E-Commerce and Privacy: Exploring What We Know and Opportunities for Future Discovery

JOURNAL OF INFORMATION SYSTEMS
Vol. 25, No. 2
Fall 2011
pp. 11–45

American Accounting Association
DOI: 10.2308/isys-10090

E-Commerce and Privacy: Exploring What We Know and Opportunities for Future Discovery

J. Efrim Boritz
University of Waterloo

Won Gyun No
Iowa State University

ABSTRACT: Electronic commerce (e-commerce) has a built-in trade-off between the necessity of providing at least some personal information to consummate an online transaction and the risk of negative consequences from providing such information. This requirement and the increased sophistication of companies' personal information gathering have made e-commerce privacy a critical issue and have spawned a broad research literature that is reviewed in this paper. Key research issues and findings are organized, using a framework defined by four key stakeholder groups—companies, customers, privacy solution providers (PSPs), and governments—as well as the interactions among them. The review indicates that the published research on e-commerce privacy peaked in the early 2000s; thus, it has not addressed many of the technological advances and other relevant developments of the past decade. Potential research opportunities for researchers in Management Information Systems (MIS) and Accounting Information Systems (AIS) include: company privacy strategies, operations, disclosures, and compliance practices; customer privacy concerns arising from company practices such as Internet activity tracking, physical location tracking, personal information gathering by social networks, and information exchanges in cloud computing environments; privacy-enhancing technologies, controls, and assurance practices developed by PSPs; and privacy regulations relating to various industries, countries, and cultures. More use of experimental and archival research is encouraged.

Keywords: privacy; e-commerce; review; research opportunities.

We gratefully acknowledge the financial support provided by the University of Waterloo Centre for Information Systems Assurance, sponsored by the Canadian Institute of Chartered Accountants, ISACA, and CaseWare IDEA Inc. We are also grateful to Roger Debreceny and two anonymous reviewers whose constructive criticisms of earlier drafts helped us to improve this review.

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

Published Online: November 2011

I. INTRODUCTION

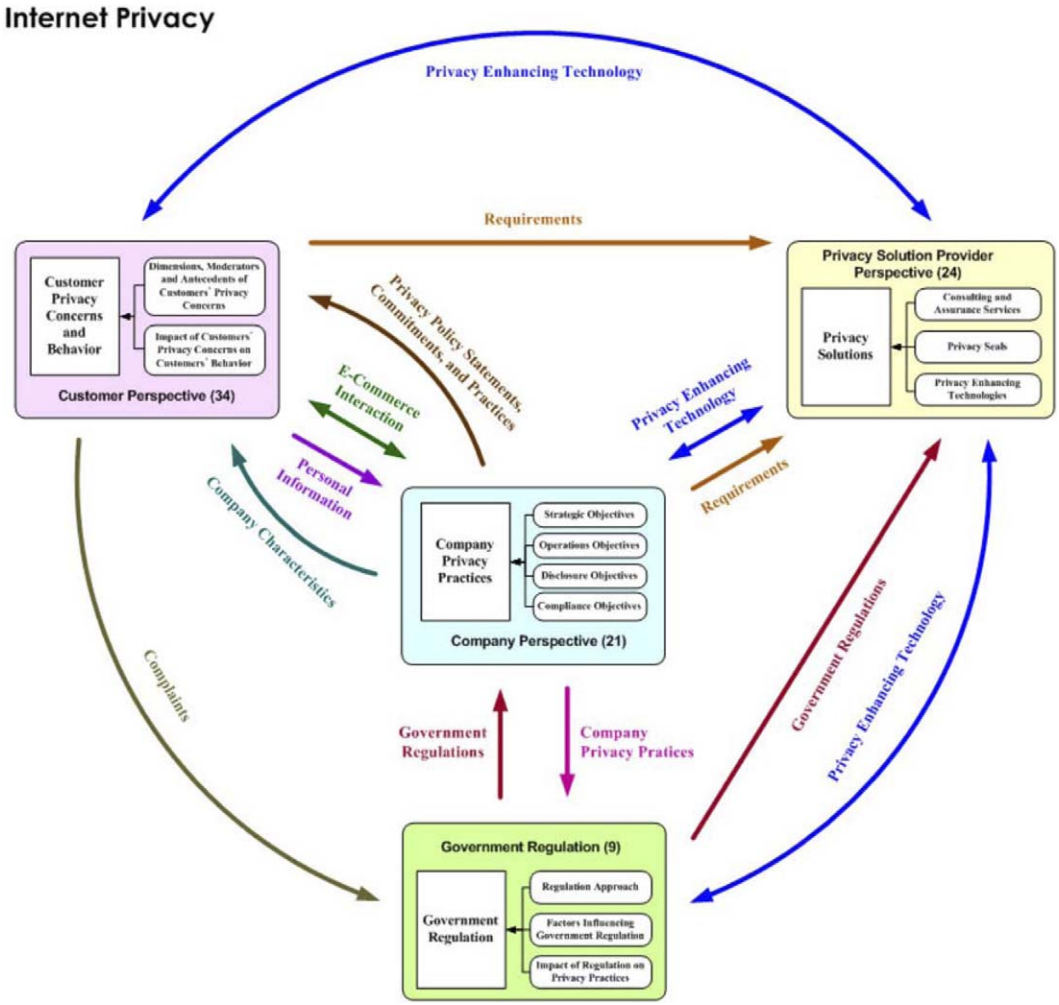
Most e-commerce companies collect, store, and exchange personal information obtained from individuals and use that information to support marketing strategies, gain greater insights into individuals' behavior, and meet their needs and wants more effectively. However, concerns about the inappropriate use of personal information can reduce customer trust in online transactions and potentially jeopardize the proliferation of e-commerce (Hoffman et al. 1999; Milne and Boza 1999; Shankar et al. 2002). Studies have shown that individuals' growing privacy concerns put pressure on companies to develop customer-focused privacy practices (Culnan 2000; Culnan and Armstrong 1999; Shapiro and Baker 2001) and on governments to protect individuals' privacy (Bowie and Jamal 2006; Westin 2003). Growing privacy concerns also create threats and opportunities for the providers of technologies, processes, and systems for capturing, using, and protecting personal information.

E-commerce privacy is one of the information privacy issues that should be on the agenda of management information systems (MIS) and accounting information systems (AIS) researchers. We offer this review of relevant research that has been conducted in the fields of information systems, business, and marketing and that has addressed e-commerce privacy to identify research opportunities for the MIS and AIS research community. We create a framework (Figure 1) that links the four key stakeholders addressed in the literature—companies, customers, suppliers, and governments, and the interactions among them, and identifies the key research areas pertaining to each stakeholder group. We use the framework for classifying extant research studies, reviewing key findings, and identifying opportunities for future research. Although some of our discussion may apply to broader enterprise information privacy concerns (i.e., non-e-commerce settings), we limit the scope of our review in this paper solely to privacy in an e-commerce setting. A paper by Kauffman et al. (2011) addresses research on the broader information privacy issues.

The importance of privacy to the AIS research community was recognized almost a decade ago. Three chapters in a research monograph edited by Arnold and Sutton (2002) identify privacy as being a critical issue for AIS. Dillard and Yuthas (2002, 190) identify privacy as one of the key ethical issues of the information age and assert that it represents "one of the most immediate dilemmas facing AIS." Gray and Debreceny's (2002) review of research in electronic commerce emphasizes the importance of customer concerns about privacy to the creation and maintenance of trust in both business-to-consumer (B2C) and business-to-business (B2B) e-commerce. They note the paucity of research on the risk-reducing, value-adding role of trust-enhancing assurance services. Boritz (2002) identifies information systems assurance services relating to privacy and related processing integrity controls as a topic requiring AIS research attention. However, together, these three chapters on AIS research opportunities identified only eight papers that addressed privacy; all published pre-2000.

