Organization Science

Publication details, including instructions for authors and subscription information:
http://pubsonline.informs.org

# Information Privacy: Corporate Management and National Regulation

Sandra J. Milberg, H. Jeff Smith, Sandra J. Burke,

To cite this article:
Sandra J. Milberg, H. Jeff Smith, Sandra J. Burke, (2000) Information Privacy: Corporate Management and National Regulation. Organization Science 11(1):35-57. http://dx.doi.org/10.1287/orsc.11.1.35.12567

# Information Privacy: Corporate Management and National Regulation

Sandra J. Milberg • H. Jeff Smith • Sandra J. Burke
*McDonough School of Business, Georgetown University, Old North Hall, Washington, D.C., 20057, milberg@msb.edu*
*Babcock Graduate School of Management, Wake Forest University, P.O. Box 7569, Winston-Salem, North Carolina 27109, Jeff.Smith@mba.wfu*
*Department of Marketing, Faculty of Economics, University of Sydney, Sydney, Australia NSW 2006, sandrab@econ.usyd.edu.au*



## Abstract

The 1990s have seen a resurgence of interest in information privacy. Public opinion surveys show that many citizens are becoming greatly concerned about threats to their information privacy, with levels of such concern reaching all-time highs. Perhaps as a response to the growing concerns of citizens, the media are devoting more attention to privacy issues, and governmental regulation of the corporate privacy environment is increasing in many countries. Almost all developed countries have grappled with the trade-offs between open access to information—which enables economic efficiency—and an individual's right to privacy. Consistent with these trade-offs, many recent incidents suggest that regulatory approaches to information privacy, corporate management of personal data, and consumer reactions are becoming tightly interwoven around the world. To provide some insights into these relationships, we develop a conceptual model and test it with a cross-cultural sample from 19 different countries.

In general, we find that a country's regulatory approach to the corporate management of information privacy is affected by its cultural values and by individuals' information privacy concerns. In addition, as governments become more involved in the corporate management of information privacy, internal management of such issues seems to tighten. This result supports previous observations that most firms take a primarily reactive approach to managing privacy by waiting for an external threat before crafting cohesive policies that confront their information practices. Moreover, when corporations are not perceived to adequately manage information privacy issues, and/or when privacy concerns rise, individuals are more inclined to prefer government intervention and be distrustful of firm self-regulation. As such, citizens may look to lawmakers to enact stricter regulation to reduce their privacy concerns. These findings and several international trends suggest that the self-regulatory model of privacy governance may not be sustainable over the long term.

Findings from this research constitute an important contribution to the emerging theoretical base of information privacy research and should be particularly enlightening to those managing information privacy issues. Several directions for future research are also discussed.

(*Information Privacy*; *National Regulation*; *Corporate Management*; *Partial Least Squares)*

## Introduction

> Privacy in the modern age has largely been an issue of physical walls—walls that protect our possessions, shield our secrets and provide a haven for lives that are different from our public personas. But the very nature of virtual life seems to rebel against this opacity. . . . Privacy will never be the same.
> (Dunn 1996, p. 1)

The 1990s have seen a resurgence of interest in information privacy—"a condition of limited access to identifiable information about individuals" (Smith 1993, p. 106). Public opinion surveys show that many citizens are becoming greatly concerned about threats to their information privacy, with levels of such concern reaching all-time highs (Equifax 1996; Westin 1997, 1998). A large number of the issues revolve around *corporate* collection, use, and sharing of personal data, which is the subject of this paper.[1]

Within the field of normative ethics,[2] there is substantial debate regarding whether or not a "right to privacy" exists; how such a right is derived philosophically; and the extent to which such a right, if it does exist, is bounded (see, especially, Schoeman 1984). A "right to privacy" has been taken to include a number of "interests"

1047-7039/00/1101/0035/$05.00
1526-5455 electronic ISSN

that converge and diverge. Flaherty (1989) has documented a set of thirteen such interests as they have been observed around the world (see Table 1). Some ethicists have argued for global acceptance of a "right to privacy" that appears to include all the interests in Table 1. Such an argument usually begins with consideration of privacy as a "human right" and draws inferences from that premise (see Schoeman 1984 for an excellent anthology of perspectives, and see Smith 1994 for additional background on this specific philosophical claim). But other observers (see, for example, Posner 1984) strongly dispute this normative perspective. And note that, from a descriptive perspective, these normative views may be quite disconnected from cultures' explicit (e.g., codified in law) and implicit (e.g., exhibited in norms) definitions of a "right to privacy."

In a descriptive sense, then, what determines a society's boundaries on a "right to privacy"? Although rarely acknowledged explicitly, there is some evidence that the fundamental societal tension derives from the inevitable tradeoffs between the 13 interests in Table 1 and the manner in which the society's economic and social systems function (for a narrow consideration of this concept in the privacy domain, see Smith 1994, p. 173; for a broader perspective that extends beyond privacy issues and into other concepts of business ethics, see Vogel 1992). As one example, consider the debate about targeted marketing that is occurring in many countries. While organizations argue that they have the right to conduct business, consumers and privacy advocates often claim the right to be free of unwanted solicitations. While organizations claim the right to use information technology to improve efficiency, consumers often exhibit the desire to control the flow and dissemination of their personal information. While businesses claim the right to record information generated from their transactions, consumers increasingly want to know that this information has been gathered and stored and to control its uses (Goodwin 1991). Thus, the trade-off between the benefits that accrue from marketers' use of personal information and consumer rights to information privacy must be recognized (Milne and Gordon 1993).

**Table 1 Privacy Interests of Individuals**

According to Flaherty (1989), individuals can assert privacy interests in information about themselves in the right to:

- Individual autonomy
- Be left alone
- A private life
- Control information about oneself
- Limit accessibility
- Exclusive control of access to private realms
- Minimize intrusiveness
- Expect of confidentiality
- Enjoy solitude
- Enjoy intimacy
- Enjoy anonymity
- Enjoy reserve
- Secrecy

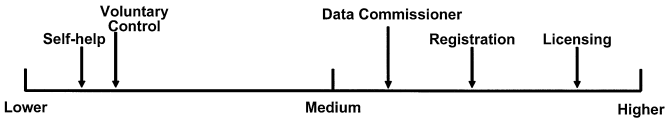
*Source:* Adapted from Flaherty (1989, p. 8)

It is not our intention in to resolve the debates between these various parties. We note these disputes only because of their substantive *impact:* in order to manage the competing trade-offs, some societal mechanism must be in place. The most common approach, over the last 30 years, has been a societal embrace of one or more regulatory models that toggle between an acceptance of managerial self-regulation and a governmental imposition of control on corporations.

More specifically, an analysis of the forms of information privacy governance around the world reveals a broad continuum of approaches. As can be seen in Figure 1, the approaches vary significantly in terms of governmental involvement in day-to-day corporate operations (Bennett 1992, Flaherty 1989, Milberg et al. 1995, Regan 1995, Smith 1994). At the low government involvement side (left end) of the continuum—the position embraced to date by the United States and, to a slightly lesser extent, Japan—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—of which Sweden is the most prominent example—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. While not absolute, it can be inferred that privacy debates on the left end of the continuum will normally be resolved more by market forces; on the right end, more by regulatory oversight.[3]

While there is a broad divergence of approaches to the governance of information privacy, as illustrated in Figure 1, a trend of increased governmental regulation of the corporate privacy environment is developing in many countries (Dresner 1996a, Franklin 1996, Hendricks 1998b). This response seems to be associated with the growing privacy concerns of citizens regarding corporate information practices and with the media coverage of these practices. Against this backdrop, governments and citizens are calling for increased organizational aware-

**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 ensure compliance.

3) The Data Commissioner Model 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 legislature, press, and the public.

4) The Registration Model creates a requirement that each data bank containing personal data be *registered* (usually upon payment of a fee) *by a separate governmental institution.* Although the data banks must be registered, the governmental 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 data bank containing personal data be licensed (usually, upon payment of a fee) by a separate governmental 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 a *prior* approval for any use of data.

*Notes:* *Adapted from Milberg et al. (1995) and Smith (1994); categories based on Bennett (1992).

ness to privacy issues—as well as for increased leadership from corporate managers (for example, see Cespedes and Smith 1993; Culnan 1993; Kallman and Grillo 1996; Mason et al. 1995; Oz 1994; Smith 1993, 1994). These trends and recent incidents seem to suggest that privacy regulation, corporate management of personal data, and consumer reactions are tightly interwoven around the world. Consider the following examples:

• In *Australia* in 1996, a survey of 120 large businesses, conducted by Price Waterhouse, showed that two-thirds of respondents favored the extension of the country's Privacy Act to the private sector. (The Privacy Act had covered public sector activities since 1988.) (Dresner 1996b). However, by March 1997, the Australian Prime Minister, John Howard, had announced that the Privacy Act would not be extended due to the "increase in compliance costs for all Australian businesses." This position struck many as unfounded, and it appears that a battle is coming soon in Australia (Colman 1997).

• In *Belgium* in 1995, legalized prohibitions on reuse of personal data led to a judgment against the major financial institution Kredietbank. Some of Kredietbank's customers made their insurance payments through Kredietbank, and Kredietbank analyzed their payment orders. It was able to determine the exact amounts of the contributions as well as the insurer to which payment was made. Since Kredietbank was beginning to sell its own insurance services, it was in a privileged position to contact the customers and offer them a better insurance deal. A judge ruled against Kredietbank's using the data in this manner, citing Belgium's 1992 law for the Protection of Personal Privacy in the Area of Personal Data Processing (Blas 1995).

• In 1996, *Sweden's* national telephone company, Telia,[4] as required by law, applied to the federal Data Inspection Board (DIB) for permission to create a massive new database that would include the names and addresses of all telephone subscribers in Sweden along with personal data from the Motor Vehicle Register, National Land Register, Patent and Registration Office, and a federal census-related register known as Statistics Sweden. The stated purpose of the new database was direct mail advertising, market research, and telemarketing. The DIB denied the request, although an appeals procedure is still available to Telia. The merging of private with public data was particularly troubling to the Director General of the DIB, who stated ". . . there is reason to believe that the commercial profit looks so attractive as to make [many involved] blind to the violation of privacy involved. . ." (Bondestam 1996, p. 9).

• In the *United States,* it was reported in February 1998 in the *Washington Post* that two Washington-area drug store chains, Giant and CVS, were sharing customer prescription records with a drug marketing firm (O'Harrow 1998a). Faced with an enormous public backlash, within days both Giant (1998) and CVS (1998) had run full-page ads in which they promised to discontinue the practice. But the revelation apparently led to a quickly passed bill in the Virginia legislature and provided additional support for a federal bill that had already been introduced (O'Harrow 1998b, 1998c).

As these incidents illustrate, governmental actions, corporate practices and consumer responses are inextricably connected. However, our understanding of these interre-

lationships is somewhat limited and based primarily on anecdotal evidence. Therefore, in this study we examine some internal factors that influence and are influenced by the information privacy regulatory and corporate management environments.[5] More specifically, we examine internal factors that influence a society's approach to the governance of corporate information privacy practices, how a society's regulatory approach influences the corporate management of information privacy, and how the corporate management environment, in turn, affects citizens' preferences for different regulatory approaches. Based on our findings and some trends in the external environment, we discuss the sustainability of the forms of governance for information privacy.

In the sections to follow, we first discuss several information privacy challenges to corporations operating in an international environment. Next, we develop and explain a theoretical model that links corporate privacy management practices with individuals' concerns about privacy and regulatory options. We then provide details of our study's methodology and results. We conclude with a discussion of the findings and their implications for both corporate management of privacy and governments' regulation thereof. Findings from this research should be particularly enlightening to those managing privacy issues in an international environment, since organizations are facing an increasing number of challenges in this regard.

