JOURNAL OF INFORMATION SYSTEMS
Vol. 25, No. 2
Fall 2011
pp. 47–79

American Accounting Association
DOI: 10.2308/isys-10091

A Survey of Consumer Information Privacy from the Accounting Information Systems Perspective

Robert J. Kauffman
Dartmouth College and Singapore Management University

Yong J. Lee
Marilyn Prosch
Paul J. Steinbart
Arizona State University

ABSTRACT: The information privacy of consumers is an important public policy issue in today's society, and one that businesses, industries, and governments are continuing to struggle with as information technology (IT) innovations create ever-stronger impacts. In this article, we explore consumer information privacy issues and review the results of related prior research. We provide a survey of the literature on information privacy based on our assessment from: (1) the societal and public policy perspective, (2) the business practices perspective, and (3) the individual privacy and consumer behavior perspectives that relate to the disclosure of private information by individuals to firms. From the societal and public policy perspective, we identify a number of research directions that relate to the social welfare implications of personal information surveillance, the safeguards needed at the societal level, and the nature of privacy-enhancing regulations. From the business practices perspective, we suggest other research directions that involve the examination of factors influencing organizational choices of privacy practices. We also offer some ways to discover how organizations can leverage their investments in information privacy. The individual and consumer behavior perspective, in turn, prompts Accounting Information Systems (AIS) researchers to look at the nature of people's beliefs and attitudes about privacy; the ways such attitudes affect their intentions and behaviors; and how individuals' behaviors can be influenced by organizational privacy policies and practices. The main contribution of this article is to understand these issues and identify opportunities for AIS researchers to enrich the current body of knowledge on this critical topic.

The authors thank Roger Debreceny (special issue editor), Ann Cavoukian, Mary Culnan, Efrim Boritz, Eric van Heck, Kalle Lyytinen, Ben Shao, Julie Smith-David, Chris Westland, and two anonymous reviewers for their input on this article for the special issue of the *Journal of Information Systems*. Professor Kauffman acknowledges generous support from the W. P. Carey Chair in Information Systems at Arizona State University, and the Shidler College of Business, University of Hawai'i at Mānoa. Yong-Jick Lee thanks the Doctoral Program and the IS Department at the W. P. Carey School for funding. All of the authors appreciated the support from the Center for Advancing Business through Information Technology at Arizona State University.

Editor's note: Accepted by Roger S. Debreceny, Guest Editor.

Published Online: November 2011

Keywords: business practices; consumer information privacy; Generally Accepted Privacy Principles (GAPP); information privacy; information technology; firms; privacy; societal issues; public policy.

Privacy . . . represents the control of transactions between persons and others, the ultimate aim of which is to enhance autonomy and to minimize vulnerability. (Margulis 1977, 10; emphasis added)

Information is the key asset of every 21st century business. The viability of virtually every organization depends on the ability to access throughout the enterprise a broad range of accurate, reliable, and timely information. But despite the critical value of information, it has not traditionally been managed to reflect its importance to businesses, consumers, and employees. (Breuning et al. 2008, 1; emphasis added)

Information privacy is the interest an individual has in controlling, or at least significantly influencing, the handling of data about themselves. (Clarke 2006; emphasis added)

I. INTRODUCTION

News stories about the role of information technology (IT) in the loss of personal information and the transformation of individuals' "personal space" have made information privacy a major concern in public policy (Price 2006; Clarke 1999; Turner and Dasgupta 2003). People are worried about the misuse of their personal information, which could result in identity theft, even with a variety of laws and regulations and technology-based preventive measures (Cranor 1999; Federal Trade Commission 2000; Hann et al. 2007). These concerns are heightened by the fact that individuals do not have the ability to protect their personal information fully, but must rely on the firms that collect their information to safeguard it (Milne and Culnan 2002). Consequently, the issue of trust has become paramount. Yet, although customers are viewed as strategic stakeholders for success, surveys of practice (e.g., PricewaterhouseCoopers 2008) indicate a number of problematic areas, relative to how companies protect the information privacy of consumers. Failure to protect personal information undermines customer relationships in many business contexts, and may lead to increased oversight by regulators and policy makers (Liu et al. 2004; Kim et al. 2008a).

Further complicating this situation is that once an individual's personal information is collected by one firm, it is often shared with other firms that may not employ the same level of safeguards and precautions to protect that information (Culnan 1993, 2000; Miyazaki and Fernandez 2000; Olivero and Lunt 2004; Awad and Krishnan 2006). In response, various stakeholders have initiated information privacy-related actions in the business economy and in society to protect individuals as consumers, customers, and employees (Oz 1992; Smith 1993; Hoffman et al. 1999; Culnan and Milne 2001; Hui et al. 2007). Understanding that the best way to safeguard stakeholder trust is to never lose it in the first place, for example, innovative technology-producing firms have introduced new approaches and privacy-enhancing technologies to protect privacy in our digital society (Adam and Wortmann 1989; Garfinkel et al. 2002, 2007; Dinev and Hart 2006; Kalvenes and Basu 2006).

Meanwhile, government regulators across the globe have promulgated numerous regulations mandating the protection of specific types of information.[1] In response to the complex and

[1] Representative examples include the Privacy Act 1988 (Australia), the Personal Information Protection and Electronic Documents Act (Canada), the European Union Directive, the Organization of Economic Development's Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, the Federal Trade Commission's Privacy Online—Fair Information Practices (FIP) in the Electronic Marketplace (United States), the Health Insurance Portability and Accountability Act (HIPAA; United States), and the Gramm-Leach-Bliley Act (GLBA; United States).

sometimes conflicting government regulations, the American Institute of Certified Public Accountants and the Canadian Institute of Chartered Accountants (AICPA/CICA 2004, 2006) jointly developed and announced a set of Generally Accepted Privacy Principles (GAPP; AICPA/CICA 2006, 2009; Lesser 2010; Prosch 2008). GAPP is not law. Rather, it delineates best practices that reflect the key principles found in all major global privacy regulations. GAPP provides specific criteria that firms can use to guide their efforts to comply with applicable laws and regulations. Finally, GAPP provides a useful framework to analyze the existing literature about privacy, and to identify fruitful topics for future research.

The purpose of this article is to explore information privacy issues for individuals as consumers, and review the results of related prior research to enable Accounting Information Systems (AIS) researchers to understand these issues and identify opportunities for enriching the current body of knowledge on this important topic. For a work of this nature to be meaningful for the intended audience, we must be careful to supply new perspectives and knowledge, and we must do this in a manner that will enable others to take advantage of our analytical approach. An interested observer who follows the popular press and the Internet, or reads the current annals of law and public policy, can easily point to current developments, offer riveting anecdotes, and share knowledge of popular interpretations of issues that have arisen around information privacy. We aim to bring our understanding of the relevant theoretical perspectives to bear and, in that way, create the basis for making a contribution of new knowledge.

We also compare and contrast different views of privacy around the globe, particularly the different views expressed in the European Union versus the United States. A fundamental difference is that in the European Union, privacy is regarded as a fundamental human right, whereas in the United States it is not an explicit constitutional right. This difference is paradoxical: In the United States, the primary concern is protecting the individual from government intrusions on privacy, whereas in the European Union the primary concern is protecting the individual from misuse of personal information by corporations. The European Union and the United States also differ in their approaches for protecting privacy legally. E.U. countries tend to have only a few laws that are comprehensive in scope, whereas the United States has a myriad of laws that each address only a specific area (e.g., HIPAA applies to personal medical information; Gramm-Leach-Bliley applies to financial information; the Family Education Rights and Privacy Act, FERPA, applies to students' academic information, etc.). These kinds of differences not only have practical implications for citizens, but also need to be considered by researchers.

The remainder of this article is organized in the following manner. Section II presents the scope of consumer information privacy issues that we address, and defines information privacy for this research. Sections III, IV, and V examine privacy issues from three important theoretical perspectives: public policy and societal concerns, particularly the need for regulations governing how firms handle the personal information of their customers; business practices related to the collection and use of personal information; and consumer behavior and marketing issues that determine whether, and to what extent, individuals are willing to provide their personal information to firms. Section VI concludes with an assessment of what we have contributed and questions for future research that we believe are most actionable for researchers in the AIS community.

II. INFORMATION PRIVACY: PRELIMINARIES

Westin (1967) called for explicit definitions of privacy, so that it would be possible to develop effective legal responses to protect it. Warren and Brandeis (1890) earlier discussed the need for the law to change in response to various developments in order to protect privacy effectively. They defined privacy as simply "the right to be left alone." Margulis (1977, 10), in contrast, offered a more transaction-oriented view by stating that privacy is "the control of transactions between

persons and others, the ultimate aim of which is to enhance autonomy and to minimize vulnerability." Clarke (2006) offered an even more specific definition of information privacy: "the interest an individual has in controlling, or at least significantly influencing, the handling of data about themselves."

Solove (2004) has asserted that many privacy problems have nothing to do with technology, but rather are related to the law. He noted that in the 19th century, Ralph Waldo Emerson, referring to the mail, declared that it was unlikely that "a bit of paper, containing our most secret thoughts, and protected only by a seal, should safely travel from one end of the world to the other, without anyone whose hands it had passed through having meddled with it" (Solove 2004, 225). Subsequently, in response to the concerns of Emerson, laws were created to protect the post offices' mail.

Consumer and governmental concerns about privacy rights have become more acute as IT has become more powerful and widely diffused. Recent information privacy issues include consumer privacy and secondary information use, governmental collection and use of personal information, workplace privacy and employee monitoring, and online social media privacy. Each issue area has unique characteristics and involves various players or stakeholders. We will limit our discussion to consumer information privacy and the use of consumer information, focusing on the collection, storage, use, dissemination, and destruction of personal information by firms.

We also distinguish information privacy from the information security concept of confidentiality.[2] Confidentiality refers to the objective of controlling access to and providing protection from unauthorized disclosure of information about the firm's transactions, its intellectual property, and other sensitive information provided by its business partners. Information privacy, in contrast, is concerned with controlling access to and protecting personal information that is acquired from individuals (AICPA/CICA 2003). Thus, the focus of confidentiality is primarily on protecting business data through techniques such as encryption and access control. The focus of information privacy is on enabling individuals to control how their personal information is acquired and used (Culnan and Bies 2003), but it also extends to issues of encryption and access control, and other factors related to confidentiality and regulatory concerns. Consequently, public policy considerations play an important role in information privacy, with many jurisdictions adopting regulations governing the collection, use, and retention of personal information.

Our review of prior research identifies three distinct theoretical perspectives that have been employed to study information privacy. The societal and public policy perspective examines such issues as the meaning of privacy, the need for standards and regulations on privacy issues, and

[2] Still another issue is data ownership for consumers, which, in the business context, implies the residual rights of control to determine access privileges for data that might be accorded to others (Van Alstyne et al. 1995)—a definition that is based on the incomplete contracts theory of Grossman and Hart (1986) and Hart and Moore (1990). According to Loshin (2002), ownership "implies power as well as control. The control of information includes not just the ability to access, create, modify, package, derive benefit from, sell or remove data, but also the right to assign these access privileges to others." Scofield (1998) has further written: "Telling a user that he 'owns' some corporate data is a very dangerous thing. He might try to exercise 'rights' of ownership [that] could be disastrous to the enterprise and its data. To talk about 'ownership of data' is tempting, but dangerous. The term 'stewardship' may be a better term to use, because it implies a broader responsibility where the user must consider the consequences of making changes over 'his' data." These issues are well recognized in settings that involve the broader perspectives of human rights in health care and human genetics-related research, but less well appreciated in contexts involving marketing data for customers, and human resources data for employees (U.S. Department of Health and Human Services 2010). In the broader context, data ownership is an issue for citizens and it should be protected with some of the fundamental privacy protection rights accorded to people as human rights. We refer the interested reader to the following conventions: the International Covenant on Civil and Political Rights (Office of the United Nations High Commissioner for Human Rights 1966), the United Nations Declaration on Human Rights (United Nations 1948), and the Convention for the Protection of Human Rights and Fundamental Freedoms (often referred to as the European Convention on Human Rights [Council of Europe 1950]).

political developments and social pressures for such efforts (Mason 1986; Caudill and Murphy 2000; Lee and Rao 2007). Research motivated by this perspective focuses on concerns about the effects of information privacy policy failures such as identity theft, protecting the privacy of health care information, and privacy on the Internet (Rensel et al. 2006). The business practices perspective examines how well firms comply with the applicable information privacy norms, practices, and laws, as they go about the conduct of their day-to-day business (McLeod and Rogers 1982; Greenaway and Chan 2005; Ashrafi and Kuilboer 2005; Greenstein and Hunton 2003). It also emphasizes the manner in which practice changes in the presence of technological innovation. The individual privacy and consumer behavior perspective investigates factors that drive individuals' decisions about whether and what personal information to share with firms. Of interest is the balance between the benefits of individual profiling and the costs of protecting privacy (Bellman et al. 2001; Brown and Muchira 2004).

The next three sections review relevant prior research from each of these perspectives. To support this effort, we conducted a review of the relevant journals and literature, based on journals in the accounting, IS, law, and other disciplines. (Appendix A lists the journals from which we have selected references for inclusion in this article.) We used the following approach: (1) Initially, we approached the problem of understanding information privacy by sketching the different kinds of stakeholders and the information privacy issues and tensions that exist among them. (2) We identified leading theoretical perspectives from AIS and IS research that enabled us to evaluate the issues in terms of the literature. (3) Thereafter, we expanded our coverage of relevant theory in two ways: (a) by including theoretical perspectives from other referent disciplines, and (b) by including additional theoretical perspectives that specifically helped us to frame a more balanced view of the international context of information privacy. Some of the other interdisciplinary research reflects the political, societal, psychological, behavioral, and public policy overtones of consumer information privacy issues. (4) This process allowed us to represent the current state of knowledge in this area, as well as to identify gaps in the current knowledge as a basis for suggesting future research directions for the AIS research community. (5) Finally, we drew upon relevant materials from accounting practice, especially related to policy circulars associated with the Generally Accepted Privacy Principles (GAPP), as a means of making our work salient to AIS researchers. Appendix B uses the GAPP framework to summarize the various research topics discussed in this review.