Our review indicates that the research on e-commerce privacy published in the four research databases covered by our review peaked in the early 2000s. Thus, it has not addressed many of the privacy issues arising from technological advances during the past decade such as Internet access through mobile devices; the growth of social networking; the move toward cloud computing; and the growth of threats to privacy from technologies for capturing personal information without an individual's knowledge or consent such as online tracking software, global positioning systems, and radio frequency identification devices (RFID). Also, most of the studies to date have relied on surveys of stakeholder opinions and attitudes rather than actual behaviors. There has been virtually no empirical work relating companies' privacy behavior to factors such as corporate and IT governance, corporate financial performance, and market reactions to privacy initiatives. As well, Gray and Debreceny's (2002) and Boritz's (2002) calls for research into privacy assurance appear to have gone largely unheeded. In addition, the research to date has focused almost entirely on

FIGURE 1
E-Commerce Privacy Research Framework



privacy in the B2C e-commerce context. However, there are significant privacy issues in B2B settings, which represent more than 90 percent of e-commerce activity (U.S. Census Bureau 2009).

The remainder of the paper is organized as follows. First, we define privacy, briefly discuss privacy issues in e-commerce, and introduce the framework that was used to classify the studies that were reviewed. Then, we use the framework to organize and summarize our review findings. Next, we discuss future research opportunities. Finally, we conclude with a brief summary of our review.

II. PRIVACY AND E-COMMERCE

Definition of Privacy in an E-Commerce Context

One of the earliest, often-quoted, definitions of privacy is "the right to be let alone" (Warren and Brandeis 1890). Other definitions include: "the claim of individuals, groups, or institutions to

determine for themselves when, how, and to what extent information about them is communicated to others" (Westin 1967); "the selective control of access to the self" (Altman 1975); and "a capability to determine what one wants to reveal and how accessible one wants to be" (Bellotti 1997). This review focuses on privacy in an e-commerce context. In such a context, the invasion of privacy is commonly viewed as the unauthorized collection, use, and transfer of *personal information* as a direct result of e-commerce transactions (Milberg et al. 2000; Petty 2000; Rezgui et al. 2003). Personal information is information that is, or can be, about or related to an identifiable individual. It includes any information that can be linked to an individual or used, directly or indirectly, to identify an individual. Individuals must disclose personal information to complete e-commerce transactions, and research shows that individuals are, in fact, willing to do this in exchange for anticipated economic and social benefits after assessing the risks of disclosure—whether their personal information will subsequently be used fairly, and whether they will suffer negative consequences (Laufer and Wolfe 1977; Stone and Stone 1990). Therefore, in the context of e-commerce, the following definition of privacy is used throughout this review: "individuals' right to control their personal information with respect to its collection, use, and transfer by entities engaged in e-commerce."

Privacy in E-Commerce

Companies use e-commerce sites to reach potential customers. During the e-commerce process, companies have many opportunities to collect and use personal information to differentiate themselves through improved customer relationships, one-to-one communications, and personalized services (Gurau et al. 2003). The personal information that companies gather can be used to provide better services; however, it can also be misused; for example, by sending unwanted emails to customers, selling customers' information to others, or disclosing potentially sensitive information that the customer would prefer to keep private.

The easiest way to gather personal information is during a registration or ordering process. Customers are asked for personal information such as name, email address, and credit card number. Some of these data are required to process transactions. However, additional information can also be collected such as preferences, income, and other types of personal information that can help target marketing efforts. Another approach is to capture customers' Internet Protocol (IP) addresses and to use these IP addresses to track the specific web pages the customer has viewed and the sequence of the web pages the customer visited (Carr 2010). A third approach is to gather customers' personal information by the use of a "cookie"—a file stored in an individual's computer that contains information such as the customer's traits, preferences, and behavioral information that can be accessed and used to identify the individual (Harper 2010). Recently, a fourth approach became available: harvesting personal information from social networks such as Facebook, Twitter, YouTube, and Flickr (Ingram 2009). Finally, new and emerging technologies such as radio frequency identification (RFID) tags and global positioning systems (GPS) embedded in mobile devices enable identifying and tracking the physical location and movement of individuals (Bustillo 2010; Steel and Scheck 2010). Cloud computing enables, and may require, the transmission of personal information from an originator to layers of service providers with potentially weaker privacy practices (Hoover 2010; Katzan 2010). New customer-tracking technologies can aid companies' marketing tactics and could be helpful to customers by serving them information that is personalized to their interests, but customers are often concerned that companies might sell, trade, or share that information among third-party companies without

their knowledge or consent, or otherwise compromise their privacy (e.g., through inadequate security over personal information).[1]

The privacy risks described above can be countered by a number of approaches, including regulation, privacy-enhancing technologies and, in the extreme, opting out of e-commerce activity partially (e.g., browsing for products but paying offline) or entirely (e.g., not engaging in e-commerce).

Privacy Research Framework and Scope of Review

We searched four journal databases (i.e., AAA Digital Library, ACM Digital Library, ABI Inform (ProQuest), and ScienceDirect) from 1993 to 2009 using the search strings: "Privacy" and "Privacy and E-Commerce" to identify research papers that addressed privacy in an e-commerce setting, identifying 116 such studies.[2] We developed a framework for classifying and relating the research works that we found, and identified future research opportunities. The framework is organized around four main stakeholders and the interactions among them as depicted in Figure 1: companies (including not-for-profit organizations); customers (including other stakeholders such as donors to not-for-profit organizations); privacy solution providers (hereafter, PSPs); and governments (including quasi-governmental regulatory agencies). For each stakeholder group the framework also identifies the key issues around which we organized this review.

Companies are at the center of the framework in Figure 1. According to the enterprise risk management (ERM) framework established by COSO (2004) companies may pursue four categories of overlapping objectives: strategic, operations, reporting, and compliance.[3] Privacy relates to all of these objectives. The risk management challenge for e-commerce companies is to balance the benefits and risks associated with use of customers' personal information. The benefits include strategic competitive advantage and the operational effectiveness and efficiency, whereas the risks are alienating customers through unacceptable privacy practices, attracting sanctions by government regulatory agencies for failing to comply with privacy laws and regulations, and civil litigation for damages caused by breaches of customers' privacy. In response to customers' increasing privacy concerns, companies may implement privacy protections (e.g., information privacy controls) and disclosures (e.g., privacy policy statements). Their privacy practices not only influence customers' privacy concerns, but also affect the programs, services, and technologies offered by PSPs, and government regulations aimed at protecting privacy.

Another main stakeholder group is customers, a key source of personal information. Although they are somewhat vulnerable, they can adopt privacy-enhancing technologies (e.g., encryption, the Platform for Privacy Preferences (P3P), and Anonymizer) or lobby for government regulation of

[1] According to an article titled "Customer Data Means Money" in *InformationWeek* (Rendleman 2001), business and information brokers may sell individuals' personal information on their prescription drug purchases, credit information, civil and criminal legal information, professional licenses, property ownership, marriage and divorce records, and retail purchases. This information is culled from public records, catalog and online purchases, credit reports, product warranty cards, and consumer surveys.

[2] These searches yielded more than 500 hits. Thus, we used the following additional criteria to select papers. Privacy had to be a main research topic of the paper; the paper focused on privacy issues in e-commerce (i.e., we excluded job privacy, government privacy, etc.); we excluded privacy issues with respect to health information, child privacy, and detailed privacy technology papers; and, we generally excluded conference proceedings.

[3] According to COSO (2004), entity objectives can be viewed in the context of four categories: (1) Strategic objectives are related to high-level goals that are aligned with and support the entity's mission/vision; (2) operations objectives are associated with effectiveness and efficiency of the entity's operations, including performance and profitability goals. They vary based on management's choices about structure and performance; (3) reporting objectives are concerned with the accuracy, completeness, and reliability of the entity's reporting. They include internal and external reporting and may involve financial or nonfinancial information; and (4) compliance objectives are related to the entity's compliance with applicable laws and regulations.

companies' privacy practices.[4] If customers are not able to rely on government regulation, companies' self-regulation, and privacy-enhancing technologies, they may decline to provide or may fabricate personal information (Lwin and Williams 2003), refuse to interact with untrustworthy e-commerce sites (Culnan and Milne 2001), or refuse to participate in e-commerce altogether.