### Corporate Information Privacy Challenges in an International Environment

Corporations are coming under increasing pressure to consider the implications of managing personal data. Consideration of information privacy issues must increasingly be in an international context, as people in 240 of 250 countries are now connected to the Internet (AP 1998). There are a number of factors contributing to the international challenges of privacy management. In particular, the challenges associated with transborder exchanges of data (Samiee 1984), although somewhat muted during much of the 1980s (Kane and Ricks 1988), are likely to increase as the European Union (EU) implements its Privacy Directive from late 1998 to 2000. This directive will codify a consistent set of privacy laws that mandates "fair information practices" for EU members. These include the right to see and correct virtually any personal data, and the requirement that companies "fairly obtain" information, meaning that they must notify individuals of intended uses and gain consent for the release of data for other purposes. The EU Privacy Directive is resulting in pressure on non-EU countries to adopt more stringent privacy laws or face restrictions in transporting data out of the EU to countries deemed to have inadequate privacy laws (Dresner 1996a, Hendricks 1998b). Several countries' regulatory statutes, such as those in the United States and Japan, lack adequate privacy protection by the standards set forth in the EU Privacy Directive and, therefore, may be adversely affected by its restrictions.

In addition to legislative threats, several other factors add to the international privacy challenges. First, perceptions of privacy differ across cultures. While all cultures value intimacy in some form, the lines between public and private behavior are drawn quite differently, not only in the Western and non-Western tradition but even between different sectors of the same country (Flaherty 1972, Westin 1967). Second, countries exhibit different sets of cultural values (Hofstede 1991), and these values become intertwined with different privacy regulatory approaches (Milberg et al. 1995).

Third, perceptions regarding ethical and unethical behavior, and how those ethical perceptions are enforced in a social sense, are known to vary across cultures (Dubinsky et al. 1991, Langlois 1993, Langlois and Schlegelmilch 1990). Protection of privacy is considered one of the most important "ethical issues of the information age" (Mason 1986, p. 4) and is increasingly being viewed as an international "human rights" issue (Smith 1994). Therefore, managers confronting privacy issues may increasingly find themselves grappling with cross-cultural ethical quandaries.

Fourth, at an operational level, the development and implementation of international information systems is becoming increasingly complex, partially because of constraints surrounding the collection and transfer of personal data (Ives and Jarvenpaa 1991). Managers attempting to gain strategic advantage through creative uses of such systems (Cash et al. 1992) may soon find themselves frustrated by differing expectations regarding privacy in different societies around the world.

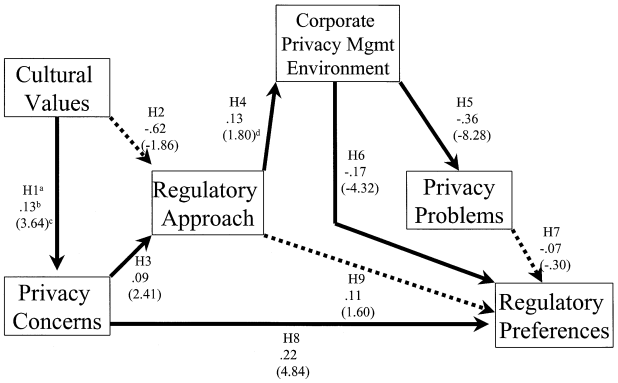
## Conceptual Framework and Hypotheses

We develop a conceptual framework that considers the dynamic interrelationships among some key factors considered to be most salient based on current research and theory (see Figure 2). In the following sections, we describe each of the components of the proposed model and develop hypotheses regarding their associations.

### Cultural Values

Values are group norms or shared beliefs that have been internalized by individuals (Engel et al. 1986). Research has shown that values differ to some degree across countries and influence a society's responses to the environ-

**Figure 2 Conceptual Framework**




[a] "H" notations refer to hypotheses from the text.
[b] Standardized coefficients.
[c] T-values are shown in parentheses; paths denoted by solid lines are significant at p<.05 or better, unless noted otherwise.
[d] H4 path is significant at p<.05, directional test. A directional test is acceptable, as the direction of the relationship was hypothesized a priori.

ment. For example, it has been shown that cultural values affect the development and maintenance of social institutions, including political and legislative bodies (Hofstede 1991). Such values may also be associated with individual privacy concerns.

### Individual Privacy Concerns

Privacy is hardly a unidimensional construct. In a previous study, Smith et al. (1996) examined the numerous factors that have been claimed to be components of the privacy construct by academic writers, privacy advocates, and/or corporate managers. They then completed an exhaustive exercise, using 15 different samples from various populations, to ascertain which of the factors actually comprised the construct "individuals' concerns about organizational practices in managing information privacy." They identified four dimensions of that construct and created a 15-item instrument—used in this study—that measures individuals' levels of concern for each factor. The four factors are: collection, unauthorized secondary use, improper access, and errors.

*Collection.* This area of concern reflects the perception that "There's too much damn data collection going on in this society" (Miller 1982, p. 96). Individuals often perceive that great quantities of data regarding their personalities, background, and actions are being accumulated, and they often resent this.

*Unauthorized Secondary Use.* Sometimes, information is collected from individuals for one purpose but is used for another, secondary purpose without authorization from the individuals. Even if contained *internally* within a single organization, unauthorized use of personal information will very often elicit a negative response. Specific examples of such secondary, internal uses are also covered in the literature: for example, "sugging"—a practice in which data are collected ostensibly for research only to be used later for marketing purposes—falls into this area of concern (Cespedes and Smith 1993). Some studies (for example, Tolchinsky et al. (1981)) have found that concerns about secondary use are exacerbated when personal information is disclosed *externally* to a third party (i.e., another organization). The most commonly cited examples of this concern are the sale or rental of current or prospective customers' names, addresses, phone numbers, purchase histories, categorizations, etc., on mailing "lists," which are often transferred between the organizational entities as digital files.

*Improper Access.* Who within an organization is allowed to access personal information in the files? This is a question not only of technological constraints (e.g., access control software) but also of organizational policy. It is often held that individuals should have a "need to know" before access to personal information is granted. However, the interpretation of which individuals have, and do not have, a "need to know" is often a cause of much controversy.

*Errors.* Many individuals believe that organizations are not taking enough steps to minimize problems from errors in personal data. Although some errors might be *deliberate* (e.g., a disgruntled employee maliciously falsifying data), most privacy-related concerns involve instead *accidental* errors in personal data. Provisions for inspection and correction are often considered as antidotes for problems of erroneous data (HEW 1973, PPSC 1977, Smith 1994). But many errors are stubborn ones, and they seem to snowball in spite of such provisions (Smith 1994). In addition, a reluctance to delete old data—which can clearly become "erroneous" because of their static nature in a dynamic world—can exacerbate this problem (Miller 1982). Also at issue are questions of responsibility in spotting errors: does a system rely on individuals to monitor their own files, or is there an overarching infrastructure in place (Bennett 1992)? Although errors are sometimes assumed to be unavoidable, problems in data handling, whether controls are or are not included in a system, does represent a value choice on the part of the system's designers (Kling 1978, Mowshowitz 1976).

*Privacy Concerns in Context.* Milberg et al. (1995) found that the hierarchy of concerns—that is, how levels of concern about the above dimensions are rank ordered—is surprisingly consistent across cultures, with unauthorized secondary use almost always reported to be of the most concern. Privacy concerns have been shown to "stem from a variety of factors, including the individual's previous learning, cultural milieu, and physiological

reactivity" (Stone and Stone 1990, p. 386). Consistent with this, associations between both country and individual level traits and information privacy concerns have been found (Milberg et al. 1995, Stone and Stone 1990). For example, individuals in different countries exhibit different levels of concern about the management of information privacy (Milberg et al. 1995).

Prior research has also shown positive associations between individual personality traits, such as levels of trust and social criticism, and information privacy concerns (Smith et al. 1996). Because "culture is to a human collectivity what personality is to an individual" (Hofstede 1980, p. 25), cultural values may likely be associated with differences in consumer information privacy concerns as well. In particular, this should be true for four cultural values identified by Hofstede (1980, 1991): individualism/collectivism (IND), masculinity/femininity (MAS), power distance (PDI), and uncertainty avoidance (UAI). The IND value index measures an individual's independence/dependence on organizations. The extent to which a society values "assertiveness, the acquisition of money and things, and *not* caring for others, the quality of life, or people," (Hofstede 1980, p. 46) is measured by the MAS index. The PDI measures the degree to which a society accepts inequality in institutional power between a less powerful individual and a more powerful other. The extent to which individuals in a society feel threatened by uncertain and ambiguous situations is measured by the UAI (Hofstede 1980, 1991).

Earlier research suggested associations between cultural values and levels of consumer information privacy concern (Milberg et al. 1995). Specifically, Milberg et al. (1995) proposed that citizens in high "individualism" countries would exhibit higher levels of concern for information privacy. They based their assertion on prior work that found that a societal norm associated with countries that strongly value individualism is the belief that everyone has the right to a private life, while in countries for which individualism is of lower importance there is more of an acceptance of organizational practices that will intrude on one's private life (Hofstede 1980, 1991). Additionally, Milberg et al. (1995) proposed that since high scores on the UAI have been found to be associated with high levels of anxiety, stress, and concern for security, concerns for privacy may also be positively related. Finally, they suggested PDI should be positively associated with information privacy concerns based on previous findings that high PDI countries exhibit lower levels of trust (Hofstede 1991) and that there is a positive association between interpersonal distrust and concerns for personal privacy (Smith et al. 1996). However, Milberg et al. (1995) found no support for these associations. One possible explanation may have been the use of a limited set of cultural values and countries. Since we use a larger set of countries and an additional cultural value, i.e., MAS, the relationships between cultural values and consumer information privacy concerns is incorporated in our framework. Thus, we hypothesize the following:

HYPOTHESIS 1. *Cross-cultural values will be associated with differences in levels of information privacy concerns.*

**Regulatory Approaches**

What are some of the factors that influence a society's means of governance? Previous research has suggested that cultural values influence a society's responses to the environment through the development and maintenance of social institutions (Hofstede 1991). Thus, differences in political systems and legislation in various countries can be interpreted as consequences of societal value differences and the degree to which members of a society look to the government to remedy social issues (Milberg et al. 1995). With respect to the information privacy environment, previous work has shown associations between cultural values and regulatory approaches to information privacy (Milberg et al. 1995). For example, countries high in uncertainty avoidance have been shown to vigorously embrace legislative solutions in general (Hofstede 1991) and in particular to regulating information privacy (Milberg et al. 1995). However, countries that strongly value individualism tend to desire fewer organizational and governmental rules and regulations in general and with respect to managing information privacy (Milberg et al. 1995). Thus, when developing a framework of the information privacy environment, the link between cultural values and regulatory approaches must be considered. Therefore, we hypothesize:

HYPOTHESIS 2. *Cross-cultural values will be associated with differences in levels of government involvement in corporate privacy management.*

Many writers have suggested that a country's regulatory approach to privacy is also, to a great degree, a function of the level of privacy concern and discontentment in that country (Bennett 1992, Flaherty 1989, Smith 1994). As privacy concerns among the populace increase, a natural reaction among legislators is to put in place more restrictive structures. Milberg et al. (1995) found support for this positive association between the level of privacy concern and the level of governmental involvement in corporate management of information privacy. Thus,

HYPOTHESIS 3. *Higher levels of concern for information privacy will be associated with higher levels of government involvement in corporate privacy management.*

**Corporate Privacy Environment**

Corporate privacy management processes encompass, at a rudimentary level, several important areas, such as the level in the organization at which privacy issues are managed, official information privacy policies, the management of these policies through day-to-day practices, and the importance of privacy issues to management (Mintzberg 1973, Simon 1976, Smith 1994). For several reasons, it is expected that a relationship exists between different approaches to privacy regulation and the approaches that companies take toward privacy management in their internal operations.