III. THE SOCIETAL AND PUBLIC POLICY PERSPECTIVE

Formulating policy for the protection of information privacy has always been difficult, as multiple cultures and varied global perspectives on individual privacy and the role of government make the issues complex. Two theoretical lenses can help to understand the sociopolitical forces underlying the myriad of regulations and policies that have been developed around the globe: the multiple stakeholder theory of privacy and cultural lag theory. We consider the U.S. and E.U. approaches to privacy protection in our discussion. Table 1 gives the key research questions that need to be investigated, relevant references, and important findings of prior research.

What Are the Social Welfare Implications of Personal Information Surveillance?

Stone and Stone-Romero's (1998) multiple stakeholder theory of privacy focuses on privacy as a problem of information control. Information moderates and informs the relationship between individuals and firms, and its availability enables firm decision making for effective strategy and operations. Three groups of stakeholders are relevant and are common across cultures and geographic borders: firms, employees, and consumers. Stakeholder values and expectations are based on cultural norms, laws, and economic and other environmental variables. Consequently, in

TABLE 1

Overview of the Literature on the Societal and Public Policy Perspective

Key Questions	Selected Citations	Research Findings
What are the social welfare implications of surveillance involving individuals' personal information?	Mason (1986) Stone and Stone-Romero (1998) Levin and Nicholson (2005)	Balancing the different needs of firms, individuals, and society as a whole must be considered.
What safeguards are needed at a societal level to provide behavioral norms for firms to ensure consumer privacy protection?	Warren and Brandeis (1890) Ogburn (1957) Westin (1967) Culnan (2000) Solove (2004) Markel (2006) Prosch (2008)	Alternative processes, technologies, and controls can help to bring stakeholder needs back into balance. Individuals, to enjoy their liberties and freedom, must be able to control whether personal information is collected about them, in balance with societal needs.
What privacy-enhancing regulations and co-regulations should be promulgated for ITs that exploit consumer privacy?	Aguilar (2000) Karol (2001) Cain (2002) Mitrano et al. (2005) Garfinkel et al. (2007) Clarke (2008) Warren et al. (2008) Clarke (2009) Tene (2009)	The effectiveness of direct regulation and laws, co-regulation and non-governmental monitoring, and self-regulation should be evaluated relative to different ITs and the privacy-enhancing approaches that can be implemented in light of them.

multinational firms, different stakeholders are likely to have diverse values and concerns over privacy, based on their local culture of origin. Levin and Nicholson (2005) discussed the difference between the United States, European Union, and Canadian laws to highlight some of these basic approaches. For example, among the E.U. member countries, privacy protects the "dignity" and the "public images" of citizens. In the United States, however, privacy has essentially been derived from Libertarian thought, which equates with the political philosophy of individual freedom from government control. Levin and Nicholson (2005) pointed out that the Canadian model of privacy protection is focused on individual autonomy through personal control of information, which is akin to the U.S. perspective. These different approaches are a result of and have an impact on societal values.

Further complicating matters is that a stakeholder can be involved in multiple roles. The multiple stakeholder theory of privacy brings to light privacy issues associated with common internal auditing practices, where multiple stakeholder roles have meaning. For example, internal auditors routinely examine the personal information of employees, such as home addresses, to identify potential conflicts of interest. So data mining is important for maintaining sound internal control for companies in some countries, but it is illegal in many other countries.

Many U.S. firms employ attachment-scanning software to search for such content. AIS researchers can leverage the criteria included in GAPP, including Privacy Awareness and Training (Criterion 1.2.10; AICPA/CICA 2009, 21), Risk Assessment (Criterion 1.2.4; AICPA/CICA 2009, 15), and Information Security Program (Criterion 8.2.1; AICPA/CICA 2009, 49) to guide a systematic study of policies and procedures governing employers' expectations, monitoring techniques and practices of firms, and employee training processes. Simulations, with incentives offered to employees, can be designed and implemented so that the associated risks and costs of

various monitoring techniques can be examined in different cultural settings. Such research will provide useful guidance to regulators and internal auditors on the most effective practices for privacy risk reduction to individuals and society as a whole.

Still others view privacy as an ethical issue. Mason (1986) asked: What information about one's self or one's associations must a person reveal to others, and under what conditions, and with what safeguards? What information can people keep private and not be forced to reveal to others? Some other GAPP criteria can be used to guide researchers with respect to the aforementioned issue of ethics and the social welfare implications of personal information surveillance. They include Communication to Individuals (Criterion 3.1.1; AICPA/CICA 2009, 26–27), Consequences of Denying or Withdrawing Consent (Criterion 3.1.2; AICPA/CICA 2009, 27), and Consent for New Purposes and Uses (Criterion 3.2.2; AICPA/CICA 2009, 28–29). Specifically, Criterion 3.1.1 requires that "individuals are informed about (a) the choices available to them with respect to the collection, use, and disclosure of personal information, and (b) that implicit or explicit consent is required to collect, use, and disclose personal information, unless a law or regulation specifically requires or allows otherwise" (AICPA/CICA 2009, 26).

Coercive consent is not considered acceptable in most cases, and it hardly seems ethical. Informed consent is problematic also, since consumers often need to consent to sharing their information or they will not be able to get the good or service they wish to acquire (Shapiro and Baker 2001). Personal information that is collected may be part of the financial accounting system's audit trail, but much of it may not directly relate to a financial transaction. AIS researchers also can study personal information stored by the systems for human resources, payroll processing, and internal audit monitoring. They also can assess the appropriateness of the business purposes that are identified, the consistency of use of the data by human resources and internal auditors with the stated purposes, and the appropriateness of choices that are made.

Some of Mason's (1986) other primary concerns are relevant as well. For example, how important is accuracy, and who is responsible for such accuracy and the damages that ensue from inaccurate information? Data quality is one of the ten principles of GAPP. For example, Criterion 9.1.1 asserts that "individuals [should be] informed that they are responsible for providing the entity with accurate and complete personal information, and for contacting the entity if correction of such information is required" (AICPA/CICA 2009, 57).

Responsibility and accountability of damages from inaccurate information are covered in multiple places in GAPP. For example, the assignment of responsibility and accountability is covered in Criterion 1.1.2 (AICPA/CICA 2009, 13–14). Enforcement and monitoring, however, are also important to consider for instances of non-compliance. Criterion 10.2.2 is related to Dispute Resolution and Recourse (AICPA/CICA 2009, 61–62), and Criterion 10.2.4 addresses Instances of Non-Compliance (AICPA/CICA 2009, 63–64). The latter states that "instances of non-compliance with privacy policies and procedures [should be] documented and reported and, if needed, corrective and disciplinary measures [should be] taken on a timely basis" (AICPA/CICA 2009, 63). AIS researchers can draw upon the continuous audit and monitoring literature (Vasarhelyi and Harper 1991; Vasarhelyi et al. 2004). They can develop techniques for assessing data accuracy; test data that can be run through systems to see if seeded databases with falsified data are flagged; and use logging techniques to track the movement from detection of inaccurate data to the correction of data, and the resolutions of problems with inaccurate data.

What Safeguards Are Needed at a Societal Level?

There has been a global debate about IT privacy and the efficacy of direct regulation through government laws; self-regulation by firms without the penalties of law but the sanctions of community stakeholders; and co-regulation involving a legislative act that puts enforcement in the

hands of non-governmental partners, including industry and technology associations (Winn 2011). Senden (2004, 2005) identifies co-regulation and self-regulation as "soft laws," which do not have the binding force of government laws, including things such as codes of conduct and practice guidelines. Nevertheless, co-regulation can involve meaningful sanctions. For example, in the United States, public accounting firms are responsible for auditing whether financial statements comply with the applicable standards of the Generally Accepted Accounting Principles. Failure to comply with those standards results in an audit opinion that is not "unqualified"; such audit opinions can adversely affect equity prices and loan covenants. Another example of co-regulation is related to firm choices on Internet websites; it is the World Wide Web Consortium's Platform for Privacy Preferences Project (P3P Project). It offered a protocol to codify the intended uses of consumer and user information collected from websites and provided guidelines for a firm's notifications to consumers about what it is doing with their private information (Reagle and Cranor 1999).[3]

Nevertheless, Winn (2011) points out that, in contrast to their European counterparts, American business leaders, observers, and academicians have been especially subject to the "romance of self-regulation" when it comes to the Internet, pointing to the example *laissez-faire* practices of "*lex mercatoria*" (mercantile law) traditions of medieval European city-states. She presents a more contemporary viewpoint, quoting the perspective of Tambini et al. (2008, 294), that "the ideal of a pristine Internet, free from regulation, is a myth, and not a particularly helpful one. Internet communication, similar to all kinds of communication, is a social practice that comes with responsibilities, ethics, norms, disputes, and harms. Whether the necessary rules are formal or informal, and whether they should be agreed with the specific involvement of state institutions or formal democratic accountability are pragmatic questions best to be resolved through public debate case by case." Clarke (1999) reinforces this view by emphasizing that legislatures should provide incentives to encourage compliance and disincentives that discourage inappropriate behavior, while the role of self-regulation should be to provide industry-specific privacy principles. He further argues that self-regulation should work alongside privacy-enhancing technologies to ensure there is appropriate enforcement and application of sanctions.

The works by Warren and Brandeis (1890), Westin (1967), and Solove (2004) are seminal pieces that can guide AIS researchers in this area, especially in developing more critical insights about the soft law approaches. In light of the rapid changes that technological innovations have wrought, we recognize that it takes a while for the information privacy stakeholders in society—individuals, firms, solution providers, and regulators—to figure out what the impacts will be. Cultural lag theory (Ogburn 1957) is useful for understanding the effects of this phenomenon. The theory, when extrapolated to the privacy arena, allows for the possibility that individual expectations about privacy will not adequately take into account the effects of new technologies (Prosch 2008). As people become aware of new threats to privacy, they will begin to demand that the firms with which they share their personal information employ countervailing protective measures. In response, technology-solution providers will develop new products to meet this demand, and standard-setting and regulatory stakeholders may mandate the use of new privacy-enhancing technologies and the deployment of privacy-related controls.

Culnan (2000) reported that although 67 percent of sampled firms posted privacy disclosures on their websites, only 14 percent of the policies were considered to be comprehensive. Markel

[3] The P3P Project is well known among IS and computer science researchers, and has not proven to be as useful or as widely adopted as was initially expected. Although P3P does not ensure information privacy for users in their interactions with websites, it helps users make informed decisions about handling their private and sensitive information. Thus P3P is more of a tool for providing guidelines for many different kinds of organizations, including firms that offer connections to people who are Internet users.

(2006) studied 20 large companies and found that 19 of them were not in compliance with their own posted privacy policies. These findings suggest that self-regulatory efforts have been largely ineffective. Jamal et al. (2005), however, found no differences in compliance with policies between firms in the United Kingdom, which has had mandatory national privacy regulations, and firms in the United States, which has lacked such regulations. The ongoing debate and the seeming contradiction of prior research findings suggest a potentially fruitful direction for future exploration by AIS researchers.

The implementation of new technologies before appropriate internal controls can be developed always raises various issues of risk for society and firms; so cultural lag theory, as it relates to the introduction of new technologies, has significant implications for AIS researchers. The introduction of laptops with USB drives, for example, provides greater data storage capacity and flexible external storage, and supports greater ease of connectivity to peripherals. It also introduces the added possibility of data leakage and the loss of massive amounts of potentially sensitive information, with consequences that may be unexpected and detrimental to society, however. For example, a health care provider was sanctioned for losing a USB drive that contained unencrypted health care information (Information Privacy Commissioner of Ontario 2009). That provider was directed to encrypt all such information on mobile devices, similar to what we see in the financial services industry in the United States.

AIS researchers can investigate the time lag between the introduction of new technologies, the risk impacts of such technologies, and the required and successful implementations of associated privacy enhancing technologies. Once again, GAPP criteria can be useful in guiding research. Specifically, Criterion 8.2.3 states that "physical access is restricted to personal information in any form (including the components of the entity's system(s) that contain or protect personal information)" (AICPA/CICA 2009, 52). Criterion 8.2.6 recommends that "personal information stored on portable media or devices is protected from unauthorized access" (AICPA/CICA 2009, 54). These recommendations suggest the importance of an approach called "privacy by design," suggested in the 1990s (Cavoukian 2009). This perspective has been gaining increasing prominence in the minds of corporate information security officers and government regulators (Langheinrich 2001; U.K. Information Commissioner's Office 2008b; Cavoukian 2009; IBM Research 2009), and is the subject of current joint academic-industry research (Rodriguez 2009; David and Prosch 2010).

What Privacy-Enhancing Regulations Should Be Promulgated, Related to IT?

Due to the different privacy perspectives across countries, firms approach the formulation of their information privacy strategies differently in different parts of the world. In the United States, although national regulations have been implemented to protect specific types of personal information (e.g., HIPAA for health information and GLBA for financial information), the overall approach has generally been one of self-regulation. In fact, the U.S. Constitution does not view individual privacy as a fundamental human right (Alderman and Kennedy 1995; Cate 1997). In contrast, in the European Union, comprehensive privacy laws or equivalent legislation have been enacted to protect individuals' information privacy. The implementation details of those laws typically vary, depending on the country's culture, social values, and history.