The third main stakeholder group is PSPs, ranging from professional associations (e.g., American Institute of Certified Public Accountants (AICPA)) to not-for-profit organizations (e.g., TRUSTe) to commercial solution providers (e.g., Web Entrust), that have created privacy services and technologies that other stakeholders can use to enhance privacy. For example, the AICPA and Canadian Institute of Chartered Accountants (CICA) have produced a set of Generally Accepted Privacy Principles (GAPP) summarized in Table 2 that entities can use to obtain assurance services, attesting that their privacy practices are effective and comply with their privacy notices. Organizations such as TRUSTe and BBBOnLine have created web privacy seals to signify that a website adheres to disclosed privacy practices. Still other organizations have created encryption systems (e.g., PKI), privacy protocols (e.g., P3P), and privacy-enhancing technologies (e.g., Anonymizer) to protect customers' privacy.

Finally, governments may seek to protect individuals' privacy by enacting laws, overseeing the implementation of these laws, educating the public about privacy issues, encouraging industry self-regulation, and regulating solutions offered by PSPs (e.g., encryption technologies). Such government activities can affect customers' privacy concerns, companies' privacy practices, and PSPs' offerings. Many countries, for example, the United Kingdom, Germany, and Canada, have enacted privacy legislation governing some aspects of the collection, use, and transfer of personal information, including the transfer of such information to other countries that have not adopted similar privacy protection legislation. Regulatory actions can vary across economic sectors, with more focused privacy laws covering sensitive sectors such as health care and financial services. Some countries, such as the United States, have taken a comparatively liberal industry self-regulation approach. Under the industry self-regulation approach, each company is responsible for deciding on the degree of information that is collected and used, and for developing its own privacy policy statement aligned with its industry guidelines. Government agencies only get involved in egregious breaches of privacy such as RealNetworks (Macavinta 1999), DoubleClick (Charters 2002), ChoicePoint (Kane and Hines 2005), Facebook (Bardeesy 2009), and others (see Peltier et al. 2009). RealNetworks provided a free music player that secretly sent back information to RealNetworks about the music played by users. DoubleClick used a combination of cookies and databases to track users' browsing behavior. ChoicePoint failed to protect the personal information of individuals against theft by criminals. Facebook failed to provide privacy controls to its members and made members' personal information available to marketers and others without their consent.

Some countries have no formal privacy regulations in place. Each company decides upon the degree of information that it will collect and use to achieve its objectives. However, companies' practices may anticipate and, hence, may be influenced by customers' privacy concerns and behaviors. Some governments encroach on the privacy of their citizens by monitoring their online activities, but this aspect of privacy is outside the scope of our review.

Table 1 classifies prior privacy studies published in the sources that we reviewed according to the major research areas and year of publication. Table 1 indicates that between 1993 and 1998, the early years of Internet-based e-commerce, there was virtually no research published in this area; the period 1999–2001 saw a dramatic increase in e-commerce privacy research, culminating in a peak two-year period between 2002–2003 that by itself accounted for 33 percent of the studies reviewed

[4] The P3P is a standardized, machine-readable protocol, which enables websites to express their privacy practices. Anonymizer is website browsing software that makes individuals' activity on the Internet untraceable.

TABLE 1

Summary of Reviewed Studies by Year of Publication

Research Framework		1993	1994	1995	1996	1997	1998	1999	2000	2001
Company Perspective	Strategic Objectives									
	Operations Objectives									
	Disclosure Objectives								1	
	Compliance Objectives									
Customer Perspective	Dimensions, Moderators, and Antecedents of Customers' Privacy Concerns	1		1				4	3	3
	Impact of Customers' Privacy Concerns on Customers' Behavior							1		
Privacy Solution Provider Perspective	Consulting and Assurance Services					1				
	Privacy Seals							1		2
	Privacy-Enhancing Technologies							1	1	
Government Perspective	Regulation Approaches				1				1	1
	Factors Influencing Government Regulation			1					1	
Company-Customer Interaction	Company Characteristics and Customer Perceptions/Attitudes							1	1	
	Company Characteristics and Customer Behavior							1		
	Company Privacy Disclosures and Practices and Customer Behavior							1	1	
Company-Privacy Solution Provider Interaction	Company Privacy Policies and Practices and Privacy Seals								1	
	Company Privacy Practices and Privacy-Enhancing Technologies									
Company-Government Interaction	Impact of Company Privacy Practices on Government Regulation								1	
	Impact of Government Regulation on Company Privacy Practices								1	1
Customer -Privacy Solution Provider Interaction									1	
Customer-Government Interaction										
Privacy Solution Provider-Government Interaction										
Higher Order Interaction										
Total		1	0	2	1	1	0	10	13	7

(continued on next page)

TABLE 1 (continued)

Research Framework		2002	2003	2004	2005	2006	2007	2008	2009	Total
Company Perspective	Strategic Objectives		1							1
	Operations Objectives		2							2
	Disclosure Objectives	3	2	1	2	2	1		1	13
	Compliance Objectives	1	1		1	1			1	5
Customer Perspective	Dimensions, Moderators, and Antecedents of Customers' Privacy Concerns	3	1	2		1				19
	Impact of Customers' Privacy Concerns on Customers' Behavior	1	3	2	3	2		3		15
Privacy Solution Provider Perspective	Consulting and Assurance Services		1					1		3
	Privacy Seals	1	3	1						8
	Privacy-Enhancing Technologies	3	3		1		1	2	1	13
Government Perspective	Regulation Approaches	1		1		2				7
	Factors Influencing Government Regulation									2
Company-Customer Interaction	Company Characteristics and Customer Perceptions/Attitudes		1		1		1			5
	Company Characteristics and Customer Behavior	1								2
	Company Privacy Disclosures and Practices and Customer Behavior	1				1	1			5
Company-Privacy Solution Provider Interaction	Company Privacy Policies and Practices and Privacy Seals	1					1			3
	Company Privacy Practices and Privacy-Enhancing Technologies	1	1				1	1		4
Company-Government Interaction	Impact of Company Privacy Practices on Government Regulation									1
	Impact of Government Regulation on Company Privacy Practices		1		1			1		5
Customer-Privacy Solution Provider Interaction		3			1	2	1	2		10
Customer-Government Interaction										0
Privacy Solution Provider-Government Interaction								1		1
Higher Order Interaction			1				1			2
Total		20	21	7	10	11	8	11	3	126[a]

[a] The following journal databases were searched: AAA Digital Library, ACM Digital Library, ABI Inform (ProQuest). A total of 116 key studies on privacy in an e-commerce setting were identified and reviewed. Some studies are counted more than once if they fit more than one research area.

TABLE 2

Generally Accepted Privacy Principles (GAPP)[a]

Principles	Description
1. Management	The entity defines documents, communicates, and assigns accountability for its privacy policies and procedures.
2. Notice	The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed.
3. Choice and Consent	The entity describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of personal information.
4. Collection	The entity collects personal information only for the purposes identified in the notice.
5. Use and Retention	The entity limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The entity retains personal information for only as long as necessary to fulfill the stated purposes.
6. Access	The entity provides individuals with access to their personal information for review and update.
7. Disclosure to Third Parties	The entity discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.
8. Security for Privacy	The entity protects personal information against unauthorized access (both physical and logical).
9. Quality	The entity maintains accurate, complete, and relevant personal information for the purposes identified in the notice.
10. Monitoring and Enforcement	The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy-related complaints and disputes.

[a] Source: AICPA/CICA (2009).

here. Since that peak, the volume of e-commerce privacy research has returned to more modest levels. Over the period covered by the review, 21 studies have addressed the company perspective, 34 have addressed the customer perspective, 24 have addressed the PSP perspective, and nine have addressed the government perspective. In addition, 37 studies have investigated two or more interactions between these stakeholders. Table 1 indicates that a few areas of potential research interest have been addressed extensively, but most have had scant research attention paid to them. This is ironic given the importance attributed to privacy as an issue for AIS researchers and practitioners almost a decade ago by Dillard and Yuthas (2002), Gray and Debreceny (2002), and Boritz (2002).