In previous U.S.-based research, corporate privacy policy making and management have appeared primarily reactive in nature. Corporate privacy policies have tended to "drift" until confronted by an external "threat"—very often, in the form of regulation—at which time corporations react with tighter, more formalized policies and direct greater attention to the management of actual practices across the organization (Smith 1993, 1994). It would be expected, then, that a corporation's privacy management processes would vary according to the regulatory "threats" that it perceived—which are dependent on the regulatory structures under which a country operates. Note also that privacy policies can be either explicit or implicit, and the practices may or may not match them:

> Explicit policies provide an official focal point for the entire organization and, subject to the communication of the policies, a valid reference for decision making. Thus, explicit policies will generally be codified in a written form and will have been approved by a senior executive. Implicit policies, less formal than explicit ones, serve a useful purpose in moving the organization toward a particular goal; however, they may not be as easily communicated, and they can be more difficult to enforce . . . in some situations, neither explicit nor implicit policies exist; in those cases, though, practices are still evident (Smith 1994, p. 96).

If the U.S.-based observations of corporate reactivity hold elsewhere, corporations in countries with higher levels of governmental involvement in corporate privacy management should react to regulation by devoting more attention to the development of adequate, explicit privacy policies and to an internal structure that ensures consistency between those policies and actual practices across the corporation. Most commonly, this internal structure will include the placement of management responsibility for privacy issues at a high level in the organization (Cespedes and Smith 1993, Kallman and Grillo 1996, Smith 1994).

Organizations also mirror the values and attitudes of their key executives as they set strategic direction (Porter 1980), develop policies (Porter 1980, Selznick 1957, Simon 1976), and manage those policies through their day-to-day implementation (Cyert and March 1963, Mintzberg 1973, Simon 1976). It has been argued that a company's approach to value-laden ethical issues is a "moral projection" of its executives' perspectives (Goodpaster and Matthews 1982). In a given corporation senior manages could place a high priority on privacy issues or could view such issues as being of much less importance. Based on the discussion above, we hypothesize:

HYPOTHESIS 4. *In countries with higher levels of government involvement in corporate privacy management, a) organizational privacy policies will be perceived as more adequate; b) there will be a more positive perception of the match between official policies and actual practices; c) corporate privacy management will occur at a higher level in organizations, and d) privacy will be perceived as more important to senior managers.*

We further note that specific problems associated with information privacy are more likely in organizations with looser (less adequate) privacy management than in those with tighter management. ("Tighter" management processes constitute those consistent with the policies and practices for managing privacy as were described in Hypothesis 4). In particular, based on the work of Smith (1994) and Smith et al. (1996), some specific problems often emerge in organizations that are "drifting" in their privacy management processes: for example, excessive errors in data with inadequate correction processes, sloppy handling of personal information, and inadequate access controls for personal data. Thus, we hypothesize:

HYPOTHESIS 5. *In organizations with tighter privacy management processes, fewer information privacy-related problems will prevail than in organizations with looser processes.*

**Regulatory Preferences**

To the extent that a country's regulatory structure reflects the desires of its populace (Bennett 1992, Flaherty 1989, Milberg et al. 1995, Regan 1995), it is instructive to consider the factors that may influence preferences for increased government regulation. Bennett (1992), Flaherty (1989), and Smith (1994) contend that regulatory structures are to a great extent *reactions* to conditions within a country's data-processing structures. For example, Swe-

den—which utilizes ten-digit "birth numbers" for each individual and has a tradition of strenuous record keeping and computerization at almost all levels of society—also has one of the highest levels of governmental involvement in corporate privacy management to be found in the world. Such an extensive level of privacy regulation can plausibly be viewed as a reaction to the data-processing environment in the country (Flaherty 1989).

It is becoming increasingly apparent that perceptions of how well corporations manage privacy drive desires for government intervention. Public opinion polls (Equifax 1990, 1993, 1996; Equifax Canada 1992) and psychological research (see review in Stone and Stone 1990) strongly suggest that consumers' perceptions of data handling in different industries impact their propensity to complain about privacy-related matters and to demand additional governmental involvement. If one perceives that current corporate approaches to handling consumer data are sufficiently tight, one will be less inclined to call for more government regulation and be more willing to rely on corporate self-regulation. However, if one perceives inadequacies in existing approaches, one will adopt the opposite position. Thus,

HYPOTHESIS 6. *Tighter management of corporate privacy will be associated with less preference for strong laws in regulating privacy and greater preference for corporate self-management.*

We also consider the relationship between the number of information privacy-related problems in the organization and regulatory preferences. Theoretical development in this area is weak, but an exploratory hypothesis can be constructed based on an intuitive argument: Since small numbers of problems should be reflective of a tighter management environment, it seems plausible to suggest that the number of problems in an organization should also be associated with privacy regulation preferences. Furthermore, as suggested by Bennett (1992), calls for additional regulation may be grounded in specific observations of privacy problems in a corporate environment. We therefore state this *exploratory* hypothesis:

HYPOTHESIS 7. *Fewer privacy problems in the corporate environment will be associated with less preference for strong laws in regulating privacy and greater preference for corporate self-management.*

In addition, across broad portions of the continuum (see Figure 1), higher levels of privacy concern in a country are associated with higher levels of governmental involvement in corporate privacy management (Milberg et al. 1995). Moreover, some public opinion surveys (see, especially, Equifax 1991, 1992) have suggested that individuals with higher concerns about privacy are more likely to call for stronger privacy laws. A similar finding was observed by Stone et al. (1983), and some anecdotal support was found by Smith (1994). We therefore state:

HYPOTHESIS 8. *A high level of personal concern for information privacy will be associated with greater preference for strong laws in regulating privacy and less preference for corporate self-management.*

Previous research has shown that in many contexts individuals will use existing information to form opinions and attitudes about future or uncertain phenomena. For example, Tversky and Kahneman (1981) suggest that prior to evaluations, alternatives in a choice set are framed as positive or negative deviations from an identified "neutral" reference point such as the status quo. Additionally, individuals will use "reference points" derived from environmental cues and observations to assess specific evaluative data such as product pricing (see Mayhew and Winer 1992 for review) and missing information (Ross and Creyer 1992). This general behavioral tendency to look to the environment, given information, or the status quo to set an anchor or reference point in forming judgments should also apply to the formation of information privacy regulatory preferences. Specifically, current information on privacy regulatory approaches in a country is likely to affect individuals' preferences for the type of regulatory approach they would like to see enacted. Thus, the following hypothesis is posited:

HYPOTHESIS 9. *Higher levels of current governmental involvement in corporate privacy management will be associated with greater preference for strong laws in regulating privacy and less preference for corporate self-management.*

## Method

### Sample and Procedure

The Information Systems Audit and Control Association (ISACA), an international organization of information systems (I/S) and financial auditing professionals, sponsored a study of its members. Since ISACA members are regularly involved in the examination of policies and procedures in computerized environs, they offered a well-informed perspective on the collection, use, and protection of consumer data.

In spring 1993, presidents of all 120 ISACA chapters received a cover letter from the ISACA executive director asking for their cooperation in the study. Enclosed with the letter were a set of procedures for administering the survey, questionnaires, and a return sheet. The procedures

requested that the president distribute the surveys at a regular ISACA meeting, have the members complete the surveys while at the meeting, and collect the surveys for return to the ISACA office. Although the ISACA organization offered the option to all 120 chapters, the decision of whether or not to participate was made by each local chapter's officers; 63 chapters did participate, leading to a *chapter* response rate of 52.5%. Chapter presidents were asked to return a control sheet to the researchers indicating the conditions of the questionnaire administration.

The researchers received a total of 595 usable surveys from *internal* auditors (responsible for auditing systems in their *own* organizations) of 25 different nationalities (self-reported) in these 63 chapters.[6] Respondents were 70% men and 26% women (4% did not answer a gender question) who occupied various levels in their organizations: 4% executive level, 37% director/manager level, 26% at the level of supervisor or project leader, and 27% at the nonmanager level (6% either left the question blank or provided a noninterpretable response). They had worked an average of 7.6 years for their present employer, had an average of 8.9 years of audit experience, and had an average of 16.4 total years of business experience. Respondents worked in a variety of industries: 36% banking, 13% government, 11% insurance, 10% financial, 10% manufacturing, 6% utilities, 3% education, 2% retail, and 9% other (industries in the "other" category represent less than 2% of respondents).[7]

### Questionnaire Development

The written survey solicited the ISACA members' perceptions of the information privacy management environment in their corporation, regulatory preferences, concerns about privacy, and accounts of privacy problem areas in their firm (see relevant items in the Appendix). The survey was developed from materials previously validated in earlier studies. In addition, two items were developed, in conjunction with ISACA officers and members, to examine senior management attitudes toward information privacy and accountability for privacy management. ISACA officers, the ISACA Research Board, and selected ISACA members tested the survey to ensure it was clear and easy to answer.

Since there were ISACA chapters in most regions of the world, it was deemed important to take reasonable steps to insure the respondents' ability to understand the questions and to minimize any confusions that might be caused by terminology, technical expressions, or other factors. ISACA headquarters indicated that all meetings worldwide were conducted in English and that all members were well-educated professionals. Hence, we felt confident that satisfactory results could be achieved by administering the questionnaire in English.

To test the questionnaire for international acceptance, we asked various constituencies to complete the instrument and comment on any questions or difficulties. Those asked included colleagues and friends of foreign origin, international college and graduate students, college professors familiar with a foreign culture not their own, teachers of foreign languages and cultures, and foreign businesspeople and other professionals contacted through third parties. The countries and numbers of testers were as follows: China (2), Finland (1), France (5), Germany (1), India (5), Italy (2), Japan (5), Russia (1), Thailand (1). The overwhelming response was that, with a few minor changes, the questionnaire was clear and understandable and that a business professional could certainly answer it with ease.

### Measures

Several measures were required to evaluate the hypotheses. In particular, measures of 1) the corporate privacy management environment, 2) corporate information privacy-related problems, 3) preferences regarding information privacy regulation, 4) individual concerns about information privacy, 5) existing approaches to information privacy regulation (by country), and 6) cultural values were obtained.

To assess *the corporate privacy management environment,* several measures based on prior research (Smith 1994) were used. Specifically, subjects responded to questions concerning corporate policies and practices, senior management attitudes, and the title of the person responsible for managing information privacy. Subjects indicated, on two seven-point scales, the adequacy of their organization's official policies for handling sensitive personal data (1 = not very adequate, 7 = very adequate) and how well the actual practices and operations in their organization match the official policies regarding the handling of sensitive personal information (1 = very poor match, 7 = very good match) (see § III, items 2 and 3 in the Appendix). In addition, to measure senior managers' attitudes toward information privacy, subjects indicated, on a seven-point scale, "how important to the senior management of your organization is information privacy" (1 = not important at all, 7 = very important) (see item 4 in § III in the Appendix). Further, subjects indicated the title of the person accountable for managing privacy issues in the organization (see item 5 in § III of the Appendix). The levels of the accountable individuals were coded into three categories: executive (e.g., CEO/EVP/VP), management (e.g., manager/supervisor), and nonmanagement (e.g., staff).