Many privacy researchers assert that the United States has been lax in enacting universal privacy laws. Cain (2002) pointed out that the E.U. Directive generally requires prior, unambiguous consent, whereby an individual "opts in" to permit their personal information to be collected or redistributed. The contrast is that the U.S. approach is to ask for an "opt-out" decision on the individual's part. Cain further asserted that the U.S. Constitution is the source for most of the differences between the United States and international regulatory approaches to information

privacy. The constitutional right to privacy applies mainly to government intrusion, but not to invasions from others in the private sector.

Nevertheless, although there are marked differences between the E.U. and the U.S. approaches to privacy protection, progress toward a shared global view of necessary protections may be hindered by too much focus on arguing about which approach is better. Aguilar (2000, 57) has commented on this continuing debate: "These competing visions will result in no e-consumer protection and an inability for e-businesses to stave off litigation." He has advocated a hybrid approach to privacy protection, and called for government-enforced self-regulation. This, he has argued, can take various forms, such as industry participation in legislative drafting, where industry standards are elevated to the force of law, or industry, or other self-regulatory enforcement processes that come to be government sanctioned and consequently operate with the force of law.

The efficacy of regulations as a global solution to improve privacy, however, has been challenged on two bases. One argument from Tene (2009, 14) is that in non-democratic societies, the lack of an independent judiciary and other institutions means that regulations create "more privacy on their books than on the ground." He further argues that in strong democracies, effective data privacy protection is possible without enacting the full complement of explicit regulations that exist in the European Union. This is an empirical question that can be studied by AIS researchers because of their experience with internal controls and risk assessment processes. A second argument is that regulations do not protect privacy, but only provide sanctions for violations and, therefore, that technological solutions are required (Garfinkel et al. 2007). We agree that research on privacy-enhancing technologies is important, but we have excluded it from the purview of this article because AIS researchers are unlikely to contribute.

Another approach with greater potential for positive impacts for all stakeholders is the use of privacy impact assessments (PIA; Clarke 2009; U.S. Census Bureau 2010; U.S. Department of the Interior 2010). In the global context, these are referred to as privacy risk assessments (PRA), and there is a greater emphasis placed on the firm context (Mitrano et al. 2005). The primary focus has been on government agencies' performance relative to the information privacy of citizens, leading to institution-based trust. Many different forms of impact assessments have been used over the years in Europe, North America, Australia, and elsewhere to address the issues in specific domains. They include environmental impact assessments, social impact assessments, and—since the 1980s—privacy impact assessments.

Karol (2001) stated that PIAs "provide a framework for identifying and reviewing privacy issues as they arise within particular contexts. The concept is to ensure that privacy is considered throughout the business redesign or project development cycle, particularly at the conceptual stage, the final design approval and funding stage, the implementation and communications stage, and the post-implementation audit or review stage." The most notable research to date is the work of Clarke (2008, 2009), who has chronicled the history, the intended impacts, and the implementation issues associated with government-agency use of PIAs, while arguing on behalf of their efficacy in association with other means. Stewart (1999) also conducted research to evaluate how to improve the implementation of PIAs, and concluded that they could become a powerful vehicle for effective regulation.

Warren et al. (2008) sought to understand how one country (the United Kingdom, in this case) could learn from the experience of other countries in its use of PIAs to be effective in protecting information privacy, when systems and technologies affect information sharing. A current effort is unfolding in North America with the activities of the AICPA in the United States and the CICA in Canada. They are exploring how best to guide firms with their efforts to implement PRAs. In particular, this joint effort (AICPA/CICA 2006, 2009) advocates establishing and managing a privacy program based on five different kinds of activities: (1) strategizing about how to perform privacy strategic and business planning; (2) diagnosing privacy gaps with risk analysis; (3)

implementing the development, documentation, rollout, and institutionalization of the program's action plan, including establishing controls over personal information; (4) sustaining and managing the activities of the privacy program with ongoing monitoring; and (5) auditing the firm's privacy program, by engaging internal and external auditors.

The research in this area is nascent but rich in opportunities for AIS researchers, and our impression is that this area needs additional study and attention. Especially valuable will be empirical evaluation to uncover the elements of a variance theory that can explain the circumstances under which these tools offer the best means to support individual privacy protection at the firm and societal levels. We discuss some related methods in the next section.

IV. THE BUSINESS PRACTICES PERSPECTIVE

We next review research on how firms make choices about the level of security that they provide to achieve information privacy protection. This pertains to GAPP Principle 8, Security for Privacy (AICPA/CICA 2009, 48). When transactions occur between firms and consumers, the consumers' personal information is passed on to the firms. Such information may be required for the transactions themselves (names, billing and shipping address, etc.), or may be used in profiling and target marketing (optional information such as area of interest, profession, etc.). Some sensitive information may also be generated and collected during the transactions without the consumers' consent (click-stream data, purchase history, geo-location data, etc.). Though the transactions involve the consumers' personal and sensitive information, it is the firms that decide how much information will be collected during the transactions, regardless of the information type. Firms set privacy strategies, such as how much information will be gathered, how long it will be stored, who will have access to the information, and how the information will be used and shared (for profiling, target marketing, etc.). Once privacy strategies are set, firms may publish them, so that consumers can decide how much private information they will share with the firms.

Due to growing concerns about consumer privacy and an increase in privacy regulation requirements, firms are increasingly advised by their auditors and lawyers to maintain higher standards of information privacy (Kirk 2007). They are concerned about reputational and financial damage, and rightly so. A firm that does not protect its customers' private information jeopardizes its relationship with them, and may also be liable for severe monetary and other damages. ChoicePoint and T.J. Maxx, for example, were fined millions of dollars for security breaches that resulted in the loss of customers' private information, including credit card numbers, and lost brand value as well (Bavis and Parent 2007). An information security breach often affects the stock price of the company and creates negative customer opinions (Acquisti et al. 2006). So it makes economic sense for the firm to understand more fully how to effectively invest in the protection of its customers' information.

The growing concerns are further emphasized by the consequences resulting from security breaches and privacy violations, and their effects on trust and reputation (Culnan 1993; Smith et al. 1996). In this context, firms have begun to emphasize the development of a new discipline for information security and privacy protection investment decision making. Such actions are consistent with the Criterion 8.2, Procedures and Control (AICPA/CICA 2009, 48); and more specifically, Criterion 8.2.1, Information Security Program; Criterion 8.2.2 and 8.2.3, Logical and Physical Access Controls; and Criterion 8.2.7, Testing Security Safeguards (AICPA/CICA 2009, 49–53 and 56). Their investment strategies are dependent upon internal factors, such as a firm's desire to balance the use of information for its business purposes while preserving information privacy for customers. There are also other competitive considerations in the marketplace, and natural disasters and environmental hazards that are considered in Criterion

8.2.4 on protecting personal information from natural disasters and environmental hazards (AICPA/CICA 2009, 53).

Table 2 provides an overview of the key research questions, selected references, and basic findings of prior research on information privacy and the related business practices in this area. (Again, we refer the reader to Appendix B for additional research questions that tie our discussion of the issues in this section to the GAPP.)

What Factors Influence the Choice of Privacy Practices?

Several external forces regulate firms' use of private information. We classify those external forces into three groups, based on a theoretical contribution to the literature by Mizruchi and Fein (1999). Coercive inputs present the strongest degree of enforcement, and include regulations and laws. Normative inputs, on the other hand, involve voluntary compliance and do not have explicit enforcement mechanisms. Finally, mimetic inputs have no formal definitions whatsoever, though they may be widely adopted throughout the industry. They include industry best practices and norms, but may have no formal elements.

Coercive Inputs—Regulations and Laws

We mentioned earlier that the United States and the European Union have different approaches to privacy regulations. Many observers have suggested that the implied, but not explicit, right to privacy in the U.S. Constitution has left the United States with ambiguity and discontinuities in its information privacy doctrine and regulations, leading to the result that senior managers in U.S.

TABLE 2

Overview of the Literature on Business Privacy Practices

Key Questions	Selected Citations	Research Findings
What factors influence firms' choice of privacy practices? What are the factors that influence firms' decisions about information privacy policies?	Straub and Collins (1990) Culnan (1993) Smith et al. (1996) Milne and Culnan (2002) Sarathy and Robertson (2003) Cavusoglu et al. (2004) Ashrafi and Kuilboer (2005) Acquisti et al. (2006) Schwaig et al. (2006) Garfinkel et al. (2007) Kirk (2007) Menon and Sarkar (2007) Crothers (2009)	Firms still seek specific actionable plans suitable for their own situations. Privacy strategies are dependent upon regulations and laws, self-regulations, and industry best practices and norms. Privacy strategies also depend upon industry-specific sensitivity to privacy risks and concerns.
How should firms approach achieving optimal investments in information security for themselves and information privacy for their customers?	Soo Hoo (2000) Longstaff et al. (2000) Gordon and Loeb (2002) Schechter and Smith (2003) Wang et al. (2008) Lee et al. (2009) Png and Wang (2009)	Although consumers want full protection of their information privacy, a firm's investment level is constrained by budget and profit considerations. Providing full information privacy protection may be socially desirable, but it may not be an equilibrium outcome for heterogeneous firms in the competitive environment.

firms have not always benefited from clear or broadly accepted guidance based on the law. Consequently, they often have adopted industry-specific best practice approaches.

Normative Inputs—Self-Regulation

An example of self-regulation is based on the recommended practices of an international agreement between the United States and the European Union, the Safe Harbor Agreement, which helps U.S. companies that wish to do business with Europe identify how to comply with guidelines that match the E.U. Directive on the Protection of Personal Data (Directive 95/46/EC).[4] Compliance with the Safe Harbor Agreement is overseen by the U.S. Department of Commerce (Langheinrich 2002). All of the seven key principles in the Safe Harbor Agreement are covered in GAPP as follows. Notice is covered by Principle 2—Notice. Choice is covered by Principle 3—Choice and Consent. Onward Transfer is covered by Principle 7—Disclosure to Third Parties. Security is covered by Principle 8—Security for Privacy. Data Integrity is covered by Principle 9—Quality. Access is covered by Principle 6—Access. And Enforcement is covered by Principle 10—Monitoring and Enforcement. The effectiveness of such attempts at self-regulation, however, depends upon both the degree to which firms disclose and comply with their self-imposed privacy policies and the ability to monitor compliance and to require firms to rectify any violations.

Regarding monitoring and sanctions, there are questions about the U.S. Federal Trade Commission's performance in dealing with false claims about compliance with the Safe Harbor agreement (Connolly 2010). However, monitoring and compliance issues occur not only in the context of self-regulation, but also in settings with government regulation of privacy. For example, there is evidence from the United Kingdom that many firms in the real estate industry are not providing the regulatory agency with the required notifications about handling personal data (U.K. Information Commissioner's Office 2010). Thus, the mixed evidence from practice indicates that compliance with self-stated privacy policies is an issue to which AIS researchers can contribute by conducting rigorous, cross-sectional, and cross-cultural studies to identify the conditions most conducive to effective self-regulation.

Mimetic Inputs—Industry Best Practices and Norms

Determining the best practices for business to follow, and identifying the norms of behavior are intended to create an environment of trust and mutual respect between consumers and the firms with which they interact. Although there are many regulations and guidelines available to help firms formulate privacy strategies, senior managers still seek actionable plans that are suitable for their own situations and the technical solutions that are available in the marketplace or can be built in-house. Complicating their decisions, today there are many privacy-enhancing technology alternatives and solutions that have different capabilities, levels of effectiveness, and associated

[4] The U.S. Department of Commerce's (2000) International Trade Administration's Electronic Commerce Task Force listed seven key principles to govern U.S. firms' handling of personal information in international transactions: (1) Notice: Firms are required to notify consumers about personal information collected from them. (2) Choice: Consumers should be able to choose whether personal information they provide to firms will be used. (3) Onward transfer: Consumers also should be able to choose whether their private information is ever shared with third parties by the firm that collects it. (4) Security: Consumers should be assured that their data will be used for the intended purpose, and protected so that it cannot be acquired by others in any way. (5) Data integrity: Consumer data must be accurate and current, and unnecessary data should not be collected. (6) Access: Consumers should be given access to the personal information, and be able to change it so that it's accurate. (7) Enforcement: Consumers should be further protected by mechanisms that ensure firm compliance with Principles 1 to 6, and firms should bear the burden of verification that they are in compliance.

costs for protecting personal data stored in databases and data warehouses (Sarathy and Muralidhar 2006).[5] The issue has become even more pressing with the recent extensive use of data mining techniques for deriving insights for decision making or target marketing (Menon et al. 2005; Bapna and Gangopadhyay 2006; Menon and Sarkar 2007). Moreover, the stringent demands placed on the protection of sensitive data such as health care information, according to Health Insurance Portability and Accountability Act (HIPAA) requirements, make this privacy issue practically challenging (Garfinkel et al. 2007).

Although the FIP and GAPP guidelines (mentioned in footnote 1 of this article) should guide firm-level privacy investment strategies, they do not dictate uniform implementation of privacy programs or anything specific regarding privacy-enhancing technologies. This makes their application possible across different industries in which senior managers have diverse perceptions about information privacy. Schwaig et al. (2006) reported that firms in different industries use different information practices that are considered fair, even though they may not address information privacy in a uniform way. The sensitivity of consumer information also differs by industry. As a result, some industries are subject to government regulations, such as health care with HIPAA, which makes dealing with information privacy in different industries even more challenging.