In the next two sections, we use the framework in Figure 1 to discuss relevant literature and address directions for future research, respectively.

III. REVIEW OF PUBLISHED RESEARCH ON E-COMMERCE PRIVACY

In this section, we review published research addressing e-commerce privacy issues for each of the four main stakeholder groups in our framework. For brevity and focus, we discuss only a few specific studies that are representative of the areas discussed. In addition, due to space limitations,

we restrict our discussion to basic stakeholder-focused research and two-way interactions between companies and the three other stakeholder groups, although Table 1 includes the studies that we found in other categories.

Company Perspective

The framework developed by COSO (1992) and expanded by COSO (2004) embodies a broad view of management control and enterprise risk management (ERM). After the PCAOB (2004, 2007) enshrined it in the auditing standards related to SOX 404, this framework became a *de facto* standard for assessing enterprise controls and risk management practices. Thus, we classified the studies that we reviewed in this category into four subcategories based on the four key objectives identified in COSO's (2004) ERM framework: strategic, operations, disclosure, and compliance objectives.

Strategic Objectives: Strategic Privacy Choices

Prior research has suggested that privacy protection can be a strategic asset (Ashworth and Free 2006). For example, the Royal Bank of Canada (RBC) established a Corporate Privacy Group and became recognized as a North American leader in the area of privacy management.[5] Sarathy and Robertson (2003) introduced a model wherein a company's privacy strategy is affected by its environmental context such as national history, culture, and existing and pending legislation; the ethical frame of the firm and top management; and firm-specific factors such as information intensity of the business, age and experience of the firm, and corporate culture. Cost-benefit analysis plays a role in the privacy strategy adopted by the company. That is, the company adopts different strategies depending on the analysis of economic benefits (e.g., meeting customers' needs and relationship management) and cost of compliance (e.g., the cost of granting access to data). This model is comprehensive, but has not been empirically tested.

Operations Objectives: Operational Practices

Privacy-related operations include collection, recording, and use of information, and protecting the information through various security measures. The one study on collection, recording, and use of personal information, Gurau et al. (2003), examined French (93), U.K. (106), and U.S. (92) sites and found differences among the countries in the form of data request used for personal information. For example, the U.S. sites used more intrusive approaches such as data requests through pop-up windows. However, the study did not address whether the form of data request (e.g., intrusiveness) hampered or enhanced the collection of personal information.

Threats to privacy in an e-commerce setting include sniffing, spyware, phishing, bogus websites, and other such techniques designed to steal personal information. These threats can be mitigated with the use of privacy-enhancing technologies such as physical and logical access controls, data communications controls (e.g., encryption), P3P, and Privacy Inc. Software Agent (PISA). There is an extensive literature on information security, most of which does not focus specifically on e-commerce and privacy and is, therefore, outside the scope of this review. For instance, Seničar et al. (2003) discuss privacy threats on the Internet as well as the possible solutions for addressing such threats.

[5] Presentation by Peter Cullen, at a panel on e-privacy at the University of Waterloo Centre for Information Systems Assurance, Symposium on Information Systems Assurance, October 4–6, 2001; see also http://www.microsoft.com/presspass/press/2003/jun03/06-23cullenpr.mspx.

Disclosure Objectives: Disclosure of Privacy Commitments and Practices

In an e-commerce setting, privacy disclosures include privacy policy statements, privacy seals, and similar descriptions of an entity's commitments to protecting customers' privacy. Desai et al. (2003) examined Internet policies posted on 40 U.S. companies' websites from 1999 to 2001. They found that privacy-related policies were the most frequently posted policies on companies' websites. Milne and Culnan (2002) studied the changes and trends in voluntary privacy disclosures by analyzing four web surveys conducted between 1998 and 2001, and found a significant increase in the number of privacy disclosure statements over time as well as in privacy policy disclosures about information collection, revealing information to third parties, and choice. However, Liu and Arnett (2002) analyzed 497 websites of the Fortune 500 and found that only approximately 50 percent of these websites disclosed a privacy policy. In the not-for-profit sector, Hoy and Phelps (2003) conducted a study of 102 Christian churches' websites. They found that the vast majority (99 percent) of churches' websites collected personal information, but few sites provided information about their privacy polices (i.e., less than 3 percent posted a privacy policy statement, and only 23.5 percent provided some form of information practice statement).

Several studies have examined the ways that companies communicate their privacy policies and the readability of their privacy policy disclosures. For example, based on the four types of social action in Habermas' Theory of Communicative Action (i.e., communicative, instrumental, discursive, and strategic), Schwaig et al. (2005) attempted to explain the role of privacy policies in Fortune 500 companies. They concluded that companies do not really want to reveal whether they adhere to their privacy policies (communicative action) or the principles embodied in fair information practices (discursive action). Rather, companies want to limit the scope of privacy policies to reduce their liabilities (instrumental action); hence, they use the privacy policies as a strategic mechanism that conveys a positive public image without providing actual protection (strategic action). Similarly, Pollach (2007) examined the language of privacy policies of 50 successful e-commerce sites based on four parameters in critical linguistics (Fowler et al. 1979).[6] Pollach (2007) showed that privacy policy statements not only failed to address important areas of individuals' concern, but also were written in a way that protects companies from potential privacy litigation by concealing privacy infringements (e.g., omitting references regarding unethical data handling practices). Milne et al. (2006) conducted a longitudinal study of 312 online privacy policy notices contained in privacy policy statements and found that the readability of online privacy notices had declined, while their length had increased between 2001 and 2003. They also noted that nearly half of U.S. individuals did not have the education level needed to understand approximately half of privacy policies analyzed in their study (i.e., 47.9 percent of the U.S. population did not have any college education, whereas 53.8 percent of privacy notices required education beyond high school).

Apart from the format or style of communicating is the issue of the types of information contained in companies' privacy policy statements, relative to the information that users want to know about companies' privacy practices. Based on the brainstorming results of two panels (11 experts and 16 information systems executives), Dhillon and Moores (2001) found that the most important privacy concerns pertained to companies' use of spam, selling personal information, preventing theft of personal information, eliminating the chance of losing personal files, and maximizing security. Earp et al. (2005) analyzed privacy policy statements of 50 U.S. companies' websites and conducted a survey of 827 U.S. Internet users. They showed that the information

[6] The four parameters are lexical choice (the systematic use or avoidance of words), syntactical transformation (the use of passive voice and nominalizations), negation (issues that are denied), and modality (the certainty of the speaker about the content of an utterance).

addressed in the privacy policy statements did not fully provide the information that users wanted to know. In their study, users were most concerned about (1) transfer or sharing of their personal information; (2) what information was collected and how it was used; and (3) how organizations stored and maintained their personal information. However, the three information items most frequently included in companies' privacy statements were: (1) security over data collection and transfer; (2) how data was collected; and (3) consent about information collection.

Compliance Objectives: Compliance of Privacy Practices with Laws and Regulations

To address customers' privacy concerns, companies need to be aware of applicable laws and regulations specific to their industries as well as to the area of operation. In the United States, privacy legislation exists at both industry and state levels (Baumer et al. 2004; NCSL 2009; Peslak 2005).[7] The U.S. Federal Trade Commission (FTC) has identified four principles as representing Fair Information Practices (FIPs): Notice/Awareness, Access/Participation, Choice/Consent, and Security/Integrity, and several studies have examined whether companies comply with such recommendations. For example, Liu and Arnett (2002) found that many Fortune 500 websites failed to cover all four privacy principles recommended by the U.S. FTC. Schwaig et al. (2006) also investigated the privacy policies of the Fortune 500 and found that the Fortune 100 complied with the FTC's FIP more than the rest of the Fortune 500 did. They also found that firms in information-intensive industries and B2C e-commerce companies were more likely to comply with the FIP than their counterparts. Reay et al. (2009b) examined the privacy policies of websites to assess the level of compliance to legal mandates under which the websites operate. By examining available P3P documents (2,287 full policies and another 2,294 compact policies) from the 100,000 most popular websites, they found a lack of adherence to legal mandates in the stated privacy policies. That is, the websites generally did not follow all the privacy-protection mandates in their respective legal jurisdictions.