To measure the *extent to which information privacy problems exist within the corporate environment* a list of four information privacy problem areas that have been found to emerge in organizations that are lacking in their management processes (Smith 1994) and that reflect dimensions of privacy concerns identified by Smith et al. (1996) were presented to subjects. Respondents placed a check mark next to each of the following items that, in their judgment, was a cause of problems with information privacy in their own organization: the kinds of information stored in databases, error detection with inadequate correction processes, sloppy handling of personal information, inadequate access controls for personal data (see item 6 in § III of the Appendix). The number of checked items was summed to form an index.

*Preferences for regulation of information privacy* were assessed by asking subjects the extent to which they agreed or disagreed (1 = strongly disagree, 7 = strongly agree) with each of the following statements: "the best way to protect personal privacy would be through strong laws," and "the best way to protect personal privacy would be through corporate policies, which the corporations would develop themselves" (corporate self-management). (See § II of the Appendix.) The *difference* between these two measures (preference ratings for strong laws *minus* preference ratings for corporate self-management) was used to indicate the degree to which respondents preferred government regulation over corporate self-management.

Measurements of *personal information privacy concerns* were obtained using a validated instrument containing 15 items on seven-point Likert scales (Smith et al. 1996). This instrument measures personal information privacy concerns about four dimensions: "collection," "secondary use," "errors," and "improper access" (see sample items in § I of the Appendix).

To measure *information privacy regulatory approaches,* each of the relevant countries' existing formal regulatory policies were coded according to the regulatory "model" (see Figure 1) that it matched most closely.[8] Specifically, two judges, blind to the purposes of the study, were given extensive descriptions of information privacy regulatory models as shown in Figure 1. These descriptions were used as the classification codes. In addition, the judges were provided with extensive descriptions of each country's existing information privacy regulations from Dresner (1996a) and Franklin (1996). The judges indicated on seven-point scales the degree to which each regulatory model (see Figure 1) was reflected in the Dresner (1996a) and Franklin (1996) descriptions of a country's information privacy policies. They then classified each country according to which of the five regulatory models best reflected the written policies in that country as of March 1993. In addition, a classification for "no formal information privacy regulation" was available to the judges as a classification option. The interjudge reliability of the coding was 0.88 with disagreements being reconciled by a third independent judge and by the study's authors. Results of the coding process can be seen in Table 2.

Finally, four *cross-cultural value indices* developed and validated by Hofstede (1980,1991)—individualism/collectivism (IND), masculinity/femininity (MAS), power distance (PDI), and uncertainty avoidance (UAI)—were used as measures of cultural values for the countries in this study. The value indices range from 0 to 120. In our sample of countries, the IND scores ranged from 20 in Thailand to 91 in the U.S.; the MAS scores ranged from 14 in the Netherlands to 95 in Japan; the PDI scores ranged form 18 in Denmark to 104 in Malaysia; and the UAI scores ranged from 23 in Denmark to 94 in Belgium.

**Table 2 Country Classifications**

| Classification | Countries |
|---|---|
| No *formal* information privacy regulation[a] | Argentina<br>Italy<br>India<br>Malaysia<br>Thailand |
| Self-Help (Model 1) | None |
| Voluntary Control (Model 2) | Japan<br>United States |
| Data Commissioner (Model 3) | Australia<br>Canada<br>Finland<br>Germany<br>New Zealand<br>Switzerland |
| Registration (Model 4) | Belgium<br>Denmark<br>France<br>Netherlands<br>U.K./England/Scotland |
| Licensing (Model 5) | Norway |

*Note:* [a]Classifications in this table are based on the country's codified laws, as detailed in the text. It is possible, of course, that some uncodified norms for data collection and use could also exist in the society. However, evaluation of such norms is beyond the scope of the present study.

## Results

### Method of Analysis

To test the hypothesized associations and proposed framework, the Partial Least Squares method of structural equation modeling was employed using Lohmoller's (1981) Partial Least Squares (PLS) algorithm. PLS is a structural equation method for estimating systems of causal relationships among observable and unobservable variables. Estimation is based on Ordinary Least Squares (OLS) fixed point iterations on subsets of model parameters (Fornell and Larcker 1981), thus requiring few distributional assumptions. PLS is more appropriate than maximum likelihood structural equation methods like LISREL and its derivatives when the goal of the research is *prediction* or when assumptions regarding multivariate normality of the data might not hold (Fornell and Bookstein 1982). The model being tested in this study involves staged causal variables, latent variables (e.g. the privacy concern variable with 15 measures), and categorical variables (e.g. regulatory approach). Given these *data assumptions* and the *predictive objectives* of this study, PLS is an appropriate estimation method that accommodates the data requirements, provides error specification for latent variables and experiment-wise error, and predicts point estimates of variables.

### Measurement

Composite reliability (internal consistency) considers the ratio of nonrandom variation associated with all measures of a construct to total variation associated with all these measures. The composite reliabilities for the information privacy concerns and the corporate privacy management environment constructs were all above 0.80 (see Table 3), which meets Nunnally's (1978) guidelines. The average variance extracted (AVE) is the amount of variance captured by the construct in relation to the amount of variance attributed to measurement error. AVEs in the constructs were all over 0.50 (see Table 3), which is the rule of thumb for the adequacy of this measure (Bagozzi and Yi 1988) and is indicative of convergent validity. Discriminant validity was demonstrated in that the variance shared between constructs (squared correlation) was less than the average variance extracted by the constructs. Further, an examination of latent variable correlations (see Table 4) showed that they were all significantly different from one ($p < 0.05$). These psychometric properties are sufficiently strong to enable interpretation of structural parameters.

### Tests of Hypotheses

The results of the PLS estimation are illustrated in Figure 2. The significance of path coefficient estimates was assessed using PLS jackknifing (Fornell and Barclay 1983). The estimation provides some support for eight of the nine hypotheses.

*Effects of Cultural Values.* As hypothesized (Hypothesis 1), cultural values are associated with differences in levels of consumer information privacy concerns (coefficient = 0.13, t = 3.64, $p < 0.01$). Specifically, the value dimensions of power distance, individualism, and masculinity each have a positive effect (weights = 0.31, 0.56, 0.77, respectively) on the overall level of information privacy concerns, whereas the uncertainty avoidance value dimension has a negative relationship (weight = −0.37) with the level of privacy concerns.

As hypothesized (Hypothesis 2), cultural values are also associated with differences in regulatory approaches, albeit at a marginal level of significance (coefficient = −0.62, t = −1.86, $p < 0.09$). In particular, the value dimensions of power distance, individualism, and masculinity each are negatively associated with the levels of government involvement in the regulation of information privacy practices. However, the uncertainty avoidance value dimension has a positive relationship with the level of government involvement in information privacy regulation.[9]

*Effects of Privacy Concerns.* In support of Hypothesis 3, privacy concerns have a significant effect on regulatory approaches (coefficient = 0.09, t = 2.41, $p < 0.02$), such that higher levels of concern are associated with more restrictive regulatory approaches. Privacy concerns also have a significant, positive effect on regulatory preferences (Hypothesis 8) (coefficient = 0.22, t = 4.84, $p < 0.001$), suggesting that high levels of personal concern for information privacy are associated with higher preferences for strong laws over corporate self-management.

*Effects of Regulatory Approach.* In support of Hypotheses 4 and 9 respectively, regulatory approach has some effect on both the corporate privacy environment and regulatory preferences. Specifically, regulatory approach has a positive significant effect (coefficient = 0.13, t = 1.80, $p < 0.05$) on the corporate privacy environment which is defined/measured as an explanatory combination of the indicators: 1) adequacy of corporate privacy policy, 2) the match between official policies and actual corporate practices, 3) importance of the privacy issue to senior management, and 4) the job level of the person responsible for privacy management. All four of these indicators load positively on the corporate privacy environment construct (loadings = 0.83 for adequacy, 0.84 for match, 0.74 for management attitudes, and 0.33 for management level). Thus, the results suggest that when there is more government involvement in the regulation of corporate information privacy practices, percep-

**Table 3 Multiple-Item Construct Loadings**

| Construct | Item | Loading | AVE | CR |
|---|---|---|---|---|
| Cultural Values[a] | IND | 0.31 | | |
| | MAS | 0.56 | | |
| | PDI | 0.77 | | |
| | UAI | −0.37 | | |
| Privacy Concerns[b] | Collection | | 0.61 | 0.88 |
| | COLL1 | 0.65 | | |
| | COLL2 | 0.55 | | |
| | COLL3 | 0.96 | | |
| | COLL4 | 0.64 | | |
| | Errors | | 0.60 | 0.85 |
| | ERR1 | 0.64 | | |
| | ERR2 | 0.81 | | |
| | ERR3 | 0.70 | | |
| | ERR4 | 0.86 | | |
| | Unauthorized Secondary Use | | 0.52 | 0.83 |
| | SEC1 | 0.69 | | |
| | SEC2 | 0.61 | | |
| | SEC3 | 0.67 | | |
| | SEC4 | 0.89 | | |
| | Improper Access | | 0.55 | 0.81 |
| | ACC1 | 0.72 | | |
| | ACC2 | 0.75 | | |
| | ACC3 | 0.83 | | |
| Corporate Privacy Management Environment | | | 0.56 | 0.80 |
| | Policy Adequacy | 0.83 | | |
| | Policy-Practice Match | 0.84 | | |
| | Senior Management Attitudes | 0.74 | | |
| | Level of Responsibility | 0.33 | | |

*Notes:* [a]As defined and previously validated by Hofstede [1991]. The cultural values construct was specified as a formative latent variable; thus, these estimates represent *weights* rather than loadings. Because raw data are not available, AVE and CR cannot be computed for these values.

[b]As defined by Smith et al. [1996], this construct contains 15 items, each of which measures the level of concern for a particular dimension of information privacy. As noted in the text, the four dimensions are Collection (COLL), Errors (ERR), Secondary Use (SEC), and Improper Access (ACC). Prior to testing our hypotheses using PLS, we revalidated Smith et al's [1996] information privacy concern scale using LISREL. The items were interpersed in the actual instrument but are grouped by dimension in this table.

**Table 4 Correlations of Latent Variables**

| Latent Variable | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| 1. Cultural Values | 1.000 | 0.126 | −0.611 | −0.191 | 0.120 | −0.125 |
| 2. Privacy Concerns | — | 1.000 | 0.010 | 0.005 | 0.141 | 0.207 |
| 3. Regulatory Approach | — | — | 1.000 | 0.134 | −0.135 | 0.094 |
| 4. Corporate Privacy Management Environment | — | — | — | 1.000 | −0.363 | −0.126 |
| 5. Privacy Problems | — | — | — | — | 1.000 | 0.010 |
| 6. Regulatory Preferences | — | — | — | — | — | 1.000 |

tions of the adequacy of management policies, the match between policy and practice, management attitudes regarding importance of privacy issues, and the management level at which these issues are handled are all elevated. The results indicate that regulatory approach also has a marginal positive affect on regulatory preferences (coefficient = 0.11, t = 1.60, $p < 0.10$), suggesting that in countries where there is more governmental involvement in corporate information privacy management, there is also a higher preference for strong laws over corporate self-management of privacy issues.

*Effects of the Corporate Privacy Management Environment.* In support of Hypotheses 5 and 6, the corporate privacy management environment significantly affects privacy-related problems and regulatory preferences, respectively. Specifically, the corporate privacy environment has a significant negative effect (coefficient = −0.36, t = −8.28, $p < 0.001$) on the number of privacy-related problem items checked by respondents, and a significant negative effect (coefficient = −0.17, t = −4.32, $p < 0.001$) on preference for strong laws over corporate self-management of privacy issues. These results suggest that in organizations with higher levels of the four indicators of the corporate privacy environment (tighter management of privacy), fewer privacy-related problem areas are reported. Further, tighter (more adequate) management of privacy within an organization reduces preferences for strong government (over corporate self-) regulation. Finally, there is no support for the suggestion that the number of privacy-related problem areas in an organization affects preferences for government over corporate self-regulation of privacy issues (Hypothesis 7).