Most firms are likely to underinvest in proactive privacy protection approaches, due to the lack of appropriate incentives (U.K. Information Commissioner's Office 2008a). They will comply with the minimum requirements for protection, but few have the procedures and metrics in place to achieve a meaningful financial return from additional privacy protection (PricewaterhouseCoopers 2008). Thus, they will have a hard time rationalizing the allocation of resources for this purpose.

AIS researchers should study adoption issues related to firm-wide privacy strategy. For example, the study of how voluntary guidelines are adopted based on the characteristics of the implementing firms would be worthwhile, since not all firms are equally effective this way. Competitors, government regulators, and industry standard setters all may affect firm-level privacy strategy adoption decisions, just as much as market conditions, customer attitudes toward privacy protection, and the existence of substitutable and complementary solutions will. In addition, the effects of internal factors such as corporate culture, ethical positioning, and top management's perspectives have not been fully investigated, related to the strategies for information privacy protection that firms choose to employ. We know that different types of firms face different situations, and regulations and will require different information privacy protection strategies. So understanding the factors that influence their choices will provide managers with a better understanding of the adoption issues surrounding information privacy strategy.

[5] Different approaches have been proposed to protect information privacy in databases. Query restriction produces a correct answer to a query or refuses to provide any answer. It limits the types of queries and the level of analysis, so that only statistical information, not confidential individual data, is revealed to users. Different methods such as limiting query set size, controlling the overlap among the queries, auditing series of queries performed, and partitioning have been employed to implement query restriction (Adam and Wortmann 1989; Chin and Ozsoyoglu 1982). Data perturbation, in contrast, responds to queries with answers that are only statistically correct, but may not be true for individuals (Garfinkel et al. 2002). No original values in a database change, so data accuracy will be maintained. It does so by adding random noise to database query outputs so that confidential information can be protected. Additive and multiplicative data perturbation create perturbed data by using the covariance between a confidential data set and the perturbed data set (Muralidhar et al. 1995, 1999, 2001). Again, the original data values are unchanged. This data storage perspective assumes that users have legitimate access to the data stored in databases, but with different access rights. It does not consider other privacy-enhancing technologies, such as intrusion detection systems, that aim to deter intruders though (Cavusoglu et al. 2004). Nor does it consider the implementation of database query tools that preserve anonymity (Gavish and Gerdes 1998)—for example, for health care patients—yet permits an analyst to pull out relevant case-related and population-related data for closer scrutiny (Garfinkel and Goes 2002). The emergence of these other methods makes decision making more difficult.

Even though the introduction of many regulations and guidelines seems to have increased firms' awareness and ability to react to recent privacy issues, key questions still remain unanswered. Why are privacy problems so prevalent, even when there are so many related regulations and guidelines? Regulations and guidelines alone apparently do not address all the recent privacy issues, because firms consistently underinvest in information privacy protection. AIS researchers should conduct research on the factors that affect firm decision making about their information privacy protection investments. New theoretical perspectives are needed to obtain a clearer picture about the key factors. For example, Culnan and Williams (2009) argue that one reason underlying the existence of so many privacy problems is that managers typically do not consider the firms' ethical and moral responsibility for protecting the personal information they collect from consumers. The authors also make a number of recommendations for changing that situation, along with claims that doing so would yield tangible benefits. AIS researchers should empirically test those claims. In doing so, it might be useful to consider how differences in culture and regulatory regime affect managerial attitudes.

How Should Firms Establish Appropriate Investment Levels for Information Security?

Failure to achieve proper protection for customer information subjects a firm to risk and liability (Straub and Collins 1990; Menon and Sarkar 2007). Although managers may recognize the importance of protecting customer information, it is often difficult and costly to do, because the activities of collecting, storing, and analyzing personal information span the spectrum of a firm's operations. To address these issues, there has been research on the direct economic and financial effects on the firm, resulting from privacy violations that are permitted to occur (Cavusoglu et al. 2004; Acquisti et al. 2006). Contrary to other problems where the value of information is well defined, the value of protecting against the potential loss of customer information is difficult to quantify, but still critically important (Acquisti et al. 2006). Losses from information security and customer privacy breaches can be potentially significant, and their recovery may require an unspecified length of time (Crothers 2009). Yet, the manner in which senior management and employees understand information privacy issues will shape their approach to formulating strategy.

Building the financial rationale for information privacy protection investments begins with cost-benefit analysis. Its goal is to justify investments in information security and data privacy solutions to be used within a firm and across its boundaries to mitigate risk. Cost-benefit assessments of information privacy strategies most often are framed in terms of how to cope with environmental uncertainty. The uncertainty includes the unpredictable risks of privacy breaches, maintaining control to avoid improper use of consumer information, and ensuring that sensitive data are not lost (Sarathy and Robertson 2003).

Game theory provides a useful modeling and theoretical basis to create insights for understanding how firms ought to protect their customers' private data from those who would acquire and exploit it. Png and Wang (2009) have evaluated how firms should structure the analysis of value-optimizing managerial actions to minimize the risks they face of losing their customers' private information and their own internal data, as hackers seek to break their defenses. Their game-theoretic approach encourages managers to understand that investments must be made with Nash equilibrium outcomes in mind, a perspective that emphasizes the behavioral aspects of decision making in complex competitive environments. Other game-theoretic research has shown that investments in information privacy can actually create leverage for other value-creation processes that are constrained by the risk of private information loss (Longstaff et al. 2000; Schechter and Smith 2003), similar to the manner that the diminution of informational asymmetries enhances the value of financial market mechanisms and economic exchange.

Financial risk management theory provides another means of justifying information privacy protection investments, and analyzing the related costs and benefits. Gordon and Loeb (2002) used an economic model to determine the optimal investment required to protect a firm's information. They reported several key results. They showed that, in the presence of limited financial resources for investment, value-maximizing decision making should focus on protecting information assets with "mid-range" vulnerability. The protection of highly vulnerable information is too expensive, and the likelihood of achieving a return on investment will be low. By the same token, investment in the protection of lower-vulnerability information is unlikely to produce returns, since the likelihood of its loss is not high. Second, they showed that it never pays to invest to protect customer information fully; instead, maintaining some degree of vulnerability, paradoxically, will be value maximizing for the firm. Soo Hoo (2000) formulated an alternate decision-analysis approach to provide evidence for the value of different information security safeguards based on the annual loss-expectancy value, in the presence of perfect and imperfect information on loss-generating events. This permits management analysts to connect information privacy investments with their firm's budget cycle, and, in light of the evolution of technology, market, and regulatory conditions.

These also will provide a basis for "new measures [that] may become necessary to meet acceptable levels of protection," related to Criterion 8.2.5, Transmitted Personal Information (AICPA/CICA 2009, 53–54). One of the principles in GAPP is a governance concept called "Management." Several of the criteria can be helpful in considering risk management of privacy processes. Specifically, Criterion 1.2.4 requires that a risk assessment process is used to establish a risk baseline and to, at least annually, identify new or changed risks to personal information and to develop and update responses to such risks. Also, Criterion 1.2.5 requires that contracts be periodically reviewed to ensure that the privacy policies and procedures are not in violation of any such contract and hence increase the risk. Finally, if a breach does occur, Criterion 1.2.7 requires that organizations have a defined and implemented privacy incident and breach management program in place.

Jorion (2000), who suggested the use of value-at-risk theory from financial economics, offered a poignant and useful approach for risk management assessments of information privacy-protecting investments. He noted that traditional risk management approaches consider only the mean values of the various risk drivers. The value-at-risk approach, in contrast, considers the mean value and the related distribution of a loss function at a given confidence interval. By looking at both extreme outcomes and average outcomes, the value-at-risk approach offers firms a pragmatic, yet theory-based means to maximize the value of their information privacy-related technology spending. It will help them to know how much they will lose, based on how much they invest in information privacy protection, with what probability. Moreover, they can set their own targets and controls, just as financial market investors set stop-loss thresholds for their operations in changing and risky financial markets. Based on these ideas, we see the increasing "financification" of corporate strategy, related to information privacy protection, and the growing efforts of the consulting firms that inform the approaches that chief financial officers must take to get this right.

Wang et al. (2008) utilized value-at-risk theory to derive a model to measure firm-level information security risk, and applied extreme value analysis to estimate the value-at-risk of daily financial losses due to security breaches. Their empirical results represent one of the first attempts to gauge the impacts of information privacy problems on the market value of the firm. Lee et al. (2010) also developed a value-at-risk approach to model investment choices in information privacy protection. They showed why the typical approach to financial investment for information privacy that is most often used is misleading. They emphasized that the optimal investment choice should not be a point estimate. Instead, it is necessary to think in terms of an "efficient interval" for investments in information security technology solutions. Anywhere within this interval represents a value-maximizing managerial choice of investment, based on the simultaneous evaluation of risk

and profit, reflecting an understanding of the critical role of the probability-density function of the likelihood of information privacy breaches. Before a criterion-investment threshold is reached, the firm will inefficiently invest in information security protection, making it vulnerable to substantial losses that could occur at any time. Information security-related technology investments beyond the efficient level will not permit the firm to maximize its risk-adjusted profitability.[6]

The research agenda that is called for with respect to the business practice issues that we have discussed will be important for AIS researchers, in association with theory and methods from finance, economics, and management science. AIS researchers have an opportunity to contribute knowledge about the issues related to information privacy that financial investments should address. Moreover, AIS researchers work at the epicenter of policy development for such important approaches to the management of information privacy as GAPP. Yet, most economists and financial analysts will offer different critiques about the business value versus the social value of the implied managerial controls and process changes that need to be put into place. Our belief, however, is that there is a harmony of interests that can be pursued. Creating a research agenda that aims to build the basis for understanding what it will take to maximize a firm's profits and the related social welfare represents a key concern. This is true for environmental sustainability, for financial responsibility, and now—as we propose it—for meaningful social and business policies for consumer information security and privacy that are founded on sound principles.

The action items for carrying out such an agenda from this perspective are immediate. AIS researchers need to become involved with the research efforts of the major IT companies, the major financial strategy consultancies, and leading economics and finance researchers who are exploring the cutting edge of risk management and technology investment valuation tools and perspectives. Second, it will be important for them to conduct research about the information requirements that such new valuation perspectives mandate, so that it is possible to align the practice of information privacy protection decision making with other key modes of governance for resource allocation within firms. Third, similar to what happened in the mid-1990s, when emerging valuation perspectives caused the firm's IT leadership to rethink their approaches, so is it now the case that AIS professionals who formulate and implement accounting policy for information privacy will benefit by obtaining the most up-to-date knowledge about the fundamental changes in valuation methods that will inform their work.

V. THE INDIVIDUAL PRIVACY AND CONSUMER BEHAVIOR PERSPECTIVE

We next review research on individuals' decision processes about privacy. We will focus on the role of individuals as consumers because, in this setting, individuals have the most opportunity to make choices about whether and how much personal information to disclose. As employees, individuals are required to provide their employers with certain kinds of personal information—names, addresses, Social Security numbers, number of dependents, etc. for payroll and benefits

[6] Complementary technology investments in support of public firms' business processes are critical for them to effectively implement the safeguards associated with Sarbanes-Oxley Act compliance, especially Section 404, which pertains to the effectiveness of manual and automated internal controls in the creation of the firm's financial requirements (Damianides 2004). The approach is often guided by the tenets of the Committee of Sponsoring Organizations of the Treadway Commission (COSO) on internal control and enterprise risk management. However, Kermis and Kermis (2009) point out that the Section 404 provisions of the Sarbanes-Oxley Act and information privacy laws have been ineffective in preventing instances of privacy misconduct, such as the loss of consumer credit card information at ChoicePoint and T.J. Maxx. Consequently, further research on how firms use frameworks, including COSO, Control Objectives for Information and Related Technologies (COBIT), and the International Standards Organization (ISO) standards, to guide their investments in privacy controls is warranted For additional discussion of these issues, the interested reader should see Boritz (2002), IT Governance Institute (2006, 2007), and Weidenmier and Ramamoorti (2006).

processing. As citizens, individuals must provide certain kinds of information to government agencies—financial information to the Internal Revenue Service, Social Security numbers, etc. As consumers though, individuals are also required to provide information that is needed to complete business transactions. For example, when making purchases, customers must provide such information as their name, bill-to and ship-to addresses, and payment-related data, including their credit card numbers. However, unlike employees, consumers are also often asked to provide businesses with even more personal information about their interests, preferences, beliefs, and activities. Although government agencies may sometimes ask for similar information as part of a census, this happens much less frequently than do requests from businesses for personal information; and the former have greater resources at their disposal to protect individual privacy.

Businesses seek information from consumers in order to personalize services and products, as well as to develop more targeted advertising promotions, which supports their efforts to achieve high profits. In deciding whether to comply with requests to disclose personal information, individuals must weigh the potential benefits (personalized service, price reductions, etc.) against the potential risks that firms may misuse or fail to protect that information adequately (disclosure of embarrassing information, identity theft, etc.). There is evidence that offers to personalize services increases privacy concerns (Sheng et al. 2008). To cope with those concerns, individuals are forced to choose among several options: sharing accurate information with firms, providing misleading information, or refusing to disclose it entirely (Milne et al. 2004). Table 3 lists the key research questions, selected references, and basic findings of prior research on how individuals make these decisions in such contexts. Once again, we again refer the reader to Appendix B, which includes additional research questions that are specifically related to the Generally Accepted Privacy Principles.

What Is the Nature of Beliefs and Attitudes about Privacy?