Jamal et al. (2003) investigated 100 U.S. high-traffic e-commerce sites' adherence to opt-out choices related to the privacy principles of Notice/Awareness and Choice/Consent as described in the companies' privacy disclosures. They subscribed to the websites under assumed identities, selecting opt-out provisions in all cases, and waited to see whether unwanted email would be sent to those identities. They found that the actual privacy practices of those sites closely complied with their stated privacy policies.

Customer Perspective

The customer's perspective is often associated with marketing rather than AIS. However, the customer's perspective is important for AIS practitioners and researchers to consider as the collection, recording, and use of personal information in conjunction with transaction processing, database management, and reporting could impinge on customers' privacy rights. This is particularly the case in an e-commerce setting, which magnifies companies' opportunities to collect, record, and use customers' personal information, and has a built-in trade-off for customers between the need to provide personal information to consummate a transaction and the risks assumed by providing such personal information. These possibilities make the customer's perspective an important one for AIS practitioners and researchers to understand and consider in the design of information systems, controls, and assurance services.

[7] For instance, the Gramm-Leach-Bliley Act for the financial industry, the Health Insurance Portability and Accountability Act for the health insurance industry, and state laws related to Internet privacy in Minnesota (Statutes § 325M.01 to 0.09) and Nevada (Revised Statutes § 205.498).

Public opinion polls have revealed a general desire among Internet users to protect their privacy (FTC 2000; Harris Interactive 2003; Zogby International 2007). Prior research has investigated two key privacy issues: (1) What are the major dimensions, moderators and antecedents of customers' privacy concerns; and (2) what is the impact of customers' privacy concerns on their behavior?

The Dimensions, Moderators, and Antecedents of Customers' Privacy Concerns

As mentioned earlier, Dhillon and Moores (2001) found that customers' most important privacy concerns pertained to companies' use of spam, selling personal information, preventing theft of personal information, eliminating the chance of losing personal files, and maximizing security. In addition, they identified 18 potential ways of addressing these concerns (e.g., enact stronger laws to protect consumer privacy and make spam illegal). Since these concerns can differ depending on customers' personal or cultural characteristics, Westin proposed a typology of individuals' concerns about privacy (Harris et al. 1995). He argued that individuals can be categorized into three groups: privacy fundamentalists, privacy unconcerned, and privacy pragmatists.[8] Sheehan's (2002) email survey of 889 U.S. online users confirmed the typology, although it indicated that users fell into four distinct categories rather than three: unconcerned Internet users, circumspect Internet users, wary Internet users, and alarmed Internet users. Factors that have been found to be associated with privacy concerns include gender, (O'Neil 2001; Sheehan 1999), age (Sheehan 2002; Milne and Rohm 2000), income level (O'Neil 2001), and education (O'Neil 2001; Sheehan 2002; Phelps et al. 2000). However, these have not been matched to Westin's or Sheehan's typologies.

Apart from personal characteristics, it is possible that customer's countries and cultures impact their privacy concerns. Hofstede's (1991) four measures of cultural values (power distance, masculinity/femininity, individualism/collectivism, and uncertainty avoidance) have been investigated by Milberg et al. (1995) and Milberg et al. (2000) with respect to general information privacy, but not in an e-commerce setting. Milberg et al. (1995) found that the level of concern about privacy of personal information varied across countries, but the relative importance of four underlying dimensions of information privacy concern (i.e., collection, error, secondary use, and improper access) did not appear to vary across countries. Milberg et al. (2000) found that differences in levels of consumer privacy concerns were associated with cultural values as well as differences in regulatory approaches.[9]

Several studies have attempted to identify moderators and antecedents for customers' privacy concerns. Ackerman et al.'s (1999) online survey of 381 U.S. online users found that there were significant differences in customers' comfort levels across various types of information (e.g., demographic versus financial data). This was later supported by Earp and Baumer's (2003) study of customers' differential willingness to provide information on websites in different sectors (i.e., retail, financial, or medical/health). Ackerman et al. (1999) also found different levels of acceptance of persistent identifiers (i.e., cookies), depending on the purpose of collection and the intended use

[8] The *privacy fundamentalists* are defined as being extremely concerned about the use of their personal information and are unwilling to provide their information. Individuals in the *privacy unconcerned* group do not take their privacy into consideration and are willing to provide their personal information. The *privacy pragmatists* are concerned about their privacy, but less than privacy fundamentalists.

[9] Milberg et al. (2000) used four of the five measures of cultural values developed by Hofstede (1991): power distance, masculinity/femininity, individualism/collectivism, and uncertainty avoidance. They excluded long-term/short-term orientation. For regulation approach, they used five regulation models: self-help, voluntary control, data commissioner, registration, and licensing.

of the information (e.g., secondary use versus sharing information with third parties). Phelps et al.'s (2000) mail survey responses of 556 U.S. customers supported these findings.

Impact of Customers' Privacy Concerns on Customers' Behavior

Several attempts have been made to study the effects of customers' privacy concerns on their *privacy behavior*, which includes searching for privacy information, assessing companies' privacy policies and related privacy risks, providing or withholding certain personal information, and purchasing, which entails the provision of a certain amount of personal information.

Customers can look for privacy information by searching for privacy policy statements, privacy seals, and other information such as news releases about a company's privacy practices. Earp and Baumer (2003) conducted an online survey of 415 U.S. users and showed that younger online users (i.e., ages between 12 and 35) were more inclined to read the privacy policies of websites than older online users (i.e., ages over 35). They also found that individuals were more concerned about the presence of privacy policies than about the content of these policies. Milne and Culnan (2004) examined why online users read online privacy notices by conducting an online survey of 2,468 U.S. Internet users. They found that individuals tended to read privacy notices if they had higher concerns about the organization's privacy practices. They also observed that participants were more likely to read privacy notices when the notices were presented in a format they could understand, and were less likely to read privacy notices if they had alternative sources of information such as prior experience, company reputation, or the presence of a privacy seal.

Customers can weigh the privacy policies and practices disclosed by companies to determine whether they meet their privacy needs. To do this, they must read, understand, and weigh the disclosures and make a judgment about whether and how much personal information to provide to the company. As noted previously, many individuals find privacy policy statements difficult to read because at least some college education is required to understand the complex words and sentence structures found in most privacy policy statements (Proctor et al. 2008). Vail et al. (2008) used a survey of 993 Internet users to examine individuals' perception and comprehension of privacy policies on websites with respect to four types of privacy policy representations (i.e., typical format, goal/vulnerability statements, categorical format, and goals/vulnerabilities in policy). They found that individuals associated the typical policy presentation format with higher security compared with other formats, but they comprehended privacy policies presented in other formats better.

Customers can provide none, some, or extensive personal information. They can also provide false information. Earp and Baumer's (2003) survey of 415 U.S. online users showed that the type of website (i.e., retail, financial, or medical/health) and brand status (e.g., well-known versus unknown websites) influenced individuals' willingness to provide information. Sheehan and Hoy (1999) also found that U.S. online users were less likely to register for a website when their privacy concerns were high. In addition, as privacy concerns increased, online users were more likely to provide incomplete information and took protective actions (e.g., notified Internet service providers about unsolicited email and sent negative messages to those sending unsolicited email).

Lwin and Williams (2003) developed a conceptual model to investigate a customer's behavior in providing false information online based on two theories: Multidimensional Developmental Theory of Privacy (MDTP) and Theory of Planned Behavior (TPB) with an additional factor of perceived moral obligation. They conducted an empirical study to test the TPB portion of the conceptual model using a mail survey of 341 U.S. online users. Their results indicated that individuals are more likely to fabricate their information when they have complete control over providing their personal information and when they perceive less moral obligation to provide accurate information.