### Structural Model

PLS does not minimize residual item covariance, and thus provides no summary statistic to assess the overall "fit" of the model. However, the variance explained, the sign and significance of path coefficients, and examination of the measurement weights/loadings can be used to assess model specification. Overall, the model specification assessments support the hypothesized model. All but one path coefficient (the effect of privacy-related problems on regulatory preferences) received some statistical support and all significant paths were in the expected direction, suggesting the model exhibits nomological validity (Fornell and Larcker 1981). Eighteen of the 19 manifest variable loadings are greater than 0.5, with the loading for "level of management" on the corporate privacy environment construct = 0.33 as discussed above (see Table 4).

Of the numerous alternative models tested, this model provided the most adequate explained variance while maintaining theoretical integrity, with a structural model root mean squared residual covariance of 0.069 and a total root mean squared covariance of 0.477. Thus, the model explains 85.5% of the variable covariance, which is considered highly acceptable for behavioral models (Bentler 1989).

## Discussion

Previously, there has been very little research on the factors that influence a country's regulatory approach to information privacy (Milberg et al. 1995) and no empirical investigation of the relationships among national regulatory approaches to information privacy, corporate privacy management activities, and privacy concerns. Thus, these findings constitute a major contribution to the emerging theoretical base of information privacy research and provide the basis for some specific recommendations to those managing personal data in an international environment.

In general, the findings of this study were consistent with theoretical expectations, as eight of the nine hypotheses received some support. A country's cultural values are associated strongly with the privacy concerns that are exhibited by its populace (Hypothesis 1) and are associated marginally with its regulatory approach (Hypothesis 2). As information privacy concerns rise and governments become more involved in corporate privacy management, management of privacy seems to tighten (Hypotheses 3 and 4 respectively) and, in turn, fewer specific privacy problem areas are reported (Hypothesis 5). Moreover, if corporations exhibit loose management of information privacy, then individuals are more likely to call for strong privacy laws rather than allowing corporations to self-regulate (Hypothesis 6). Similarly, as individuals' privacy concerns rise, so do their demands for additional legal intervention (Hypothesis 8). There is also a marginal, positive association between the level of governmental involvement in corporate privacy management and respondents' preferences for strong laws (Hypothesis 9). (See Figure 2 for a diagrammatic depiction of the results.)

The single hypothesis that received no support in this study (Hypothesis 7) was an *exploratory* one that predicted that, as respondents perceived larger numbers of areas in which there were corporate privacy problems, they would call for stronger laws as a remedy and be disinclined to rely on corporate self-regulation. In fact, a much stronger predictor of regulatory preferences appears to be the manner in which corporations manage their privacy environment—via their policies and structures—rather than specific privacy problems that may be ob-

served. Although it is impossible to conclusively explain this dichotomy, we speculate that, when considering regulatory alternatives, respondents may be more influenced by managerial *intent* than by the *consequences* of the managerial actions. At any rate, this curious finding certainly merits additional research attention.

Considered broadly, these results provide a new understanding of the *interconnected nature of the relationships* between privacy concerns, a country's regulatory environment, the corporate information privacy management environment, and preferences for privacy regulation. The results suggest that if a country's current approach to regulating information privacy does not lead to perceptions of adequate corporate management of privacy, trust in the current approach diminishes, and pressures to increase government intervention are likely to occur.

These findings have regulatory, managerial, and research implications. Before examining those implications, however, it is useful to consider some limitations of the present work and to discuss the study's generalizability.

### Limitations

It is appropriate to recognize one special characteristic of the present study and a future research initiative indicated by that characteristic. Our approach, by necessity, relied on respondents' *perceptions* of their own environment rather than an in-depth examination of the firms' *actual* policies and practices and a *direct* examination of their senior managers' attitudes. (Such an approach might rely on some more interpretive research methods and dictate that smaller sample sizes be utilized.) Of course, it is reasonable to conjecture that the actual drivers of regulatory preferences may, in fact, be *perceptions* of how well corporations are managing privacy. And, similarly, it may well be that employees' *perceptions* of senior managers' attitudes are stronger determinants of management practices than are the actual attitudes themselves (Selznick 1957). To test this assertion, future studies might include measures of both actual and perceived corporate management approaches and attitudes—and draw comparisons between them.

### Generalizability

This study relied on an international sample of information systems auditors. Because of this, a few comments on the study's generalizability are appropriate. On the one hand, two of the sample's characteristics suggest that the study may be *broadly* generalizable. Because the auditors were of many different nationalities, the study's results are far more robust than would be those derived from a sample grounded in one country or, even, one geographic region of the world. And, because the auditor's organizations spanned many different industries, their perceptions of organizational practices and outcomes are, taken as a whole, not grounded in any industry-specific assumptions.

On the other hand, two different characteristics may bring into question some *boundaries* on the study's generalizability. First, it has been suggested by researchers in other domains of inquiry that one's perception of one's role prescription (e.g., how one's oversight responsibilities are defined) can have an impact on one's observations within an organization and behaviors related thereto (see, for example, Graham 1986; Miceli and Near 1984; and synthesis in Miceli and Near 1992, p. 127). If this is true, then the auditors might have been more inclined to note certain privacy problems in their organizations than would have general managers. However, it should be noted that this in no way invalidates our tests of the model itself, since the model speaks to *relative* differences.

Second, because of their training, one might argue that auditors would likely be more attuned to and concerned about issues of privacy than would members of the general public. However, the overall level of privacy concerns of auditors does not appear to differ from those of other samples. In particular, the overall level of privacy concern (as measured by the 15-item scale used in this study) of U.S. ISACA members was similar to the level exhibited by samples of U.S. master in business administration and undergraduate students ($M = 5.63$, s.d. $= 0.78$, $M = 5.56$, s.d. $= 0.83$, respectively) (Smith et al. 1996). Additionally, 78.4% of U.S. ISACA members indicated that they were "very concerned" or "somewhat concerned" in response to the following question: "How concerned are you about threats to your personal (information) privacy today?" Similarly, 79% of the U.S. general public, in the 1993 Harris-Equifax Information Privacy Survey, indicated they were "very concerned" or "somewhat concerned."[10] These comparisons seem to lend support for the generalizability of the results. As such, we now will discuss implications of our findings for the regulatory, managerial, and research domains.

### Regulatory and Managerial Implications

Given the relationships found between regulatory approaches, the corporate information privacy environment, and regulatory preferences (see above), it should not be surprising that the implications for managers and regulators are intertwined. Of particular note is the concept of self-regulation: this study showed that self-regulatory approaches (i.e., those to the left on Figure 1) were associated with perceptions of less adequate corporate man-

agement of privacy which, in turn, were associated with distrust of corporate self-regulation. This finding may have important implications for the long term.

**Sustainability of Self-Regulation?**

Managers and regulators may question whether corporate self-regulation constitutes a *sustainable* approach to the governance of information privacy. The findings suggest that *corporations* take a primarily reactive approach to the management of information privacy issues, by waiting for an external threat, such as legislation, before crafting cohesive policies that confront their practices. This is consistent with Smith's (1994) observation of a three-phrase cycle of organizational response to privacy concerns: drift, external threat, and reaction.

Further, it is widely acknowledged that *regulation* of privacy is also a reactive process (Bennett 1992, Flaherty 1989, Smith 1994), in which legislators pass additional legislation (or christen new regulatory bodies, depending on the model) in response to stories of privacy violations. Consistent with this, we found that privacy concerns were positively associated with the level of government involvement in the corporate management of privacy (see this study's Hypothesis 3). As privacy concerns and distrust of corporate self-regulation continue to rise, lawmakers may be compelled to abandon self-regulatory approaches and embrace more restrictive approaches (see Figure 1). Thus, the long-term viability of corporate self-regulation seems questionable if, as this study suggests, more government involvement in the corporate management of information privacy seems necessary to create adequate privacy protection.

*External Pressures.* While this study considered factors *internal* to countries, we did not examine the influence of *external* factors, although such a study would be quite appropriate as a future research initiative. Given the nature of transborder information flows, it may be difficult in the long term for a *nation* to embrace self-regulatory approaches to the corporate management of information privacy when other nations' regulatory approaches are more restrictive.

Consider the perspective of a firm that wishes to engage in business transactions with a firm in another nation. There is increasing evidence that many countries on the right in Figure 1—countries that, for the most part, view privacy as a "human rights" issue (Smith 1994)—are applying pressure on countries on the left of Figure 1 to enact stricter privacy legislation. This is best illustrated by the recent efforts of the European Union (EU). By creating and ratifying the Privacy Directive discussed earlier, EU members agreed to abide by a number of general principles in their nationalistic regulation, and this meant that some countries were forced to move to the right in Figure 1. Greece and Italy, for example, were deeply affected, since they had virtually no formal privacy regulation prior to the Privacy Directive discussions (Dresner 1996c, 1997).

The impact on some EU countries, while pronounced, actually served as mere foreshadowing for a larger international conflict later in the 1990s. Effective October 1998, firms in EU countries have been prohibited from transmitting personal data to firms in non-EU countries unless there are "adequate" privacy protections in those accepting countries.[11] This prohibition is predicted to have a significant impact on countries that do not meet the EU standard, such as Japan and the United States. And, despite several years of discussion between government officials in the EU and in other countries, few resolutions have been reached.[12] In an attempt to avoid commercial interruptions, a few non-EU firms have individually negotiated contracts with firms in the EU, in which they have agreed to adhere to the privacy standards specified in the Directive (Fickenscher 1998, Hendricks 1998b). But long-term viability of such an approach is questionable, since the EU's objective has been to resolve the disputes at the level of federal governments, and it is quite unclear that the EU will accept the contractual approach for the long term.[13] Therefore, for transactions that include personal data, there is much evidence to suggest that it will be difficult for a country to sustain a self-regulatory privacy posture for the long term.

In addition to asking whether it is feasible for a country to sustain a self-regulatory approach independent of approaches embraced by other countries in the international community, one should consider whether *corporations* have either the desire or ability to turn self-regulation into a meaningful approach to privacy protection. For self-regulatory approaches to work at this level, at least two conditions must be met: 1) a "critical mass" of *agreement* must be reached, either directly or indirectly, regarding the policies that will be embraced by the relevant firms; and 2) these policies must be *implemented* by a critical mass of these firms. Both of these conditions rely on the perceived existence of either positive consequences (e.g., goodwill or a strategic advantage in the marketplace) to the cooperating firms and/or negative consequences (e.g., legislative scrutiny) for those who do not develop meaningful policies (see Budnitz 1998 for a related discussion). But, to date, there are few examples of privacy being used successfully as a strategic weapon (see Culnan and Milberg 1998), thus providing little evidence of efficacy for the "positive consequences" argument. With respect to the looming specter of negative consequences, this appears closely related to the "threat" that a regula-

tory infrastructure from the right of Figure 1 will be embraced by the country or countries in which a firm does business. This then introduces a bit of circularity into the argument, since the negative "lever" can hold power only to the extent that *constant* governmental scrutiny is in place. But it is very unlikely that this preemptive governmental scrutiny can be sustained without a formal regulatory authority (i.e., on the right side of Figure 1). Perhaps because of the difficulties with both the positive and negative sides of this argument, it has been reported that U.S. executives do not wish to lead their industries by taking proprivacy positions but would rather wait for a consensus to develop in their industry or until laws have been passed (see, especially, Equifax 1990 and Smith 1994).