One important stream of IS research on consumer information privacy behavior has sought to understand the nature of individuals' attitudes, beliefs, and concerns about privacy. Smith et al. (1996) developed and validated an instrument for the construct "CFIP," to measure individuals' concerns about information privacy, reflecting attitudes and beliefs about the effect of the firm's information privacy practices. Their construct consists of four related factors: attitudes about the collection of personal information, unauthorized secondary use, accuracy, and controls over access to that information. Stewart and Segars (2002) demonstrated that the four factors could be parsimoniously represented as one second-order factor.

Whereas the CFIP is designed to measure individual concerns about formal information privacy practices in general, Malhotra et al. (2004) focused on privacy concerns associated with online companies in particular. Using social contract theory, the authors developed and validated an evaluative instrument consisting of three factors: attitudes about the collection of personal information, concern for control over the use of that information, and awareness of a firm's privacy practices. The authors reported that all three factors could be represented by one second-order factor, which they called "Internet users' information privacy concerns" (IUIPC). They also presented evidence that this construct is likely to be a better predictor than CFIP for individuals' reactions to online privacy threats. Thus, prior research suggests that privacy concerns are multidimensional, but the nature of those dimensions may differ for online versus offline contexts. There is also reason to believe that individuals' privacy concerns in a specific setting can change over time, especially when they are provided with additional relevant information. For example, Angst and Agarwal (2009) investigated attitudes about electronic health records and found that people who had strong general concerns about the privacy of their personal medical information, as

TABLE 3

Overview of the Literature for the Individual Privacy Behavior Perspective

Key Questions	Selected Citations	Research Findings
What is the nature of beliefs and attitudes about privacy?	Smith et al. (1996) Stewart and Segars (2002) Malhotra et al. (2004) Dinev and Hart (2006) Pavlou et al. (2007) Angst and Agarwal (2009)	Concern for privacy is a multidimensional construct that encompasses attitudes about the collection of personal information and its subsequent management and use in the data life cycle. Privacy attitudes and beliefs exist at both a general and situation-specific level, and may vary over time and in response to additional information.
How do attitudes and beliefs affect privacy-related decisions and behavior?	Stewart and Segars (2002) Malhotra et al. (2004) Milne et al. (2004) Awad and Krishnan (2006) Dinev and Hart (2006) Van Slyke et al. (2006) Hui et al. (2007) Pavlou et al. (2007) Sheng et al. (2008) Son and Kim (2008) Xu et al. (2008)	Privacy concerns negatively influence intent to share both directly and indirectly, by reducing trust and increasing risk perceptions. There is conflicting evidence about the effects of privacy concerns on actual information-sharing behavior. Trust increases both intent to share personal information and actual sharing behavior. Risk perceptions negatively affect willingness to share personal information and trust.
How do a firm's privacy policies and practices influence individuals' behavior?	Culnan (1993) Smith et al. (1996) Culnan and Armstrong (1999) Acquisti and Grossklags (2005) Akcura and Srinivasan (2005) Ashrafi and Kuilboer (2005) Jamal et al. (2005) Rifon et al. (2005) Awad and Krishnan (2006) Dinev and Hart (2006) Kim and Benbasat (2006) Grossklags and Acquisti (2007) Pavlou et al. (2007) Tsai et al. (2007) Hann et al. (2008) Komiak and Benbasat (2008) Son and Kim (2008) Tang et al. (2008) Xu et al. (2008) D'Souza and Phelps (2009)	Disclosure of a firm's information practices increases willingness to share personal information and reduces effects of privacy concerns. Third-party assurances (e.g., web seals) may increase trust but do not increase willingness to share personal information. Monetary incentives increase willingness to share and actual sharing behavior.

measured by CFIP, changed their attitudes about such systems after receiving additional information about the potential benefits of electronic health records.

Companies, however, do attempt to collect personal information from their customers in a variety of settings, and their privacy policies must be designed to protect customers' personal information regardless of its origin. Additional research is needed to create a better understanding of the dimensions of privacy that are of concern to individuals and to refine existing instruments used

to measure those concerns. This is important because IS researchers (Dinev and Hart 2006; Pavlou et al. 2007) often do not use either of the instruments we have discussed, but instead select a subset of items to create a short single-factor scale to measure privacy concerns. Some other complications include the likelihood that the privacy attitudes of individuals as consumers may not be stable over time, especially as they gain experience or have personal problems with the loss of private information. In addition, their information privacy behaviors may be highly situational. Their information privacy behavior when they first purchase something from an online seller may differ from what we would observe when they become repeat customers. They also may be more trusting in settings with which they think they are familiar, which is unfortunate, since this is often what happens when consumer fraud occurs on the Internet.

In this light, GAPP may provide a useful framework for such research because it contains numerous normative suggestions in the form of management criteria that AIS researchers can use to interpret results of research on the structure of individuals' privacy concerns, and identify fruitful avenues for further inquiry. For example, recall that Malhotra et al. (2004) indicated that consumer awareness of a company's privacy policies is an important determinant of their overall level of privacy concern when interacting with that company. Criterion 2.2.3 states that a firm's privacy notice should "[use] clear language" (AICPA/CICA 2009, 25). Consequently, one interesting topic for research would be to compare how well individuals understand the information privacy policies of several firms, and then to assess how their level of understanding affects their overall privacy concerns. Careful reading of the management criteria associated with all ten principles of GAPP can help AIS researchers identify other specific issues worthy of research that may provide additional insights on the factors that influence individuals' privacy concerns. The resulting research may be useful in helping firms to comply with the privacy principles that are espoused, and may even lead to modifications in GAPP's management criteria. Such research can also contribute to the broader IS literature by identifying opportunities to refine and enhance the instruments used to measure privacy concerns.

Determining if GAPP contains elements not represented in existing privacy beliefs and measures, and whether the dimensions that are present tap into issues that are not reflected in GAPP, would be another worthwhile effort. The results can help to refine the privacy principles to ensure that they address issues that are truly important to individuals and, thereby, beneficial for firms. AIS researchers should refine the available instruments to measure privacy beliefs, by examining the relationship between what GAPP proposes and existing instruments that gauge consumers' concerns about information privacy.

How Do Privacy Attitudes Affect Intentions and Behavior?

Another stream of IS research has examined the effects of privacy attitudes and other perceptions on intentions and behaviors. There is some evidence that increased privacy concerns directly reduce intentions to share personal information (Dinev and Hart 2006; Stewart and Segars 2002) and adopt personalized services (Sheng et al. 2008). Other studies, however, have found that increased privacy concerns indirectly reduce intentions to share personal information (Malhotra et al. 2004) and willingness to engage in online transactions (Pavlou et al. 2007; Van Slyke et al. 2006), as we noted earlier, by reducing trust and increasing perceived risk. Thus, it appears that privacy concerns affect intentions, although additional research is needed to determine whether the relationship is direct, or mediated by other factors.

Evidence about the effect of privacy concerns on actual behavior has been mixed though. Milne et al. (2004) have indicated that privacy concerns predict self-reported levels of engaging in privacy-protecting behaviors. In addition, Pavlou et al. (2007) conducted empirical research with secondary data and showed that increased concerns about privacy are negatively related to online

purchasing behavior. In their field study of store and consumer purchases, Hui et al. (2007) could not corroborate the prior evidence on the relationship between privacy concerns and the amount of personal information participants actually shared with online merchants, however. Thus, a need exists for additional research into the relationship between privacy concerns and actual behaviors.

In addition to privacy concerns, prior research has also examined the influence of risk perceptions and trust on intentions and behaviors. Risk perceptions appear to affect intent to provide personal information in a negative way (Awad and Krishnan 2006; Dinev and Hart 2006; Malhotra et al. 2004; Son and Kim 2008) and willingness to transact with e-retailers (Van Slyke et al. 2006). Perceived risk also reduces trust (Dinev and Hart 2006), which is important because trust is positively related not only to intent to share personal information (Van Slyke et al. 2006), but also to the actual sharing of such information with an online merchant (Hui et al. 2007), and purchase behavior (Van Slyke et al. 2006).

More generally, the nature of the relationship between privacy concerns, risk perceptions, and trust remains unclear. Some studies have shown that privacy concerns increase risk perceptions (Pavlou et al. 2007; Van Slyke et al. 2006), but other studies have found that perceptions about the riskiness of divulging personal information to websites increases privacy concerns (Dinev and Hart 2006; Xu et al. 2008). Similarly, there is evidence that privacy concerns reduce trust (Malhotra et al. 2004), but also evidence that trust decreases concerns about privacy (Pavlou et al. 2007). Research is needed to disentangle the complex inter-relationships among privacy concerns, risk perceptions, and trust.

As with research into the nature of privacy concerns, AIS researchers may be able to draw upon the tenets of GAPP to uncover ways to contribute to theory and to practice. For example, Criterion 4.2.2 states that management should ensure that "personal information is obtained (a) fairly, without intimidation or deception, and (b) lawfully" (AICPA/CICA 2009, 33). In addition, Criterion 7.2.3 points out that "personal information is disclosed to third parties for new purposes or uses only with the prior implicit or explicit consent of the individual" (AICPA/CICA 2009, 46). AIS researchers have an opportunity to design experiments to determine what is considered to be "obtained fairly" by consumers, and whether adherence to such criteria and others increases trust, and reduces risk perceptions and privacy concerns. Related to Criterion 7.2.3, they also should undertake research that will examine what consumers and firms perceive as being a "new" use of information and whether the perceptions among members of the two groups are aligned or diverse.

How Do Privacy Policies and Practices Influence Individual Behavior?

Firms want to obtain personal information from existing and potential customers to increase sales, by providing customized goods and services and targeting their advertising expenditures to those people most likely to respond. It is possible to use monetary (Acquisti and Grossklags 2005; Grossklags and Acquisti 2007; Hui et al. 2007) and non-monetary (Dinev and Hart 2006; Pavlou et al. 2007) incentives to entice people to share their personal information. Firms will not need to do so if they can create positive perceptions about fairness, however.

As a result, it is important to study and understand what drives perceptions about the disclosure of privacy practices. The available evidence suggests that perceptions about the fairness of a firm's information privacy practices influence people's willingness to share personal information (Culnan and Armstrong 1999; Son and Kim 2008). Such perceptions depend on knowledge of the firm's privacy practices. Thus, many firms will voluntarily disclose why they collect certain information, and how they will use and protect it. Indeed, GAPP principles require businesses to inform individuals about the firm's privacy policies (Criterion 2.1.1; AICPA/CICA 2009, 23) and to describe the types of information being collected (Criterion 4.1.1; AICPA/CICA 2009, 31).

Empirical evidence also indicates that such disclosures are beneficial. In a field experiment, for example, Hui et al. (2007) found that participants who visited a website that displays a privacy

statement disclosing the merchant's privacy policies tend to provide more personal information than do participants who visited a website that does not display a privacy statement. In a controlled laboratory experiment, Tsai et al. (2007) reported that participants who visited a website that provides information about its privacy policies and practices seem to purchase items more often. Even more important, they showed that participants were willing to pay a higher price to purchase items from a website that displays its privacy policies. Also, Awad and Krishnan (2006) conducted a survey of online consumers and learned that those who most desired information about a firm's privacy policies and practices (and who also had the most concerns about privacy) were less likely to agree to be profiled so they could receive personalized products. Thus, the effects of disclosing privacy policies may differ across market segments, since consumers seem to evince heterogeneous levels of sensitivity to information privacy.

The content of such disclosures, especially the company's specific privacy policies and practices, also appears to be important. As we noted earlier, the unauthorized secondary use of personal information is an important component of privacy concerns (Smith et al. 1996). Most people view unauthorized use of personal information, particularly for cross-selling, in a negative way (Culnan 1993). Consequently, Criterion 7.1.1 requires businesses to inform consumers if their personal information being collected will be shared with third parties, and further processed for additional sharing and secondary uses, as occurs in marketing and advertising programs (AICPA/CICA 2009, 44). Interestingly, the evidence indicates that even with such notice, people react negatively to the sharing of their personal information with third parties. D'Souza and Phelps (2009) showed that people are less likely to buy from a company that discloses that it will share their personal information with third parties. Moreover, they found that people are less sensitive to price when shopping at companies that promise not to share their personal information. This suggests that consumers may be willing to pay a premium for increased information privacy protection.

Efforts to avoid unwanted marketing, however, are costly and unpleasant for consumers and firms (Hann et al. 2008). Thus, it is not surprising that analytical modeling research has shown that a firm can maximize its profits by credibly committing to a specific level of cross-selling (Akcura and Srinivasan 2005), and can influence consumer beliefs by sending unambiguous signals about its intentions to protect privacy (Tang et al. 2008). Moreover, in a survey of university students, Xu et al. (2008) reported that perceptions about the effectiveness of a website's privacy policies will assuage consumer privacy concerns by reducing perceptions about the risk they face of having their personal information divulged. There also were perceptions of loss of control over the collection and use of that information. Therefore, it is important to study ways that firms can increase the credibility of their privacy policies.

One possibility that has been explored extensively in the literature and in practice is to obtain independent assurance from a third party that a firm is complying with a trust assurance provider's policies (Kim et al. 2008b). See Boritz and No (2011) for additional coverage of this issue in the electronic commerce context. Such assurance can be displayed online in the form of a web privacy seal, such as TRUSTe, BBBOnline, EuroPriSe, buySAFE, and WebTrust (Benassi 1999; Gendron and Barrett 2004). Although these seals do not have the force of law, they may be effective in changing people's attitudes and expectations about what firms are doing (and should do) to protect privacy (Shapiro and Baker 2001). The results of empirical research on consumer reactions to seals have been mixed though (Ashrafi and Kuilboer 2005; Rifon et al. 2005; Hui et al. 2007; Xu et al 2008), and practitioners and academic observers around the world express skepticism that such signaling approaches are of value. AIS researchers can explore which GAPP criteria increase or reduce trust, and then investigate how changing the explicit set of assertions provided by a web privacy seal to include additional trust-building (Kim and Benbasat 2006) and distrust-reducing (Komiak and Benbasat 2008) elements affects consumer perceptions. They also should investigate how firms can most effectively increase their employees' compliance with the firm's stated information privacy policies.