Finally, several studies have examined the relationship between customers' privacy concerns and their purchasing decisions. Koyuncu and Lien (2003) found that individuals who were more concerned about their privacy tended to purchase less over the Internet. George (2002) also examined the relationship among beliefs about privacy and Internet trustworthiness, purchasing intention, and purchasing behavior. A survey of 1,194 U.S. online users and 193 undergraduate students, respectively, revealed that beliefs about privacy and Internet trustworthiness helped shape attitudes toward the Internet, which in turn, affected purchasing intentions and purchasing behavior. George (2004) also found that customers' purchasing behavior was affected by beliefs about self-efficacy (through perceived behavioral control), but not by beliefs about unauthorized use of personal information.

Privacy Solution Provider (PSP) Perspective

This section addresses research on privacy issues related to PSPs such as privacy consulting and assurance services, privacy seals, and privacy-enhancing technologies such as P3P, physical and logical access controls, data communication controls (encryption), and other security technologies for e-commerce (see Boritz 2005).

Privacy Consulting and Assurance Services

The AICPA/CICA developed a privacy framework called the Generally Accepted Privacy Principles (GAPP), which can be used by public accountants to guide and assist organizations implementing privacy practices and policies (AICPA/CICA 2009). GAPP are based on the fair information practices included in privacy laws and regulations of various jurisdictions around the world, meant to ensure that personal information is collected, used, retained, and disclosed in conformity with the commitments in the entity's privacy notice and with criteria set forth in the GAPP principles. Table 2 provides a summary of the GAPP principles.

For each of the ten GAPP principles, relevant, objective, complete, and measurable criteria have been developed for evaluating an entity's privacy policies, communications, procedures, and controls. The scope of a privacy assurance engagement can cover: (1) either all personal information or only certain identified types of personal information, such as customer information or employee information; and (2) all business segments and locations for the entire entity or only certain identified segments of the business (e.g., retail operations, but not manufacturing operations, or only operations originating on the entity's website or specified web domains) or geographic locations (e.g., only U.S. operations). The scope of the engagement would cover all of the activities in the "information life cycle" for the relevant personal information, including collection, use, retention, disclosure and destruction, de-identification, or anonymization. When the privacy engagement relates to an online segment, the scope needs to include, as a minimum, an online business segment of the entity. For these engagements, an entity may choose to display a privacy seal.

It is noteworthy that the focus of these GAPP principles is on conformity with the commitments in the entity's privacy notice, rather than adherence to an external standard of fairness. This creates room for misalignment of individuals' privacy concerns and corporate privacy practices as found, for example, by Earp et al. (2005) in their study of the FTC's FIPs. The approach taken by GAPP places the onus on the user of an e-commerce site to read and understand the entity's privacy notice, since each entity can choose different practices. As we have already noted, research indicates that users do not find this easy to do and a privacy seal may mislead users into believing that the company's privacy practices meet some external standard, rather than indicating that the company complied with its own privacy notice.

There have been few published studies on the AICPA/CICA's GAPP and related consulting or assurance services involving GAPP. Prosch (2008) discussed how GAPP can be used to facilitate corporate operations and supervision over personal information, by implementing Continuous Control Monitoring (CCM) environments. She also introduced a Privacy Lifecycle Maturity Model to assist researchers and members of industry in enhancing data protection techniques for personal information.

Greenstein and Hunton (2003) examined skills that potential clients view as necessary to perform privacy services and whether they perceive that CPA firms possess such skills. They also investigated whether potential clients are likely to hire a CPA firm to perform privacy services and whether a brochure produced by the AICPA changes potential clients' beliefs regarding CPA firms' qualifications. Based on an experiment with 82 corporate manager participants representing 27 companies, they identified four skill-level categories that the managements of audit clients view as necessary: technical skills, legal skills, control/assurance skills, and strategic skills. Managers believed that CPA firms had high technical and control/assurance skills, but low strategic and legal skills. They also found that many respondents thought that privacy services should be separated from the auditing engagement and had low willingness to engage a CPA firm to conduct privacy services. However, the brochure produced by the AICPA influenced managers' perceptions regarding the ability of CPA firms to perform privacy services. The brochure had the greatest impact on perceptions of technical skills, legal skills, and strategic skills.

Privacy Seals

The existence of privacy principles such as the FTC's FIPs led to the creation of privacy seal programs. A privacy seal is an identifiable symbol or logo, voluntarily displayed on a website, which graphically asserts that the site has implemented and complies with specified privacy practices. Although there are several recognized privacy seal programs (Table 3), the majority of companies involved in such programs currently participate in either TRUSTe or BBBOnLine, but the number of participants is a tiny fraction of all e-commerce sites.

A number of studies have examined the role of privacy seals in e-commerce. Shapiro and Baker (2001) postulated that information privacy is socially constituted by a complex network of social institutions. They argue that the existing judicial, legislative, and private sector initiatives in North America and Europe do not adequately achieve the goals of informed consent and other fair information practices, and that privacy attestation will play a limited privacy protection role. Gendron and Barrett (2004) conducted a longitudinal field study to examine the accounting profession's attempt to develop a new market for their expertise through an assurance service that leads to granting a client the WebTrust seal. In particular, they addressed the ways in which WebTrust was originally developed and reshaped by accounting institutes, how advocates established WebTrust in the business-to-consumer (B2C) and business-to-business (B2B) market, and how the meaning of WebTrust performance shifted over time.

Kaplan and Nieschwietz (2003) developed a web assurance services model of trust for B2C e-commerce that illustrates the relationships among web assurance services, trust, and outcomes. By conducting an experiment with 225 participants, they showed that perceptions about assurance and web assurance services provider attributes influenced the formation of trust which, in turn, affected customers' willingness to purchase products, the perceived quality of products, and the perceived risk of engaging in transactions over the Internet. Prior studies also showed that a firm's participation in a privacy seal program favorably influenced individuals' information-providing and purchasing behaviors (e.g., Kovar et al. 2000; Lala et al. 2002; Nikitkov 2006). However, other studies found that the presence of a privacy seal did not affect individuals' behavior (e.g., Hui et al. 2007; Moores 2005).

TABLE 3

Dominant Privacy Seal Programs[a]

	TRUSTe	BBBOnLine	WebTrust
Organization	• Independent, nonprofit privacy organization	• Council of Better Business Bureaus	• American Institute of Certified Public Accountants (AICPA) • Canadian Institute of Chartered Accountants (CICA)
Established Year	1997	1999	1998
URL	http://www.truste.org	http://www.bbbonline.org	http://www.webtrust.org
Process	1. Create a privacy statement. 2. Complete the required paperwork. 3. Certification and review process by TRUSTe. 4. Place TRUSTe seal on the website.	1. Complete the Business Application. 2. Sign Participation Agreement and pay program fee. 3. Install the BBB Accredited Business seal on the website.	1. Contact a WebTrust provider. 2. Meet the WebTrust's Principles for Privacy as measured by the WebTrust Criteria. 3. Obtain an unqualified report from the WebTrust provider and place WebTrust seal on the site.
Complaint Mechanism	• WatchDog Dispute Resolution: Online third party dispute resolution for complaints reported by customers regarding a licensed TRUSTe website.	• Privacy Policy Review Service (PPRS): Dispute resolution process for determining the eligibility of a complaint and evaluating, investigating, analyzing, and making a decision on a complaint.	• The corporate privacy officer or other designated individual initiates privacy-related complaints, disputes, and other problems. • If problems are identified, remediation plans are developed and implemented.
Seal Holders (as of October 2006)	2,598	707	25

[a] Source: TRUSTe (http://www.truste.org), BBBOnLine (http://www.bbbonline.org), and WebTrust (http://www.webtrust.org).