*Levels and Limits.* It must also be realized that, for self-regulation to be sustained as a meaningful approach to privacy protection over long periods, entities at *multiple levels* must be involved: managers, firms, industries. It is not enough to simply codify a privacy policy at the firm level. There needs to be what Drumwright (1994, p. 4) identified as a "policy entrepreneur": a champion at the senior level of the corporate hierarchy who successfully prods his or her corporation to embrace a more responsive position on privacy. The results of this study are supportive of this concept, since it was shown that reports of more privacy-related problems were associated with 1) delegation of responsibility for privacy issues to lower levels of the organization, and 2) perceptions that privacy was of lower importance to senior managers (see this study's Hypothesis 5). Further, for self-regulation to be effective, firms also need to achieve what Culnan and Milberg (1998, p. 28) called a "culture of privacy" or what Smith (1994, p. 64) termed a "culture of confidentiality" to avoid a disjointed environment that is likely to engender more negative perceptions which, in turn, will lead to regulatory reactions. However, as our findings suggest, firms may be unmotivated to assign responsibility for privacy issues to senior management or to create a culture of privacy until there is a threat of regulation (see this study's Hypothesis 4).

Further frustrating firms' attempts to self-regulate in this manner are the limits—often grounded in technology—on a particular company's ability to create and implement policies. As one example, consumer purchases are increasingly leaving data trails on a number of different tracks, and no single company controls all the tracks. If one places an Internet order for goods from an online catalog, paying with a credit card, there are likely at least four commercial entities involved: the merchant selling the goods, the merchant's credit card company, the credit card company that issued the card, and at least one Web provider. Even if the merchant wished to tightly control the use of any personal data associated with the transaction, there would be little way that the data trails through the other organizations could be controlled without those organizations' consent. On balance, then, we conclude that there is little reason to believe that a particular firm can successfully protect privacy when its policies are at variance with those of other firms in its industry. Until a critical mass of agreement is reached regarding policies—and until a critical mass of implementation of those policies is achieved—self-regulation cannot be a meaningful approach to the governance of privacy.

At what level must this critical mass of agreement be reached? If broad consensus develops within an industry, and if self-regulation is effective within that industry, can this stem the tide of increasing privacy concerns within a society and, hence, reduce legislative reactivity? Our findings, particularly with respect to the internal societal factors that influence regulatory preferences, suggest that the answer is "probably not." More specifically, overall privacy concerns in a country, which have significant grounding in a society's cultural values, are strongly associated with desires for additional governmental involvement in corporate privacy management activities (Hypothesis 8, buttressed by Hypotheses 1 and 3). Even if we ignore the external pressures for privacy regulation, it must be realized that all industries in a society, regardless of whether or not they self-regulate, must deal with these overall privacy concerns. In the long run, a particular industry will be hard pressed to influence these concerns—at a minimum, to reduce privacy concerns, most of a society's industries would need to adopt a similar proprivacy approach to have any substantial effect. The likelihood of this occurring does not seem promising given the entrenched cycle of reactivity and the lack of enthusiasm among corporations for a more proactive approach to privacy issues.

## Privacy as a Social Issue: Corporate and Regulatory Responses

The reactive tendencies of corporations, citizens, and legislators toward information privacy issues creates uncertainty about the long-term viability of a corporate self-regulatory approach. One might reasonably ask how this reactive approach to corporate privacy management converges and diverges from the manner in which corporations and regulators approach other social issues. As a useful illustration, consider the process associated with corporate management of environmental concerns in the U.S. As one can see, the current approaches to corporate privacy management are in great measure analogous to

those embraced by corporations as they grapple with environmental issues. As defined by Menon and Menon (1997, pp. 52–55), the path to environmental management since 1970 in the U.S. is marked by three distinct periods:

(1) the "resistant adaptation" (or "mandated corporate responsibility") period, from 1970 to 1985, in which some weak integration of environmental concerns and business strategies was observed as companies adopted a defensive posture in their management of environmental issues;

(2) the "free market environmentalism" period, from 1985 to the early 1990s, during which companies became more proactive and broader in their orientation, still viewing environmental issues as problems to be solved and constraints to be managed; and

(3) the "corporate entrepreneurship" period, which has emerged during the later 1990s as some companies formulate and implement entrepreneurial and environmentally beneficial marketing activities, viewing this as a vehicle for creating revenue.

In light of Smith's (1994) findings, a reasonable assessment would find most U.S. firms in the 1990s on the same temporal path in their management of both environmental and privacy issues—but with their privacy management activities lagging about 15 years behind their environmental management activities. At present, most firms are toggling between the first and the second category on privacy matters—treating privacy issues in a defensive fashion and, in some instances, acknowledging privacy concerns as a constraint with which managers must deal.

It is also instructive to consider the regulatory processes that have been associated with each of these social issues. When Krier and Ursin (1977) examined a period that roughly equates to the one of "resistant adaptation" (Menon and Menon 1997), they found that U.S. legislators tended to believe in the fallacy of reactive "regulatory fixes" that seldom addressed the underlying social problems associated with pollution. Because many corporate executives worked to subvert, rather than support, the public policymaking efforts, an incrementalist phenomenon of "policy by least steps" (Krier and Ursin 1977) developed. And, if we consider the privacy regulatory process to date as being roughly equivalent to the "resistant adaptation" period for environmental concerns, we see some parallels in the U.S., as documented by Regan (1995): corporate resources used to delay and/or weaken privacy legislation, often coupled with regulation of smaller issues rather than larger ones (e.g., protection for video rental records rather than omnibus legislation that affects all forms of personal data).

Lest it be concluded that the managerial and regulatory processes associated with these two social concerns are isomorphic, however, it should be noted that the regulatory paths also have diverged at several points. While a federal agency for the regulation of environmental matters (the Environmental Protection Agency [EPA]) and already been established at the beginning of the "resistant adaptation" period, no such agency was in place—or even being seriously considered—as of 1998, the end of privacy's "resistant adaptation" period. In fact, only in mid-1998 was a proposal for a federal "Privacy Liaison," combined with a small role for the Office of Management and Budget, supported by the Clinton administration (Hendricks 1998a), and such a federal structure would be minuscule compared to the EPA of the early 1970s. In addition, by the mid-1970s, clear emissions guidelines had been established for several pollutants in a number of industries; to date, such clarity and crispness on issues associated with privacy have been noticeably absent.

Managerially, what remains to be seen is whether firms in countries where a more "hands-off" regulatory approach exists will take initiatives to develop broader privacy policies without additional, more restrictive government intervention or even embrace "corporate entrepreneurship" with respect to privacy issues. Some researchers have called for such an approach (see Culnan and Milberg 1998). From a regulatory perspective, a privacy-focused structure similar to the EPA still appears years away, and very few industries have clear rules for the collection, use, and sharing of personal data. Thus, there is ample evidence that not all social issues are created equally and that privacy stands in some measure as a distinct issue from others such as environmentalism.[14]

Why might this be so? Consider two different attributes on which environmentalism and privacy differ as social issues:

(1) The "neighborhood effect" is more pronounced for environmentalism than for privacy. That is, for pollution, corporations are perceived to be creating substantial harm and tangible societal costs (e.g., to remediate pollutants) without being forced to pay those costs. For privacy, the harm and costs are perceived to be more at individual and intangible levels (although some authors [e.g., Regan 1995] have convincingly argued that this perception is invalid).

(2) Environmental pollution is often a more visible irritant than are violations of individuals' privacy. One can see air pollution in the skies over Los Angeles, but many of the alleged violations of personal privacy (e.g., psychographic profiling in a data mining exercise) are hidden from view.

Thus, there is some reason to believe, in both managerial and legislative contexts, that privacy both con-

verges and diverges from other social issues with respect to its attributes and its treatment. This suggests that the stream of privacy research has unique value to managers and legislators as they struggle with privacy-related issues. Therefore,we now turn to the research implications of this study.

### Research Implications

The findings of this study, when considered along with previous work, suggest several directions for future research.

*Boundaries and Limits.* First, consistent with our discussion of self-regulation, additional research is certainly required to establish the boundaries and limits on a particular country's ability to act independently and/or to influence others. For example, it must be recognized that the process of aligning a country's regulatory structure with important factors may be driven not only by forces *internal* to the society but, on some occasions, from ones that are *external.* Other governments' pressures may prod a regulatory response of a certain form, as may well be observed in many countries as the EU implements its Privacy Directive in the coming months (Dresner 1996a). When this occurs, the predicted alignment with internal societal forces may actually be undercut by these external forces, and this could lead to a *misalignment* with internal reactions. Since this study considered only forces internal to a society, an obvious extension would include an articulation and examination of external forces that might also influence regulatory choices.

*Evolving Theoretical Model.* Second, other constructs and relationships could be considered within the evolving theoretical model. For example, many of the variables considered in this study (e.g., managerial attitudes, corporate policies, country regulatory approaches) could be characterized as political variables (Menon and Menon 1997). Economic variables such as competitive intensity and attractiveness of market opportunity that have been postulated to affect corporate management of environmental concerns could also affect the corporate privacy management environment, which in turn could impact a corporation's business performance (Menon and Menon 1997).

Our model could also be extended by considering variables uniquely associated with privacy. For example, Smith (1994) and Equifax (1993) have both suggested that the type of information in a corporation's database will impact its privacy management environment. In particular, medical data, followed closely by financial data, seem to be more sensitive than other data types. If Smith's (1994) findings hold, it could expected that firms housing medical or financial data would have tighter management processes but may also be perceived to have more privacy problems.

Moreover, a feedback loop between the regulatory preferences of individuals in a particular society and the regulatory approach that is embraced by its government could also be considered. It has long been suggested by scholars of privacy regulation (see, for example, Bennett 1992 and Flaherty 1989) that a country's privacy regulatory structures are a function of the desires of its populace. What is unknown, of course, is how this feedback mechanism might work in practice and what its temporal dynamics might be. Testing this relationship would likely require a longitudinal study of changes in regulatory preferences within a country; these changes would be mapped against legislative initiatives and outcomes over time.

*Specific Policies.* Third, in a movement that combines both positive and normative analysis, it would be helpful to evaluate the specific types of policies and practices that companies could adopt to improve their information privacy management environment to avoid legislative backlash and to take advantage of competitive opportunities. It has long been claimed, for example, that policies grounded in the "Fair Information Practices," coined in 1973 in a U.S. Department of Health, Education, and Welfare study (HEW 1973), can tighten the privacy management environment. But how these policies would be codified, and how they would be translated into practice, remain somewhat opaque areas of discussion.

## Conclusion

Without question, additional research initiatives need to be undertaken so that we can fully understand the interconnected relationships between managers', firms', industries', and nations' privacy approaches. But it is already clear that connections do exist, and they are becoming stronger over time. What makes the research agenda a complex one is that some deep dichotomies surround the concept of privacy.

For example, as has been discussed at length, our results and other trends suggest that the long-term sustainability of privacy self-regulation is questionable. But, while this conclusion appears to have some efficacy around the world, we hasten to point out that, at the same time, "one size does not fit all" with respect to regulatory implementation. Industries, firms, and managers cannot expect the same reaction from every governmental entity. Quite clearly, as Figure 1 and Table 1 indicate, there are numerous regulatory models in use. Different assumptions about the juxtaposed roles of firms and governmental entities can be observed (see this study's Hypothesis 2), and this can even prove true *within* a single

country: witness the debates between the various political parties in the United States, the U.K., and Sweden.