Once again, GAPP management criteria and the related procedures that have been suggested can provide guidance about specific practices to test. For example, Criterion 1.1.2 requires that "responsibility and accountability are assigned to a person or group for developing, documenting, implementing, enforcing, monitoring, and updating the entity's privacy policies." In addition, Criterion 1.2.10 discusses the need for "a privacy awareness program about the entity's privacy policies . . . and specific training for selected personnel" (AICPA/CICA 2009, 21). AIS researchers should examine various accountability methods, the consequences for employees due to non-compliance, and what remediation processes might be put in place. They could then experimentally examine how such various methods of enforcement and remediation affect employee compliance as well as consumer trust.

Beyond these, Criterion 8.2.7 calls for "tests of the effectiveness of the key administrative, technical, and physical safeguards protecting personal information" (AICPA/CICA 2009, 55); and Criterion 10.2.5 requires that "ongoing procedures are performed for monitoring the effectiveness of controls over personal information . . . and for taking timely corrective actions where necessary" (AICPA/CICA 2009, 64). The risk of data breaches, unfortunately, can only be reduced; they can never be completely eliminated. Therefore, firm-level incident response plans will be a key internal element for effective control. Moreover, the existence of such plans and their impact on consumer trust levels can be studied by AIS researchers in an effort to determine appropriate risk-reduction processes. The results of such research will not only be of potential interest to firms interested in increasing their customers' willingness to share personal information, but will also contribute to the IS literature on privacy. They may even facilitate further refinement of the Generally Accepted Privacy Principles.

VI. CONCLUSION

This article has presented an extensive review of prior research on consumer information privacy and identified numerous fruitful directions where AIS researchers can contribute. We focused on the relationship between individuals as consumers and the firms with which they share personal information. We also examined the issues and challenges arising in the privacy domain through different perspectives, supported by various theories and findings from the IS and AIS literature, and other interdisciplinary sources. The perspectives from which we analyzed the privacy issues included the societal and public policy perspective, the business practices perspective, and the individual privacy and consumer behavior perspective. The theories we have drawn upon include the multiple stakeholder theory of privacy, cultural lag theory, game theory, financial risk management theory, social contract theory, and others.

From the societal and public policy perspective, the main research directions that we have identified relate to the social welfare implications of personal information surveillance, the safeguards needed at the societal level, and the privacy-enhancing regulations that should especially target ITs that may affect consumer information privacy. From the business practices perspective, we suggested research directions that involve the examination of factors influencing choices of privacy practices. We also offered some ways to discover how firms can leverage their investments in information privacy. The individual and consumer behavior perspective, in turn, prompts AIS researchers to look at the nature of people's beliefs and attitudes about privacy, the ways such attitudes affect their intentions and behaviors, and how individuals' behaviors can be influenced by information privacy policies and practices. Throughout the review, we proposed a number of specific questions for future research that are derived from the aforementioned directions and aligned with the GAPP framework.

A benefit of studying information privacy issues with a focus on the relationship between individuals as consumers and the firms with which they share personal information about

themselves, through the different perspectives that we have proposed, is that the resulting review is temporally robust to the emergence of disruptive technologies, changing societal expectations, and new privacy-enhancing and privacy-robbing technologies (Au and Kauffman 2008). Consider, for example, recent developments such as cloud computing (Breuning and Treacy 2009) and the growth of social networks (Solove 2008). Instead of approaching such new uses of IT in isolation, AIS researchers can draw on the various theoretical perspectives in this review to understand different ways in which those developments might affect privacy and to identify questions and solutions that are worthy of research. Thus, many opportunities exist for conducting socially meaningful and forward-looking research on information privacy going forward. We encourage AIS researchers to play a leadership role in setting the agenda. At the same time, we exhort them to develop this agenda by building upon the understanding of the contrasting global perspectives that we have tried to characterize and explain in our present research.

REFERENCES

Acquisti, A., A. Friedman, and R. Telang. 2006. *Is There a Cost to Privacy Breaches? An Event Study*. Proceedings of the 27th Annual International Conference on Information Systems, Milwaukee, WI.

Acquisti, A., and J. Grossklags. 2005. *Uncertainty, Ambiguity, and Privacy*. Proceedings of the 4th Workshop on Economics and Information Security, Carnegie-Mellon University, Pittsburgh, PA.

Adam, N. R., and J. C. Wortmann. 1989. Security-control methods for statistical databases: A comparative study. *ACM Computing Surveys* 21 (4): 515–556. doi:10.1145/76894.76895

Aguilar, J. R. 1999–2000. Over the rainbow: European and American consumer protection policy and remedy conflicts on the Internet and a possible solution. *International Journal of Communications of Law and Policy* 4 (Winter): 1–57. Available at: http://www.ijclp.net/issue_4.html

Akcura, M. T., and K. Srinivasan. 2005. Research note: Customer intimacy and cross-selling strategy. *Management Science* 51 (6): 1001–1012.

Alderman, E., and C. Kennedy. 1995. The Right to Privacy. New York, NY: Alfred A. Knopf.

American Institute of Certified Public Accountants and the Canadian Institute of Chartered Accountants (AICPA/CICA). 2003. Suitable Trust Services Criteria and Illustrations. New York, NY: AICPA/CICA.

American Institute of Certified Public Accountants and the Canadian Institute of Chartered Accountants (AICPA/CICA). 2004. Understanding and Implementing Privacy Services. New York, NY: AICPA/CICA.

American Institute of Certified Public Accountants and the Canadian Institute of Chartered Accountants (AICPA/CICA). 2006. *Generally Accepted Privacy Principles: A Global Framework*. New York, NY: AICPA/CICA.

American Institute of Certified Public Accountants and the Canadian Institute of Chartered Accountants (AICPA/CICA). 2009. *Generally Accepted Privacy Principles: CPA and CA Practitioner Version*. New York, NY: AICPA/CICA.

Angst, C. M., and R. Agarwal. 2009. Adoption of electronic health records in the presence of privacy concerns: The elaboration likelihood model and individual persuasion. *Management Information Systems Quarterly* 33 (2): 339–370.

Ashrafi, N., and J. Kuilboer. 2005. Online privacy policies: An empirical perspective on self-regulatory practices. *Journal of Electronic Commerce in Organizations* 3 (4): 61–74.

Au, Y. A., and R. J. Kauffman. 2008. The economics of mobile payments: Understanding stakeholder issues for an emerging financial technology application. *Electronic Commerce Research and Applications* 7 (2): 141–164. doi:10.1016/j.elerap.2006.12.004

Awad, N. F., and M. Krishnan. 2006. The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization. *Management Information Systems Quarterly* 30 (1): 13–28.

Bapna, S., and A. Gangopadhyay. 2006. A wavelet-based approach to preserve privacy for classification mining. *Decision Sciences* 37 (4): 623–642. doi:10.1111/j.1540-5414.2006.00141.x

Bavis, C., and M. Parent. 2007. Data theft or loss: Ten things your lawyer must tell you about handling information. *Ivey Business Journal* (July–August): 1–9.

Bellman, S., E. J. Johnson, and G. L. Lohse. 2001. On site: To opt-in or opt-out? It depends on the question. Communications of the ACM 44 (2): 25–27. doi:10.1145/359205.359241

Benassi, P. 1999. TRUSTe: An online privacy seal program. *Communications of the ACM* 42 (2): 56–59. doi:10.1145/293411.293461

Boritz, J. E. 2002. Information systems assurance. In Research Accounting as an Information Systems Discipline, edited by Arnold, V., and S. G. Sutton. Sarasota, FL: American Accounting Association.

Boritz, J. E., and W. G. No. 2011. E-commerce and privacy: Exploring what we know and opportunities for future discovery. *Journal of Information Systems* 25 (2): 11–45.

Breuning, P. J., L. J. Sotto, M. E. Abrams, and F. H. Cate. 2008. Strategic information management. Privacy and Security Law Report 7 (36): 1361–1363.

Breuning, P. J., and B. C. Treacy. 2009. Privacy, security issues raised by cloud computing. *Privacy and Security Law Report* 8 (10): 1–4.

Brown, M., and R. Muchira. 2004. Investigating the relationship between Internet privacy concerns and online purchase behavior. *Journal of Electronic Commerce Research* 5 (1): 62–70.

Cain, R. M. 2002. Global privacy concerns and regulation: Is the United States a world apart? *International Review of Law, Computers & Technology* 16 (1): 23–34. doi:10.1080/13600860220136084

Cate, F. H. 1997. Privacy in the Information Age. Washington, D.C.: Brookings Institution.

Caudill, E. M., and P. E. Murphy. 2000. Consumer online privacy: Legal and ethical issues. *Journal of Public Policy & Marketing* 19 (1): 7–19. doi:10.1509/jppm.19.1.7.16951

Cavoukian, A. 2009. *Privacy by Design*. Toronto, Canada: Information and Privacy Commission of Ontario.

Cavusoglu, H., B. Mishra, and S. Raghunathan. 2004. The effect of Internet security breach announcements on market value: Capital market reactions for breached firms and Internet security developers. *International Journal of Electronic Commerce* 9 (1): 69–104.

Chin, R. Y., and G. Ozsoyoglu. 1982. Auditing and inference control in statistical databases. *IEEE Transactions on Software Engineering* 8 (6): 574–582. doi:10.1109/TSE.1982.236161

Clarke, R. 1999. Internet privacy concerns confirm the case for intervention. *Communications of the ACM* 42 (2): 60–67. doi:10.1145/293411.293475

Clarke, R. A. 2006. Introduction to dataveillance and information privacy, and definitions of terms. Available at: http://www.rogerclarke.com/DV/Intro.html

Clarke, R. A. 2008. Privacy impact assessment in Australian contexts. *Murdoch eLaw Journal* 15(1). Available at: https://elaw.murdoch.edu.au/archives/issues/2008/elaw_15_1_Clarke.pdf

Clarke, R. A. 2009. Privacy impact assessment: Its origin and development. *Computer Law & Security Report* 25 (2): 123–135. doi:10.1016/j.clsr.2009.02.002

Connolly, C. 2010. FTC enforcement against false safe harbor claims. Available at: http://www.galexia.com/public/research/articles/research_articles-art56.html

Council of Europe. 1950. *Convention for the Protection of Human Rights and Fundamental Freedoms*. Rome, Italy: Council of Europe. Available at: http://conventions.coe.int/treaty/en/Treaties/Html/005.htm

Cranor, L. F. 1999. Internet privacy. *Communications of the ACM* 42 (2): 28–38. doi:10.1145/293411.293440

Crothers, B. 2009. Intel finds stolen laptops can be costly. Available at: http://news.cnet.com/8301-13924_3-10225626-64.html

Culnan, M. J. 1993. How did they get my name? An exploratory investigation of consumer attitudes toward secondary information use. *Management Information Systems Quarterly* 17 (3): 341–363.

Culnan, M. J. 2000. Protecting privacy online: Is self-regulation working? Journal of Public Policy & Marketing 19 (1): 20–26. doi:10.1509/jppm.19.1.20.16944

Culnan, M. J., and P. K. Armstrong. 1999. Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science* 10 (1): 104–115. doi:10.1287/orsc.10.1.104

Culnan, M. J., and R. J. Bies. 2003. Consumer privacy: Balancing economic and justice considerations. *The Journal of Social Issues* 59 (2): 323–342. doi:10.1111/1540-4560.00067

Culnan, M. J, and G. R. Milne. 2001. The Culnan-Milne survey of consumers and online privacy notices. Available at: http://intra.som.umass.edu/georgemilne/PDF_files/culnan-milne.pdf

Culnan, M. J., and C. C. Williams. 2009. How ethics can enhance organizational privacy: Lessons from the ChoicePoint and TJX data breaches. *Management Information Systems Quarterly* 33 (4): 673–688.

Damianides, M. 2004. How does SOX change IT? *Journal of Corporate Accounting & Finance* 15 (6): 35–41. doi:10.1002/jcaf.20054

David, J. S., and M. Prosch. 2010. Extending the value chain to incorporate privacy by design principles. *Identity in the Information Society* 3 (1): 295–318. doi:10.1007/s12394-010-0059-6

Dinev, T., and P. Hart. 2006. An extended privacy calculus model for e-commerce transactions. *Information Systems Research* 17 (1): 61–80. doi:10.1287/isre.1060.0080

D'Souza, G., and J. E. Phelps. 2009. The privacy paradox: The case of secondary disclosure. *Review of Marketing Science* 7(4). Available at: http://ideas.repec.org/a/bpj/revmkt/v7y2009i1n4.html

Federal Trade Commission. 2000. *Self-Regulation and Privacy Online: A Report to Congress*. Washington, D.C.: Federal Trade Commission. Available at: http://www.ftc.gov/privacy

Garfinkel, R., R. Gopal, and P. Goes. 2002. Privacy protection of binary confidential data against deterministic, stochastic, and insider threat. *Management Science* 48 (6): 749–764. doi:10.1287/mnsc.48.6.749.193

Garfinkel, R., R. Gopal, and S. Thompson. 2007. Releasing individually identifiable microdata with privacy protection against stochastic threat: An application to health information. *Information Systems Research* 18 (1): 23–41. doi:10.1287/isre.1070.0112

Gavish, B., and J. H. Gerdes, Jr. 1998. Anonymous mechanisms in group decision support systems communication. Decision Support Systems 23 (4): 297–328. doi:10.1016/S0167-9236(98)00057-8

Gendron, Y., and M. Barrett. 2004. Professionalization in action: Accountants' attempt at building a network of support for the WebTrust seal of assurance. Contemporary Accounting Research 21 (3): 563–602. doi:10.1506/H1C0-EU27-UU2K-8EC8

Gordon, L. A., and M. P. Loeb. 2002. The economics of information security investment. *ACM Transactions on Information and System Security* 5 (4): 438–457. doi:10.1145/581271.581274

Greenaway, K. A., and Y. E. Chan. 2005. Theoretical explanations for firms' information privacy. *Journal of the Association for Information Systems* 6 (6): 171–198.