Horton et al. (2001) investigated the effect of assurance services (i.e., WebTrust) on financial analysts' earnings forecasts and stock price estimates. By analyzing a survey of 37 financial analysts and conducting an experiment with 87 analysts, they found that financial analysts perceived the WebTrust seal as a positive economic signal (e.g., the presence of a WebTrust seal would increase customers' trust and confidence in the vendor, escalate sales, and enhance competitive position). The analysts issued more positive earnings forecasts and stock price estimates when an e-commerce company acquired e-commerce assurance (i.e., WebTrust) and vendor- and outcome-based risks were high (i.e., the company was unknown and the perceived outcome risk from transactions was high).

Privacy-Enhancing Technologies

Privacy technologies can help both companies and customers to protect privacy during information collection, recording, and use. Such technologies should be considered in the design of

e-commerce systems and controls, but there has been limited research about the use of privacy technologies such as P3P, encryption, and other technologies in e-commerce. Oppliger (2005) provided an overview of the privacy-enhancing technologies that enable individuals to browse websites and publish on the web with complete anonymity. Smith and Shao (2007) also reviewed existing privacy technologies, analyzed the limitations of such technologies, and identified future directions for privacy-enhancing technologies. Although there are several privacy-enhancing technologies, P3P, encryption, and access controls are the most common technologies for privacy protection.

Platform for privacy preferences (P3P). The P3P is a standardized, machine-readable protocol, which enables a user to exercise his or her preferences over website privacy practices (Reagle and Cranor 1999). It is designed to block access to a website or automatically notify online users if the website's privacy policies are not in line with their prespecified privacy preferences; the users are then left to decide whether they still want to use the service. Grimm and Rossnagel (2000) provided an overview of P3P in terms of its history and current state and examined the effect of P3P against legal requirements. Cranor et al. (2002) examined the role of P3P in customers' privacy behavior using the AT&T Privacy Bird.[10] They found that the use of the Privacy Bird guided users to read privacy policies more often and protected their privacy more proactively. Hochheiser (2002) described three proposed P3P privacy models (OECD, U.S. FTC, and Canadian Fair Information Practices), but criticized P3P for the lack of enforcement mechanisms, ambiguities in P3P's vocabulary, and the difficulty of managing complex privacy policies and preference statements. Ashley et al. (2002) addressed the formal model of the Platform for Enterprise Privacy Practices (E-P3P), the semantics (XML) of the E-P3P language, and the authorization engine processing for enterprise privacy policies. Lee and Stamp (2008) introduced Privacy-Enhancing Agent (PEA), a P3P-based software agent, which is designed to help users by automatically retrieving, evaluating, and responding to companies' privacy policies while respecting users' privacy preferences.

Encryption. While there is an extensive literature on encryption in the context of information security, we found few studies that examined encryption in the context of privacy and none in the context of e-commerce and privacy. One of the more popular encryption schemes is Public Key Infrastructure (PKI), which uses public keys and private keys to encrypt and decrypt information. A sender encrypts a message (i.e., information) using a recipient's public key, which is open to everyone, and the recipient uses a matching private key, which is a secret and only known to him or her, to decrypt the message. This, therefore, has the effect of ensuring privacy of personal information exchanged over the Internet and stored in databases. Widespread adoption of PKI requires a technology infrastructure that is currently lacking. However, a key element of the PKI infrastructure that is in place is the reliance on Certification Authorities (CA) to verify the identity of an organization/entity prior to issuing a digital certificate that the organization/entity can use to authenticate its public keys for use in e-commerce. WebTrust for CAs is an assurance service provided by licensed CPA firms on the effectiveness of internal controls surrounding the issuance of digital certificates by CAs. We found no research on this version of WebTrust and it seems that many AIS researchers are not aware of this assurance service.[11]

A detailed examination of encryption technologies is outside the scope of this review, but relevant sources are Rice (1986), Weise (2001), and Kaya et al. (2009). Seničar et al. (2003) discuss

[10] The AT&T Privacy Bird is software designed to inform users about the privacy policies of websites they visit. It reads privacy policies written in P3P and informs the website's policies by displaying a bird icon. A green bird icon appears for websites that match users' privacy preference, but a red bird icon appears for websites that do not.

[11] More information about this program may be found at: http://www.cica.ca/service-and-products/business-opportunities-for-cas/trust-services/

the use of encryption and steganography technologies to enhance privacy on the Internet. Steganography is the creation of a hidden message in such a way that no one except the sender and intended recipient knows of or suspects the existence of the message (Provos and Honeyman 2003).

Access controls and other security technologies. Physical and logical access controls are key privacy protection techniques, as is evident from the summary of GAPP in Table 2. Protecting personal information against unauthorized access, while at the same time providing access to such information to customers to enable them to control its accuracy and use, can be challenging in an e-commerce context. However, these issues have attracted little notice in the AIS research community.

As new technologies become available, companies and other parties may adopt new means for invading customer privacy (e.g., RFID and biometrics) requiring new privacy countermeasures. Kenny and Korba (2002) introduced a potential tool for the management of personal information, Digital Rights Management (DRM), and proposed the adaptation of DRM technology to address the implementation challenges (e.g., scalability and extensibility) in Privacy Rights Management (PRM). DRM was developed to facilitate the distribution of digital information by protecting it against breaches of copyright law. DRM was designed to control what hardware manufacturers, publishers, copyright holders, and individuals can do and cannot do with digital content and devices. The three aspects of DRM functionality that could be used to protect privacy are asset creation, asset management, and asset usage. Asset creation allows digital content creators to assign rights to the content and ensures content may only be created from existing content if the rights exist to do so. Asset management supports the access and retrieval of both content and metadata in distributed databases. Asset usage supports permission management and audit trail functionality, which provides a means for monitoring and tracking content use. These three functionalities could be used to help control the collection, distribution, and use of personal information.

Government Perspective

System developers, managers, and auditors must consider the impact of relevant privacy laws and regulations on the design, operation, and maintenance of e-commerce systems and controls. This section reviews studies pertaining to government regulation of privacy in e-commerce, including regulation approaches and factors influencing regulation. The impact of regulation on companies' privacy practices is discussed in the section of the paper that deals with stakeholder interactions.

Regulation Approaches

Most studies of governments' role in protecting privacy are in a general information privacy context, which does not focus on, but includes, e-commerce privacy. Caudill and Murphy (2000) discussed online privacy conceptually, summarized privacy regulations in the United States, and proposed ethical standards that need to be addressed in corporate ethical policy and public policy. Smith (2001) investigated the differences in privacy approaches in the United States and Europe, suggesting that the voluntariness of the U.S. privacy approach limits its ability to address privacy concerns and the secondary uses of personal information. Laudon (1996) asserts that the FIPs proposed by the U.S. FTC leave individuals little or no control over the post-collection use of personal information (e.g., right for review and challenge). As one possible solution for such problems, he proposed a National Information Market (NIM) in which personal information could be bought and sold, enabling individuals to receive fair compensation for the use of information about themselves.

By using the same procedure, Jamal et al. (2003, 2005) examined 56 high traffic e-commerce sites in the United Kingdom and compared the results with their previous study (i.e., Jamal et al. 2003). They concluded that regulation in the United Kingdom (i.e., E.U. Directive) did not improve the privacy disclosures or the privacy practices of U.K. companies, compared to U.S. companies. Therefore, governmental intervention through regulation is not necessary because the e-commerce industry develops satisfactory industry standards or norms in the absence of government regulation. However, since there are many unknowns in the comparison between U.S. and U.K. e-commerce sites (such as their respective starting points, litigation environment, etc.) the weaker practices in the United Kingdom may also be viewed as grounds for the imposition of even more regulation rather than favoring a self-regulation approach. Or, it may be that fear of litigation in the United States is a more effective mechanism than government regulation.

