.edu