Greenstein, M. M., and J. E. Hunton. 2003. Extending the accounting brand to privacy services. *Journal of Information Systems* 17 (2): 87–110. doi:10.2308/jis.2003.17.2.87

Grossklags, J., and A. Acquisti. 2007. *When 25 Cents Is Too Much: An Experiment on Willingness-to-Sell and Willingness-to-Protect Personal Information*. Proceedings of the 6th Workshop on Economics and Information Security, Carnegie-Mellon University, Pittsburgh, PA.

Grossman, S. J., and O. D. Hart. 1986. The costs and benefits of ownership: A theory of vertical and lateral integration. *The Journal of Political Economy* 94 (4): 691–719. doi:10.1086/261404

Hann, I. H., K. L. Hui, S. Y. T. Lee, and I. P. L. Png. 2007. Overcoming online information privacy concerns: An information-processing theory approach. *Journal of Management Information Systems* 24 (2): 13–42. doi:10.2753/MIS0742-1222240202

Hann, I. H., K. L. Hui, S. Y. T. Lee, and I. P. L. Png. 2008. Consumer privacy and marketing avoidance: A static model. *Management Science* 54 (6): 1094–1103. doi:10.1287/mnsc.1070.0837

Hart, O., and J. Moore. 1990. Property rights and the nature of the firm. *The Journal of Political Economy* 98 (6): 1119–1157. doi:10.1086/261729

Hoffman, D. L., T. P. Novak, and M. Peralta. 1999. Building consumer trust online. *Communications of the ACM* 42 (4): 80–85. doi:10.1145/299157.299175

Hui, K. L., H. H. Teo, S. Yong, and S. Y. T. Lee. 2007. The value of privacy assurance: An exploratory field experiment. *Management Information Systems Quarterly* 31 (1): 19–33.

IBM Research. 2009. *Inventor's Corner: Innovations Enable Privacy by Design*. Yorktown Heights, NY: IBM. Available at: http://ibmresearchnews.blogspot.com/2009/10/inventors-corner-innovations-enable.html

Information Privacy Commissioner of Ontario. 2009. Commissioner Cavoukian expects health sector to encrypt all health information on mobile devices: Nothing short of this is acceptable. December 24. Available at: http://www.ipc.on.ca/images/Resources/2009-12-24-encrypt_phi.pdf

IT Governance Institute. 2006. IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control over Financial Reporting. 2nd edition. Rolling Meadows, IL: Information Systems Audit and Control Association.

IT Governance Institute. 2007. *COBIT 4.1*. Rolling Meadows, IL: Information Systems Audit and Control Association. Available at: http://www.isaca.org/Knowledge-Center/cobit/Documents/CobiT_4.1.pdf

Jamal, K., M. Maier, and S. Sunder. 2005. Enforced standards versus evolution by general acceptance: A comparative study of e-commerce privacy disclosure and practice in the United States and the United Kingdom. *Journal of Accounting Research* 43 (1): 73–96. doi:10.1111/j.1475-679x.2004.00163.x

Jorion, P. 2000. Value at Risk: The Benchmark for Controlling Market Risk. Blacklick, OH: McGraw-Hill Professional Book Group.

Kalvenes, J., and A. Basu. 2006. Design of robust business-to-business electronic marketplaces with guaranteed privacy. *Management Science* 52 (11): 1721–1736. doi:10.1287/mnsc.1060.0570

Karol, T. J. 2001. Cross-border privacy impact assessments: An introduction. *Information Systems Control Journal* 3. Available at: http://www.isaca.org/Content/ContentGroups/Journal1/20012/Cross-Border_Privacy_Impact_Assessments.htm

Kermis, G. F., and M. D. Kermis. 2009. Model for the transition from ethical deficit to a transparent corporate culture: A response to the financial meltdown. *Journal of Academic and Business Ethics* 2 (1): 49–58.

Kim, D., and I. Benbasat. 2006. The effects of trust-assuring arguments on consumer trust in Internet stores: Application of Toulmin's model of argumentation. *Information Systems Research* 17 (3): 286–300. doi:10.1287/isre.1060.0093

Kim, D. J., D. L. Ferrin, and H. R. Rao. 2008a. A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. *Decision Support Systems* 44 (2): 544–564. doi:10.1016/j.dss.2007.07.001

Kim, D. J., C. Steinfield, and Y. J. Lai. 2008b. Revisiting the role of Web assurance seals in business-to-consumer electronic commerce. *Decision Support Systems* 44 (4): 1000–1015. doi:10.1016/j.dss.2007.11.007

Kirk, J. 2007. Google calls for global online privacy standard. *IDG News Service* (September 14). Available at: http://www.infoworld.com/article/07/09/14/Google-calls-for-global-online-privacy-standard_1.html

Komiak, S. Y. X., and I. Benbasat. 2008. A two-process view of trust and distrust building in recommendation agents: A process-tracing study. *Journal of the Association for Information Systems* 9 (12): 727–747.

Langheinrich, M. 2001. Privacy by design: Principles of privacy-aware ubiquitous systems. In *Proceedings of the Third International Conference on Ubiquitous Computing*, Atlanta, GA, edited by Abowd, G. D., B. Brumitt, and S. A. Shafer. Published as *Lecture Notes in Computer Science 2201*, 273–291. Berlin, Germany: Springer.

Langheinrich, M. 2002. A privacy awareness system for ubiquitous computing environments. In *Proceedings of the Fourth International Conference on Ubiquitous Computing*, Göteborg, Sweden, Borriello, G., and L. E. Holmquist. Published as *Lecture Notes in Computer Science 2498*, 237–245. Berlin, Germany: Springer.

Lee, J. K., and H. R. Rao. 2007. Perceived risks, counter-beliefs, and intentions to use anti-counterterrorism Web sites: An exploratory study of government-citizens online interactions in a turbulent environment. *Decision Support Systems* 43 (4): 1431–1449. doi:10.1016/j.dss.2006.04.008

Lee, Y. J., R. J. Kauffman, and R. Sougstad. 2011. Profit-maximizing investments in customer information security. *Decision Support Systems* (forthcoming). doi:10.1016/j.dss.2011.02.009

Lesser, K., 2010. GAPP: Generally Accepted Privacy Principles. January 19. Available at: http://information-security-resources.com/2010/01/19/gapp-generally-accepted-privacy-principles/

Levin, A., and M. J. Nicholson. 2005. Privacy law in the United States, the E.U. and Canada: The allure of the middle ground. *University of Ottawa Law and Technology Journal* 2 (2): 357–395.

Liu, C., J. T. Marchewka, J. Lu, and C. S. Yu. 2004. Beyond concern: A privacy-trust-behavioral intention model of electronic commerce. *Information & Management* 42 (1): 127–142.

Longstaff, T. A., C. Chittister, R. Pethia, and Y. Y. Haimes. 2000. Are we forgetting the risks of information technology? IEEE Computer 33 (12): 43–51.

Loshin, D. 2002. Knowledge integrity: Data ownership. As quoted in *Data Ownership*, U.S. Department of Health and Human Services. Rockville, MD: Office of Research Integrity.

Malhotra, N. K., S. S. Kim, and J. Agarwal. 2004. Internet users' information privacy concerns: The construct, the scale, and a causal model. *Information Systems Research* 15 (4): 336–355. doi:10.1287/isre.1040.0032

Margulis, S. 1977. Conceptions of privacy: Current status and next steps. *The Journal of Social Issues* 33 (3): 5–21. doi:10.1111/j.1540-4560.1977.tb01879.x

Markel, M. 2006. Safe harbor and privacy protection: A looming issue for IT professionals. *IEEE Transactions on Professional Communication* 49 (1): 1–11. doi:10.1109/TPC.2006.870462

Mason, R. O. 1986. Four ethical issues of the information age. *Management Information Systems Quarterly* 10 (1): 46–55.

McLeod, R., Jr., and J. C. Rogers. 1982. Marketing information systems: Uses in the Fortune 500. *California Management Review* 25: 106–118.

Menon, S., and S. Sarkar. 2007. Minimizing information loss and preserving privacy. *Management Science* 53 (1): 101–116. doi:10.1287/mnsc.1060.0603

Menon, S., S. Sarkar, and S. Mukherjee. 2005. Maximizing accuracy of shared databases when concealing sensitive patterns. *Information Systems Research* 16 (3): 256–270. doi:10.1287/isre.1050.0056

Milne, G. R., and M. J. Culnan. 2002. Using the content of online privacy notices to inform public policy: A longitudinal analysis of the 1998–2001 U.S. Web surveys. *The Information Society* 18 (5): 345–359. doi:10.1080/01972240290108168

Milne, G. R., A. J. Rohm, and S. Bahl. 2004. Consumers' protection of online privacy and identity. *The Journal of Consumer Affairs* 38 (2): 217–232. doi:10.1111/j.1745-6606.2004.tb00865.x

Mitrano, T., D. R. Kirby, and L. Maltz. 2005. *What Does Privacy Have to Do with It? Privacy Risk Assessment*. Presentation at the 2005 Security Professionals Conference, Washington, D.C., April 3–5.

Miyazaki, A. D., and A. Fernandez. 2000. Internet privacy and security: An examination of online retailer disclosures. *Journal of Public Policy & Marketing* 19 (1): 54–61. doi:10.1509/jppm.19.1.54.16942

Mizruchi, M. S., and L. C. Fein. 1999. The social construction of organizational knowledge: A study of the uses of coercive, mimetic, and normative isomorphism. *Administrative Science Quarterly* 44 (4): 653–683. doi:10.2307/2667051

Muralidhar, K., D. Batra, and P. J. Kirs. 1995. Accessibility, security, and accuracy in statistical databases: The case for the multiplicative fixed data perturbation approach. *Management Science* 41 (9): 1549–1564. doi:10.1287/mnsc.41.9.1549

Muralidhar, K., R. Parsa, and R. Sarathy. 1999. A general additive data perturbation method for database security. *Management Science* 45 (10): 1399–1415. doi:10.1287/mnsc.45.10.1399

Muralidhar, K., R. Parsa, and R. Sarathy. 2001. An improved security requirement for data perturbation with implications for e-commerce. Decision Sciences 32 (4): 683–698. doi:10.1111/j.1540-5915.2001.tb00977.x

Office of the United Nations High Commissioner for Human Rights. 1966. *International Covenant on Civil and Political Rights*. New York, NY: United Nations. Available at: http://www2.ohchr.org/english/law/ccpr.htm

Ogburn, W. F. 1957. Cultural lag as theory. *Sociology and Social Research* 41: 167–174.

Olivero, N., and P. Lunt. 2004. Privacy versus willingness to disclose in e-commerce exchanges: The effect of risk awareness on the relative role of trust and control. *Journal of Economic Psychology* 25 (2): 243–262. doi:10.1016/S0167-4870(02)00172-1

Oz, E. 1992. Ethical standards for information systems professionals: A case for a unified code. *Management Information Systems Quarterly* 16 (4): 423–433.

Pavlou, P. A., H. Liang, and Y. Xue. 2007. Understanding and mitigating uncertainty in online exchange relationships: A principal-agent perspective. *Management Information Systems Quarterly* 31 (1): 105–136.

Png, I. P. L., and Q. H. Wang. 2009. Information security: Facilitating user precautions vis-à-vis enforcement against attackers. *Journal of Management Information Systems* 26 (2): 97–121. doi:10.2753/MIS0742-1222260205

Price, E. 2006. *Liberty for All: Reclaiming Individual Privacy in a New Era of Public Morality*. New Haven, CT: Yale University Press.

PricewaterhouseCoopers. 2008. *Safeguarding the New Currency of Business: Findings from the 2008 Global State of Information Security Study*. New York, NY: Security Advisory Services.

Prosch, M. 2008. Protecting personal information using Generally Accepted Accounting Principles and continuous control monitoring. *International Journal of Disclosure and Governance* 5 (2): 153–166. doi:10.1057/jdg.2008.7

Reagle, J., and L. F. Cranor. 1999. The platform for privacy preferences. *Communications of the ACM* 42 (2): 48–55. doi:10.1145/293411.293455

Rensel, A. D., J. A. Abbas, and H. R. Rao. 2006. Private transactions in public places: An exploration of the impact of the computer environment on public transactional Web site use. *Journal of the Association for Information Systems* 7 (1): 19–50.

Rifon, J. J., R. LaRose, and S. M. Choi. 2005. Your privacy is sealed: Effects of Web privacy seals on trust and personal disclosures. *The Journal of Consumer Affairs* 39 (2): 339–362.