Furthermore, it is clear that societal values and assumptions about privacy vary greatly (see this study's Hypothesis 1). One can accurately infer that regulatory preferences are in some measure a reactive function of corporate behavior in all the studied countries (see this study's Hypothesis 6); that is, when societal expectations regarding privacy management are perceived to be unmet, a legislative reaction is likely in all countries. But the *precise form* of that reaction, and the *expected policies* for data collection, use, and sharing, cannot be specified in a culture-free context. What will or will not meet "societal expectations" is highly contingent on a society itself. Consumers and legislators in different societies will exhibit varying levels of concern about information privacy, both in general and in their assessment of specific practices. Thus, a universal regulatory approach to information privacy seems unlikely and would ignore cultural and societal differences.

And therein lies the deep challenge to managers and regulators: to balance these local differences in privacy perspectives with the increasingly interconnected nature of the world's commercial activities, many of which rely on the sharing of personal information. It is common within the discipline of information systems (I/S) to refer to the "islands of automation" problem, in which an organization provides computing capabilities for various units but neglects to tie them together in a cohesive and interconnected whole, thus limiting the benefits of the I/S investment. Given the results of this study and other observable trends in the worldwide privacy domain, one might reasonably conclude that, in the long run, one's attempt to create a "privacy island"—whether at the level of a firm, an industry, or a society—will be similarly problematic and foolhardy.

## Acknowledgments

This paper is dedicated to the memory of Dr. Ernest A. Kallman, a valued colleague and friend, who passed away on September 22, 1996.

The authors gratefully acknowledge the Information Systems Audit and Control Association (ISACA); the Georgetown University Center for Business-Government Relations; the Credit Research Center at Georgetown University; the Babcock Graduate School of Management Wake Forest University; and Pontificia Universidad Catolica de Chile, Escuela de Administracion for their assistance with this study. They also appreciate the data entry help provided by Emmy Curtis, Debra Miller, and Shirmel Richards, and the research assistance on international privacy legislation performed by Cindy Manning of the Bentley College Graduate School. Mary Culnan provided very helpful comments on an earlier draft of this paper. They are indebted to their senior editor, associate editor, and reviewers at *Organization Science* for helpful remarks and guidance.

## Appendix Items from Survey[a]

**Section I—Respondents Privacy Concerns**

Sample items from each subscale are shown below:

| 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. |

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

**Section II—Protecting Personal Privacy**

There are several different ways in which personal privacy could be protected. For each of the following, indicate whether you agree or disagree with the statement by circling the appropriate number. (The items were followed by a seven-point Likert scale anchored by 1 = "Strongly disagree" and 7 = "Strongly agree.")

1. The best way to protect personal privacy would be through strong laws.

2. The best way to protect personal privacy would be through corporate policies, which the corporations would develop themselves.

**Section III—For Internal Auditors and Employees**

1. Does your organization have *official policies* or rules regarding the handling of sensitive personal information about your customers, clients, or employees? (followed by check-off options of "yes," "no," and "not sure.")

IF YOU ANSWERED "NO" OR "NOT SURE," PLEASE SKIP TO QUESTION 4.

2. In your opinion, how adequate are these policies or rules? (followed by seven-point Likert scale anchored by 1 = "not very adequate" and 7 = "very adequate"; a check-off box for "not sure" was also included.)

3. Sometimes the way that sensitive information is actually handled in an organization does not match the organization's official policies or rules. In your opinion, how well do the *actual practices and operations* in your organization match the official policies/rules regarding handling of sensitive personal information about customers, clients, or employees? (followed by seven-point Likert scale anchored by 1 = "match very poorly" and 7 = "match very well"; a check-off box for "not sure" was also included.)

4. How important to the senior management of your organization is information privacy as an objective for control? (followed by seven-

point Likert scale anchored by 1 = "not important at all" and 7 = "very important"; a check-off box for "not sure" was also included.)

5. What is the title of the person currently accountable for managing information privacy issues in your organization? (followed by a free-form fill-in along with check-off options of "not sure" and "no one.")

6. In your opinion, what are the causes of problems with information privacy in your own organization? (Check all that apply.)

| | |
|---|---|
| _____ The kinds of information stored in databases | _____ How people handle information in the office |
| _____ Error detection and correction procedures | _____ Who can access the databases |

*Notes:* [a]In addition to the items in this appendix, the survey contained some items which had been used on previous public opinion polls [Cambridge Reports 1989; Equifax 1990] as validation measures. There were also some items regarding organizational demographics (e.g., headquarters location) and how privacy was viewed by the auditing profession. Those items are not included here, as they are not utilized in this paper. However, a copy of the full survey instrument is available from the authors.

Sources for the items in this appendix are as follows: Section I—Smith et al. (1996); Section II—Smith and Kallman (1992), Smith (1994); Section III, items 1 through 3 and 6—Smith and Kallman (1992), Smith (1994); Section III, items 4 and 5—developed (and pilot tested) in cooperation with ISACA.

## Endnotes

[1]Obviously, there are many issues associated with the collection, use, and sharing of personal data by noncorporate entities (e.g., government, schools). While of great importance in all societies, such issues are beyond the scope of the immediate study.

[2]*Normative* statements are those that specify how things *ought* to be, usually from a moral perspective. *Descriptive* statements, on the other hand, specify how the world *is* (see Smith and Hasnas 1999). As a salient example, an ethicist might argue that "societies ought to recognize all the interests in Table 1 as components of a 'right to privacy' for all citizens in their dealings with both for-profit and not-for-profit entities." The fact that the ethicist makes this normative ("ought") statement in no way changes the descriptive ("is") fact that many societies do not recognize some of the privacy interests in Table 1.

[3]Whether debates are resolved by market forces (as supported by Hagel and Rayport 1997 and questioned by US FTC 1998 and Budnitz 1998) or regulatory oversight does not necessarily suggest, in and of itself, that individuals in a society will have more or less privacy.

[4]Although traditionally a governmental utility, Telia has been reorganized in corporate form and is to be privatized in the future (Bondestam 1996).

[5]We bound our discussion to include only those privacy management activities that occur in the *corporate* sector. Further, for the purposes of this study, we examine only *internal* factors (that is, *within* countries) that relate to the regulation and corporate management of information privacy. Certainly, the domains of privacy management activities in the *public* (i.e., governmental) sector and *external* country factors (e.g., pressures placed on one country by another) also merit much consideration, but such an investigation is beyond the scope of the present initiative.

[6]The ISACA membership also includes *external* auditors, who perform audits for organizations other than their own. A total of 877 surveys were returned; however, the 282 *external* auditors' responses have been excluded from this study. Of the 25 countries represented by respondents, additional data (e.g., Hofstede's (1991) cultural value indices) were not available for six of these countries (China, Hungary, Ireland, Latvia, Luxembourg, Russia). Thus, the responses from these six countries in addition to 41 responses for which a nationality was not indicated have been excluded from further analysis.

The procedure called for surveys to be distributed and collected at the same meeting, and chapter members were not to be told in advance that the survey would be administered at the meeting. Thus, nonresponse bias should not be a concern for the chapters that followed the procedures. In fact, it could be argued that these chapters had a 100% response rate for members who attended the meeting at which the survey was administered. Unfortunately, a few chapters did not follow the requested procedures carefully (ascertained from their control sheet information), so we separated their responses from the others and performed a number of t-tests to check for a pattern of response bias. No such pattern was found, so we pooled all the responses in the subsequent analyses.

[7]In spring 1993, ISACA had approximately 14,500 members in 120 chapters. By fall 1998, these numbers had increased to 19,000 members in 150 chapters, respectively. Although there had been membership growth over this period, there is no evidence that the professional mix had changed within the membership profile (see ISACA [1998]).

[8]For the purpose of this study, we have focused on the *formal* regulatory structure (or lack thereof) in each country. We acknowledge the possibility that some *informal* governance mechanisms, such as an enforced code of behavior, may be in use in certain industries in some countries. Further, it is possible that a given society's norms and culture may hold sway over certain behaviors in some contexts. However, we are aware of no clear evidence, in any country, of any such informal mechanism having a sustained, long-term impact, perhaps due to the quickly shifting technological domain.

[9]Note that the sign of the coefficient is negative and thus the valence of the effects of the cultural values are opposite of the signs of the cultural value weights.

[10]Data on these issues from the general public in other countries were unavailable.

[11]During some discussions earlier in the 1990s, the word "equivalent" had been used, but it was eventually concluded that the demand of "equivalency" would create such a high standard that few other countries would have been able or willing to meet it.

[12]In particular, negotiations between the EU and U.S. representatives have been especially problematic, since the U.S. has no specific privacy agency as do most countries on the right in Figure 1. This has been a source of frustration to the EU representatives, who often express confusion as to which U.S. officials have authority to engage in privacy-related discussions.

[13]One could argue that external pressures, such as the EU's, would act as a potent incentive to firms and industries to self-regulate, and—as long as the pressure was sustained—the self-regulation itself might be sustainable. But this ignores the strong possibility of "defectors" in industries—firms that refuse to adhere to privacy rules that have been dictated by a government other than their own. Further, it also assumes that external entities will accept such self-regulatory efforts as valid

proxies for governmental regulation. Although still in debate as of this writing, it is unclear that the EU is sympathetic to this substitution.

[14]Although beyond the scope of the present discussion, it should also be noted that both privacy and environmentalism differ from other social issues such as hunger and poverty. The "offending" actor—that is, the entity that is perceived to be the *cause* of the social problems—is often the corporation itself in both the cases of privacy and environmentalism. But it is much more difficult to blame problems such as hunger and poverty directly on corporate actions, since they are grounded in larger social systems and assumptions.

## References


Alberta, Paul. 1993. Congresswoman makes third bid to set up a U.S. privacy board. *DM News* (February 15) 1, 36.

Associated Press (AP). 1998*a.* So now it's cyber-outer-space. (online filing, July 22).

Bagozzi, Richard P., Y. Yi. 1988. On the evaluation of structural equation models. *J. Acad. Marketing Sci.* **16.**

Bennett, Colin J. 1992. *Regulating Privacy: Data Protection and Public Policy in Europe and the United States.* Cornell University Press, Ithaca, NY.

Bentler, Paul M. 1989. *EQS Structural Equations Program Manual.* BDMP Statistical Software, Los Angeles.

Blas, Diana Alonso. 1995. Belgian courts take first decisions on data protection cases—On legal uses of data. *Privacy Laws Bus.* (U.K.). (28) (February) 11.

Bondestam, Anitha. 1996. What can privacy commissioners do? The limits of bureaucratic intervention. *Privacy Laws Bus.* (U.K.). (35) (June) 7–10.

Budnitz, Mark E. 1998. Privacy protection for consumer transactions in electronic commerce: Why self-regulation is inadequate. *South Carolina Law Rev.* **49** (Summer) 847–886.

CVS Pharmacy. 1998. At CVS, we safeguard your privacy as well as your health (advertisement). *Washington Post* (February 19) B12.

Cash, James I., Jr., F. Warren McFarlan, James L. McKenney. 1992. *Corporate Information Systems Management,* (3rd ed.) Irwin, Homewood, IL.

Cambridge Reports. 1989. *Technology and Consumers: Jobs, Education, Privacy* (Bulletin on Consumer Opinion no. 157). Cambridge Reports, Cambridge, MA.

Cespedes, Frank V., H. Jeff Smith. 1993. Database marketing: New rules for policy and practice. *Sloan Management Rev.* **34,** 7–22.

Colman, Sue. 1997. Australian government abandons comprehensive privacy law—In short term? *Privacy Laws Bus.* (U.K.) (39) (August) 19–20.

Culnan, Mary J. 1993. How did they get my name?: An exploratory investigation of consumer attitudes toward secondary information use. *MIS Quart.* **17** 341–363.