Rodriguez, S. 2009. *Online Privacy Research Lab Reveals Details about Its Work*. An Announcement about the Privacy By Design Lab at the Center for Advancing Business through Information Technology, Arizona State University, Tempe, AZ, November 24. Available at: http://www.statepress.com/node/9512

Sarathy, R., and K. Muralidhar. 2006. Secure and useful data sharing. *Decision Support Systems* 42 (1): 204–220. doi:10.1016/j.dss.2004.10.013

Sarathy, R., and C. J. Robertson. 2003. Strategic and ethical considerations in managing digital privacy. *Journal of Business Ethics* 46: 111–126. doi:10.1023/A:1025001627419

Schechter, S. E., and M. D. Smith. 2003. *How Much Security Is Enough to Stop a Thief? The Economics of Outsider Theft Via Computer Systems Networks*. Proceedings of the 7th Financial Cryptography Conference, Guadeloupe, French West Indies.

Schwaig, K. S., G. C. Kane, and V. C. Storey. 2006. Compliance to the fair information practices: How are the Fortune 500 handling online privacy disclosures? *Information & Management* 43 (7): 805–820. doi:10.1016/j.im.2006.07.003

Scofield, M. 1998. Issues of data ownership. *Information Management Magazine* (November). Available at: http://www.information-management.com/issues/19981101/296-1.html

Senden, L. 2004. Soft Law in European Community Law. Portland, OR: Hart Publishing.

Senden, L. 2005. Soft law, self-regulation and co-regulation in European law: Where do they meet? *Electronic Journal of Comparative Law* 9(1). Available at: http://www.ejcl.org

Shapiro, B., and C. R. Baker. 2001. Information technology and the social construction of information privacy. *Journal of Accounting and Public Policy* 20 (4–5): 295–322. doi:10.1016/S0278-4254(01)00037-0

Sheng, H. F., F. F. H. Nah, and K. Siau. 2008. An experimental study on ubiquitous commerce adoption: Impact of personalization and privacy concerns. *Journal of the Association for Information Systems* 9 (6): 344–376.

Smith, H. J. 1993. Privacy policies and practices: Inside the organizational maze. *Communications of the ACM* 36 (12): 104–122. doi:10.1145/163298.163349

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

Solove, D. J. 2004. *The Digital Person: Technology and Privacy in the Information Age*. New York, NY: New York University Press.

Solove, D. J. 2008. Do social networks bring the end of privacy? *Scientific American* (September). Available at: http://www.sciam.com/article.cfm?id=do-social-networks-bring.

Son, J. Y., and S. S. Kim. 2008. Internet users' information privacy-protective responses: A taxonomy and a nomological model. *Management Information Systems Quarterly* 32 (3): 503–529.

Soo Hoo, K. 2000. How much is enough? A risk management approach to computer security. Working paper, Stanford University.

Stewart, B. 1999. Privacy impact assessment: Toward a better informed process for evaluating privacy issues arising from new technologies. *Privacy Law and Policy Reporter* 5 (8): 147–149.

Stewart, K. A., and A. H. Segars. 2002. An empirical examination of the concern for information privacy instrument. *Information Systems Research* 13 (1): 36–49. doi:10.1287/isre.13.1.36.97

Stone, D. L., and E. F. Stone-Romero. 1998. A multiple stakeholder model of privacy in organizations. In *Managerial Ethics: Morally Managing People and Processes*, edited by Schminke, M., 35–59. Hillsdale, NJ: Lawrence Erlbaum Associates.

Straub, D. W., Jr, and R. W. Collins. 1990. Key information liability issues facing managers: Software piracy, proprietary databases, and individual rights to privacy. *Management Information Systems Quarterly* 14 (2): 143–156.

Tambini, D., D. Leonardi, and C. Marsden. 2008. *Codifying Cyberspace: Communications Self-Regulation in the Age of Internet Convergence*. New York, NY: Routledge.

Tang, Z., Y. Hu, and M. D. Smith. 2008. Gaining trust through online privacy protection: Self-regulation, mandatory standards, or *caveat emptor*. *Journal of Management Information Systems* 24 (4): 153–173. doi:10.2753/MIS0742-1222240406

Tene, O. 2009. Israel's data protection reform: Reduce bureaucracy, increase accountability. *Privacy and Data Protection* 10 (1): 13–15.

Tsai, J., S. Egelman, L. Cranor, and A. Acquisti. 2007. *The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study*. Proceedings of the 6th Workshop on Economics and Information Security, Pittsburgh, PA, June 6–7.

Turner, E. C., and S. Dasgupta. 2003. Privacy on the Web: An examination of user concerns, technology, and implications for business organizations and individuals. *Information Systems Management* 20 (1): 8–18. doi:10.1201/1078/43203.20.1.20031201/40079.2

U.K. Information Commissioner's Office. 2008a. *The Privacy Dividend: The Business Case for Investing in Proactive Privacy Protection*. Cheshire, U.K.: U.K. Information Commissioner's Office. Available at: http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/privacy_dividend.pdf

U.K. Information Commissioner's Office. 2008b. *Privacy by Design*. Cheshire, U.K.: U.K. Information Commissioner's Office. Available at: http://www.ico.gov.uk/upload/documents/pdb_report_html/privacy_by_design_report_v2.pdf

U.K. Information Commissioner's Office. 2010. *Lettings and Real Estate Agents Risking Legal Action, Warns ICO*. Cheshire, U.K.: U.K. Information Commissioner's Office. Available at: http://www.ico.gov.uk/upload/documents/pressreleases/2010/estate_agents_notify_08092010.pdf

United Nations. 1948. *The Universal Declaration of Human Rights*. New York, NY: United Nations. Available at: http://www.un.org/en/documents/udhr/index.shtml

U.S. Census Bureau. 2010. *Census Bureau Privacy Impact Assessments*. Washington, D.C.: U.S. Census Bureau. Available at: http://www.census.gov/po/pia/

U.S. Department of Commerce. July 21, 2000. *Safe Harbor Privacy Principles*. Washington, D.C.: Electronic Commerce Task Force, International Trade Administrations. Available at: http://www.ita.doc.gov/td/ecom/SHPRINCIPLESFINAL.htm

U.S. Department of Health and Human Services. 2010. Data Ownership. Rockville, MD: Office of Research Integrity.

U.S. Department of the Interior. 2010. *Understanding the Privacy Impact Assessment*. Presentation, Washington, D.C. Available at: http://www.doi.gob/ocip/privacy/basic_pia_overview.ppt

Van Alstyne, M., E. Brynjolfsson, and S. Madnick. 1995. Why not one big database? Principles for data ownership. *Decision Support Systems* 15 (4): 267–284. doi:10.1016/0167-9236(94)00042-4

Van Slyke, C., J. T. Shim, R. Johnson, and J. Jiang. 2006. Concern for information privacy and online consumer purchasing. *Journal of the Association for Information Systems* 7 (6): 415–443.

Vasarhelyi, M. A., M. Alles, and A. Kogan. 2004. Principles of analytic monitoring for continuous assurance. *Journal of Emerging Technologies in Accounting* 1 (1): 1–21. doi:10.2308/jeta.2004.1.1.1

Vasarhelyi, M. A., and F. B. Halper. 1991. The continuous audit of online systems. *Auditing: A Journal of Practice & Theory* 10 (1): 110–125.

Wang, J., A. Chaudhury, and H. R. Rao. 2008. A value-at-risk approach to information security investment. *Information Systems Research* 19 (1): 106–123. doi:10.1287/isre.1070.0143

Warren, S., and L. Brandeis. 1890. The right to privacy. *Harvard Law Review* 4 (5): 193–220. doi:10.2307/1321160

Warren, A., A. Bayley, C. Bennett, R. Charlesworth, R. Clarke, and C. Oppenheim. 2008. Privacy impact assessments: International experience as a basis for U.K. guidance. *Computer Law & Security Report* 24 (3): 233–242. doi:10.1016/j.clsr.2008.03.003

Weidenmier, M. L., and S. Ramamoorti. 2006. Research opportunities in information technology and internal auditing. *Journal of Information Systems* 20 (1): 205–219. doi:10.2308/jis.2006.20.1.205

Westin, A. 1967. *Privacy and Freedom*. New York, NY: Athenum.

Winn, J. K. 2011. Electronic commerce law: Direct regulation, co-regulation and self-regulation. *Cahiers du CRID* (forthcoming).

Xu, H., T. Dinev, H. J. Smith, and P. Hart. December 2008. *Examining the Formation of Individuals' Information Privacy Concerns: Toward an Integrative View*. Proceedings of the 29th Annual International Conference on Information Systems, Paris, France.

APPENDIX A

JOURNALS COVERED IN THIS ARTICLE

Accounting Journals

Auditing: A Journal of Practice & Theory
Contemporary Accounting Research
International Journal of Disclosure and Governance
Information Systems Control Journal
Journal of Emerging Technologies in Accounting
Journal of Accounting and Public Policy
Journal of Accounting Research
Journal of Information Systems

Information Systems Journals

ACM Computing Surveys
ACM Transactions on Information and System Security
Communications of the ACM
Decision Sciences
Decision Support Systems
Electronic Commerce Research and Applications
IEEE Computer
IEEE Transactions on Software Engineering
Information & Management
Information Systems Management
Information Systems Research
International Journal of Electronic Commerce
Journal of Electronic Commerce in Organizations
Journal of the Association for Information Systems
Journal of Electronic Commerce Research
Journal of Management Information Systems
Management Science
Management Information Systems Quarterly
The Information Society

Law Journals and Reports

Cahiers du CRID
Computer Law & Security Report
Computer Law and Security Review
Electronic Journal of Comparative Law
Harvard Law Review
International Journal of Communications of Law and Policy
International Review of Law, Computers & Technology
Murdoch eLaw Journal
Privacy and Security Law Report (not refereed)
Privacy and Data Protection
Privacy Law and Policy Reporter (not refereed)
University of Ottawa Law and Technology Journal

(continued on next page)

APPENDIX A (continued)

Journals in Other Areas

Administrative Science Quarterly
California Management Review
Identity in the Information Society
IEEE Transactions on Professional Communication
Ivey Business Journal
Journal of Academic and Business Ethics
Journal of Business Ethics
Journal of Corporate Accounting & Finance
The Journal of Consumer Affairs
Journal of Economic Psychology
The Journal of Political Economy
Journal of Public Policy & Marketing
The Journal of Social Issues
Organization Science
Review of Marketing Science
Scientific American (not refereed)
Sociology and Social Research

APPENDIX B

RESEARCH QUESTIONS FROM THE PERSPECTIVE OF GENERALLY ACCEPTED PRIVACY PRINCIPLES OF THE AICPA/CICA

Principle	Research Questions
Management	• Which firm structures most effectively manage compliance with privacy policies? To whom should the Chief Privacy Officer (or equivalent) report? • What are current practices regarding accountability for compliance with privacy policies? What are best practices? • What factors cause top management to support the development and implementation of privacy policies? • What distinguishes high-performing and low-performing firms in regards to effective achievement of this principle? • How often do firms communicate their privacy policies to employees to ensure that they are aware of and compliant with them? How often is privacy awareness training offered? Which types of training are most effective? How is the training effectiveness evaluated? • How often do Boards of Directors discuss privacy issues? How does Board involvement affect practice? • How often are privacy risk assessments performed? Is the frequency associated with likelihood of privacy breaches?
Notice	• How well do individuals understand firms' written privacy policies? • How and why do privacy policies differ across industries? Across firms within an industry? • To what extent do firms' privacy policies distinguish between "sensitive" information (as defined in GAPP) and other personal information? Are the two types of information treated differently?
Choice and Consent	• What factors are associated with U.S. firms choosing to adopt an opt-in versus opt-out approach to consent? Are such choices related to industry? Types of information (sensitive versus other)? • To what extent do individuals consciously realize they have given implicit consent to divulge their personal information (e.g., in opt-out situations, how aware are individuals that they could have chosen to opt out)? • How does the choice of a default policy (opt-in versus opt-out) affect consumer attitudes about the firm? Likelihood of sharing their personal information with the firm? Likelihood of purchasing goods or services from the firm?

(continued on next page)

APPENDIX B (continued)

Principle	Research Questions
	• How does the choice of a default policy (opt-in versus opt-out) affect quality of data warehouse, data mining, and targeted advertising? • How often do firms change their privacy policies (particularly regarding use of the information and sharing with third parties)? How are such changes communicated (on website, by email, etc.)? • How does the firm monitor and enforce compliance with customers' wishes (e.g., if customer says "no persistent cookies" how does management ensure that web developers follow this)?
Collection	• How do firms monitor the use of personal information they collect? • How many firms disclose their use of tracking methods? How?
Use, Retention, and Disposal	• How do firms monitor use, retention, and disposal of personal information? • What factors are associated with high- and low-performing firms in terms of complying with this principle? • How do firms securely dispose of personal information?
Access	• How do access provisions differ across industries? In industries? What factors are associated with the differences? • How satisfied are individuals with their ability to access personal information they share with firms? • What types of authentication credentials are used to restrict access to personal information?
Disclosure to Third Party	• How do firms monitor compliance with their stated policy about information sharing? • How do firms obtain assurance that business partners with whom they are sharing information adequately comply with GAPP? • How do firms verify that information they obtain from third parties is legitimate to be shared with them?
Security and Privacy	• To what extent are security processes driven by privacy issues? • What are the best practices for protecting privacy? Are there differences between industries? • How do firms prevent downloading of personal information by employees to removable media (e.g., PDAs, USB devices, etc.) or effectively ensure that such data is encrypted? • How frequently are privacy-related security policies and procedures tested?
Quality	• How do firms maintain quality control over personal information they collect? • How often do firms update and correct errors in personal information?
Monitoring and Enforcement	• What is the optimal governance structure for monitoring compliance with privacy policies? • What are funding levels for privacy? Trends? • What factors are associated with firms' spending on privacy monitoring and enforcement?