——, Sandra J. Milberg. 1998. The second exchange: Managing customer information in marketing relationships. Working paper, McDonough School of Business, Georgetown University, Washington, D.C.

Cyert, Richard M., James G. March. 1963. *A Behavioral Theory of the Firm.* Prentice-Hall, Englewood Cliffs, NJ.

Dresner, Stewart. 1996a. Data protection roundup. *Privacy Laws Bus.* (U.K.) (33) (January) 2–8.

——. 1996b. Australian government proposes comprehensive national privacy laws. *Privacy Laws Bus.* (U.K.) (37) (December) 2–5.

——. 1996c. Italy's new government gives priority to data protection bill. *Privacy Laws Bus.* (U.K.) (35) (June) 2–3.

——. 1997. Greece is the last EU member state to adopt a data law but first to implement the EU DP directive. *Privacy Laws Bus.* (U.K.) (39) (August) 5–8.

Drumwright, Minette E. 1994. Socially responsible organizational buying: Environmental concern as a noneconomic buying criterion. *J. Marketing* **58** (July) 1–19.

Dubinsky, Alan J., Marvin A. Jolson, Masaaki Kotabe, Chae Un Lim. 1991. A cross-national investigation of industrial salespeople's ethical perceptions. *J. Internat. Bus. Stud.* (4th quarter) 651–70.

Dunn, Ashley. 1996. Think of your soul as a market niche. *New York Times Cyber Times* (September 11).

Engel, J. F., R. D. Blackwell, Paul W. Miniard. 1986. *Consumer Behavior.* Dryden, Hillsdale, IL.

Equifax. 1990, 1991, 1992, 1993, 1996. *Harris-Equifax Consumer Privacy Survey* (and other similar titles). Equifax Inc, Atlanta.

Equifax Canada. 1992. *Equifax Canada Report on Consumers and Privacy in the Information Age.* Equifax Canada Inc, Anjou, Quebec.

Fickenscher, Lisa. 1998. Europe privacy directive likely to leave U.S. at a disadvantage. *Amer. Banker* (August 24) 1, 10.

Flaherty, David H. 1972. *Privacy in Colonial New England.* University of Virginia Press, Charlottesville.

——. 1989. *Protecting Privacy in Surveillance Societies.* University of North Carolina Press, Chapel Hill.

Fornell, Claus, Donald W. Barclay. 1983. Jackknifing: A supplement to Lohmoller's LVPLS Program, Graduate School of Business Administration, The University of Michigan, Ann Arbor, MI.

——, Fred L. Bookstein. 1982. Two structural equation models: LISREL AND PLS applied to consumer exit-voice theory. *J. Marketing Res.* **19** 440–52.

——, David F. Larcker. 1981. Evaluating structural equation models with unobservable variables and measurement error. *J. Marketing Res.* **18** 39–50.

Franklin, Charles E. H. 1996. *Business Guide to Privacy and Data Protection Legislation.* ICC Publishing S.A., Paris.

Giant Discount Drug. 1998. The most important thing we have in our relationship with our customers is their trust (advertisement). *Washington Post* (February 18) A13.

Goodpaster, Kenneth E, John B. Matthews, Jr. 1982. Can a corporation have a conscience? *Harvard Bus. Rev.* (January–February) 132–41.

Goodwin, Cathy. 1991. Privacy: Recognition of a consumer right. *J. Public Policy Marketing* **10** (1) 149–66.

Graham, J. W. 1986. Principled organizational dissent: A theoretical essay. L. L. Cummings and B. M. Staw, eds. *Research in Organizational Behavior,* vol. 8. JAI Press, Greenwich, CT. 1–52.

Hagel, J., III, J. F. Rayport. 1997. Coming battle for customer information. *Harvard Bus. Rev.* **75**(1) 53–65.

Hendricks, Evan. 1998a. Capital insights. *Privacy Times* **18** (15) 1.

——. 1998b. EU panel explores "adequacy," finds holes in U.S. FCRA. *Privacy Times* **18** (16) 4–6.

HEW (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 Sys-*

*tems,* U.S. Government Printing Office, Washington, DC.

Hofstede, Geert H. 1980. *Culture's Consequences: International Differences in Work-Related Values.* Sage Publications, Beverly Hills, CA.

——. 1991. *Cultures and Organizations.* McGraw-Hill, Berkshire, England.

Information Systems Audit and Control Association (ISACA). 1998. Association information. *www.isaca.org/ainfo.htm.*

Ives, Blake, Sirkka L. Jarvenpaa. 1991. Applications of global information technology: Key issues for management. *MIS Quart.* **15**(1) 33–50.

Kallman, Ernest A., John P. Grillo. 1996. *Ethical Decision Making and Information Technology,* 2nd ed. McGraw-Hill, New York.

Kane, Michael J., David A. Ricks. 1988. Is transnational data flow regulation a problem? *J. Internat. Bus. Stud.* (Fall) 477–82.

Kling, R. 1978. Value conflicts and social choices in electronic funds transfer systems developments. *Comm. ACM* **21**(8) (August) 642–657.

Krier, James E., Edmund Ursin. 1977. *Pollution and Policy: A Case Essay on California and Federal Experience with Motor Vehicle Air Pollution, 1940–1975.* University of California Press, Berkeley.

Kristof, Kathy M. 1997. Experian to end free credit reports. *Los Angeles Times* (January 21) D1.

Langlois, Catherine C. 1993. National character in corporate philosophies: How different is Japan. *European Management J.* **11**(3) 313–320.

——, Bodo B. Schlegelmilch. 1990. Do corporate codes of ethics reflect national character?: Evidence from Europe and the United States. *J. Internat. Bus. Stud.* (4th quarter) 519–39.

Lohmoller, Jan-Bernd. 1981. *LVPLS 1.6 Program Manual: Latent Variable Path Analysis With Partial Least Squares Estimation.* University of the Federal Armed Forces, Munich.

Mason, Richard O. 1986. Four ethical issues of the information age. *MIS Quart.* (March) 4–12.

——, Florence M. Mason, Mary J. Culnan. 1995. *Ethics of Information Management.* Sage Publications, Thousand Oaks, CA.

Mayhew, Glenn E., Russel S. Winer. 1992. An empirical analysis of internal and external reference prices using scanner data. *J. Consumer Res.* **19** 62–70.

McCrohan, Kevin F. 1989. Information technology, privacy, and the public good. *J. Public Policy Marketing* **8** 265–78.

Menon, Ajay, Anil Menon. 1997. Enviropreneurial marketing strategy: The emergence of corporate environmentalism as marketing strategy. *J. Marketing* **61** (January) 51–67.

Miceli, Marcia P., Janet P. Near. 1992. *Blowing the Whistle: The Organizational and Legal Implications for Companies and Employees.* Lexington Books, New York.

——. 1984. The relationships among beliefs, organizational position, and whistle-blowing status: A discriminant analysis. *Acad. Management J.* **27** 687–705.

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

Miller, Arthur. 1982. Computers and privacy. W. M. Hoffman, J. M. Moore, eds. *Ethics and the Management of Computer Technology.* Oelgeschlager, Gunn, and Hain Publishers, Cambridge, MA.

Milne, George R., Mary Ellen Gordon. 1993. Direct mail privacy-efficiency trade-offs within an implied social contract framework. *J. Public Policy Marketing* **12 2** 206–15.

Mintzberg, Henry. 1973. *The Nature of Managerial Work.* Harper and Row, New York.

Mowshowitz, A. 1976. *The Conquest of Wilk.* Addison-Wesley, Reading, MA.

Nunnally, Jum C. 1978. *Psychometric Theory* 2nd ed. McGraw Hill, New York.

O'Harrow, Robert O., Jr. 1998a. Prescription sales, privacy fears. *Washington Post* (February 15) A1, A18, A19.

——. 1998b. Giant Food stops sharing customer data. *Washington Post* (February 18) A1, A10.

——. 1998c. CVS also cuts ties to marketing service. *Washington Post* (February 19) E1, E5.

Oz, Effy. 1994. *Ethics for the Information Age.* Business and Educational Technologies.

Porter, Michael E. 1980. *Competitive Strategy.* The Free Press, New York.

Posner, Richard A. 1984. An economic theory of privacy. Ferdinand Schoeman, ed. *Philosophical Dimensions of Privacy: An Anthology.* Cambridge University Press, Cambridge.

PPSC (Privacy Protection Study Commission. 1977. *Personal Privacy in an Information Society: Report of the Privacy Protection Study Commission.* U.S. Government Printing Office, Washington, D.C.

Regan, Priscilla M. 1995. *Legislating Privacy: Technology, Social Values, and Public Policy.* University of North Carolina Press, Chapel Hill.

Ross, William T., Elizabeth H. Creyer. 1992. Making inferences about missing information. The effects of existing information. *J. Consumer Res.* **19** 14–25.

Samiee, Saeed. 1984. Transnational data flow constraints: A new challenge for multinational corporations. *J. Internat. Bus. Stud.* (Spring–Summer) 141–50.

Schoeman, Ferdinand, ed. 1984. *Philosophical Dimensions of Privacy.* Cambridge University Press, Cambridge.

Selznick, Philip. 1957. *Leadership in Administration: A Sociological Interpretation.* University of California Press, Berkeley.

Simon, Herbert A. 1976. *Administrative Behavior.* The Free Press, New York.

Smith, H. Jeff. 1994. *Managing Privacy: Information Technology and Corporate America.* University of North Carolina Press, Chapel Hill.

——. 1993. Privacy policies and practices: Inside the organizational maze. *Comm. ACM* **36** (12) 105–22.

——, John Hasnas. 1999. Ethics and information systems: The corporate domain. *MIS Quart.* **23** (1) 109–127.

——, Ernest A. Kallman. 1992. Privacy attitudes and practices: An empirical study of medical record directors' perceptions. *J. Health Inform. Management Res.* **1** (2) 9–31.

——, Sandra J. Milberg, Sandra J. Burke. 1996. Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quart.* **20** (2) 167–196.

Stone, Eugene F., Donald G. Gardner, Hal G. Gueutal, Stephen McClure. 1983. A field experiment comparing information-

privacy values, beliefs, and attitudes across several types of organizations. *J. Appl. Psych.* **68** 459–468.

——, Dianna L. Stone. 1990. Privacy in organizations: Theoretical issues, research findings, and protection mechanisms. *Res. Personnel Human Resources Management* **8** 349–411.

Tolchinsky, P. D., McCuddy, M. K., Adams, J., Ganster, D. C., Woodman, R. W., Fromkin, H. L. 1981. Employee perceptions of invasion of privacy: A field simulation experiment. *J. Appl. Psych.* **66** (3) (June) 308–313.

Tversky, Amos, Daniel Kahneman. 1981. The framing of decisions and the psychology of choice. *Sci.* **211** 453–58.

United States Federal Trade Commission (US FTC). 1998. *Privacy Online: A Report to Congress.* Federal Trade Commission Bureau of Consumer Protection Washington, DC. Also available at *www.ftc.gov.*

Vogel, David. 1992. The globalization of business ethics: Why America remains distinctive. *California Management Rev.* (Fall) 30–49.

Westin, Alan F. 1967. *Privacy and Freedom.* Atheneum Publishers, New York.

——. 1997. *Commerce, communication, and privacy online.* Center for Social and Legal Research, Hackensack, NJ. Summary of findings available at *www.pandab.org/comp%20surv.html.*

——. 1998. *E-commerce and Privacy: What Net Users Want.* Center for Social and Legal Research, Hackensack, NJ. Summary of findings available at *www.pandab.org/E-Commerce%20Exec.%20Summary.html.*

*Accepted by Benn R. Konsynski; received December 1997. This paper has been with the authors for two revisions.*