Factors Influencing Government Regulation

As was the case with regulation approaches, we found research on factors influencing government regulation in a general information privacy context but none that specifically addressed e-commerce. Milberg et al. (1995) examined the interrelation among nationality, cultural values, and information privacy regulatory approaches. They found that the amount of government involvement (e.g., voluntary control, data commissioner, and regulation) was related to the cultural values identified by Hofstede (1980). That is, countries with higher level of uncertainty avoidance or power distance tended to have higher levels of government involvement (e.g., regulation), but those with high individualism had less government involvement in regulating information privacy (e.g., voluntary control). Milberg et al. (2000) also examined the relationship between cultural values and regulatory approaches. They found that countries with a higher level of power distance, masculinity/femininity, and individualism/collectivism each tended to have less government involvement, but countries with high uncertainty avoidance had higher levels of government involvement in the regulation of information privacy practices. Hence, their results were quite different from Milberg et al. (1995).

Company-Customer Interaction

Three types of company-customer interactions have been studied: the interaction (1) between a company's characteristics and customer perceptions/attitudes, (2) between a company's characteristics and customer behavior, and (3) between a company's privacy disclosures and practices and customer behavior.

Company Characteristics and Customer Perceptions/Attitudes

Milne and Boza (1999) examined the relationship between privacy concerns and trust by analyzing a mail survey of 1,508 U.S. respondents. They showed that trust was negatively related to privacy concerns, and that customers' perceptions of trust and level of concern about privacy varied by industry.[12] Earp and Baumer's (2003) online survey of 415 U.S. respondents showed that the type of website (i.e., retail, financial, or medical/health) and brand status (e.g., well-known versus unknown websites) influenced individuals' willingness to provide information.

[12] Banks, insurance, telephone, and credit card industries generated high privacy concerns. Internet access, magazines, and catalog companies generated moderate levels of privacy concerns. Airlines, bookstores, and video stores generated the lowest privacy concerns.

Company Characteristics and Customer Behavior

Swaminathan et al. (1999) examined factors affecting online purchasing behavior. Their analysis of 428 email responses indicated customers' online purchasing behavior was influenced by the perceived reliability of a vendor, the convenience of placing an order and contacting the vendor, price competitiveness, and access to information. They also showed that, on average, customers were not overly concerned about security or privacy, but customers who purchased frequently on the Internet were interested in new regulations protecting privacy on the Internet. Ranganathan and Ganapathy (2002) examined key dimensions of B2C websites as perceived by online customers. Based on an online survey of 214 U.S. online shoppers, they identified four key dimensions of B2C websites (i.e., information content, design, security, and privacy) and, contrary to Swaminathan et al. (1999), found that privacy had a significant effect on customers' purchase intentions.

Company Privacy Disclosures and Practices and Customer Behavior

Several researchers have explored whether customers' willingness to provide personal information as well as their purchasing behavior can be influenced, in part, by the quality of companies' privacy practices addressed in their privacy policy disclosures. Meinert et al. (2006) surveyed 261 graduate students' willingness to provide various types of personal information, given various levels of protection offered by privacy policy statements. They found that more than half of the participants had never read a privacy policy statement even though they were aware of privacy policy statements. However, respondents' willingness to provide their personal information increased as the level of protection offered by the statements increased, and depended on the type of information requested. Culnan and Armstrong (1999) studied the role of procedural fairness (i.e., FIPs) in addressing privacy concerns based on telephone interviews of 1,000 U.S. customers, and found that people with greater privacy concerns were less willing to be profiled when they were not told that FIPs were employed to manage their personal information.

LaRose and Rifon (2007) examined the effect of explicit privacy warnings about information practices stated in a website's privacy policy by conducting an experiment involving 227 undergraduate students. They found that explicit privacy warnings that clearly present the possible negative consequences associated with disclosure of personal information increased the individuals' perceptions of the risks associated with information practices and decreased their intentions to provide personal information.

Similarly, Miyazaki and Fernandez (2000) and Ranganathan and Ganapathy (2002) found that online purchase intention was influenced by the extensiveness of the company's privacy and security disclosures.

Company-Privacy Solution Provider (PSP) Interaction

In this section, we review studies that have investigated the relationship between companies and PSPs. The research that we identified addressed company privacy policies and practices in the context of privacy seal programs and privacy technologies such as P3P.

Company Privacy Policies and Practices and Privacy Seals

Prior research has mainly focused on the impact of privacy seals on customers' perceptions and behaviors. Little research has been conducted on the interaction between companies and seal-program providers. Palmer et al. (2000) examined how firms use privacy seals and privacy statements to build trust on their websites. By analyzing the websites of 102 publicly traded U.S.

companies, they showed that the embeddedness of the firm (i.e., the number of links into a website) increased the use of privacy statements and privacy seals. They also found that the more experience a firm had with the Internet, the more negative the effect on its use of privacy statements and trusted third parties. Sivasailam et al. (2002) conducted a survey of 72 B2C e-commerce companies from four industry sectors: computers and office equipment, general merchandisers, specialty retailers, and apparel, and found that companies in those sectors were only marginally interested in obtaining assurance seals. They also found that large companies tended to obtain more privacy seals than mid-size or small firms, and companies in the computer and office equipment industries had more privacy seals than specialty or apparel retailers. Pollach (2007) examined the privacy policies of 50 successful e-commerce sites and showed that less than half of the sites (i.e., 19 of the 50 sites) displayed at least one privacy seal. She also found that there were no significant differences between companies with and without seals, with respect to the coverage of privacy practices and communicative quality (i.e., ambiguity) in their privacy policies.

Company Privacy Practices and Privacy-Enhancing Technologies

Several attempts have been made to address the link between companies' privacy practices and privacy technologies. For instance, Reay et al. (2007) conducted a survey to examine the adoption of P3P on websites. They found that the adoption of P3P was relatively stable, but many P3P documents contained errors such as violations of the P3P XML schema and basic XML document structure. Prior studies argued that the limited adoption of P3P may be caused by the lack of enforcement (Turner and Dasgupta 2003), the lack of motivation to adopt rigorous policy automation by organizations (Hochheiser 2002), and the lack of appropriate user control mechanisms and interfaces for delivering the P3P policy (Ackerman 2004). Also, Cranor et al. (2008) examined the companies' privacy policies encoded using P3P. They found that P3P adoption had increased but varied across industries. They also discovered high rates of syntax errors among P3P policies, although most of the errors were not critical errors. They also observed several discrepancies between P3P policies and their natural language counterparts (i.e., human-readable privacy policies).

Company-Government Interaction

Government regulation can influence companies' practices and industry self-regulation, and companies' practices, in turn, can influence government regulation by increasing or decreasing the perceived need and pressure for regulation.

Impact of Company Privacy Practices on Government Regulation

As noted previously, there has been virtually no research on government regulation and privacy in an e-commerce setting. Milberg et al. (2000) showed that high levels of privacy concern are associated with greater preferences for strong laws over self-regulation. Presumably, pressures arising out of weak e-commerce privacy practices would lead to increased government regulation. However, regulatory approach is not based solely on the quality of corporate privacy management. It is also a function of regulator preferences—regulators in countries with higher levels of governmental involvement tended to have higher preferences for government regulation over corporate self-management.

Impact of Government Regulation on Company Privacy Practices

Milberg et al. (2000) also showed that countries with higher levels of governmental involvement tend to have stronger corporate privacy policies and practices and more supportive

senior management attitudes. Based on an analysis of privacy policy disclosures on 149 B2C websites across countries and industries, Johnson-Page and Thatcher (2001) also found that in some contexts, regulations improved privacy practices. Clear business regulations were associated with greater use of privacy policy statements in countries with an established market economy in which customers not only had more access to the web, but also had more experience in using it. However, as noted previously in connection with research on P3P, Reay et al. (2009a) found a lack of adherence to legal mandates in companies' stated privacy policies. Also, as noted earlier, Jamal et al. (2003) found that privacy practices in a more regulated environment (i.e., the United Kingdom) were not better than those in a self-regulated environment (i.e., the United States), but there have not been any similar studies comparing other jurisdictions.

IV. OPPORTUNITIES FOR RESEARCH

The MIS and AIS disciplines deal with collecting, recording, and using information to support entity objectives. These activities could impinge on individuals' privacy rights, making privacy an important issue for MIS and AIS researchers and practitioners. As evidenced by our literature review, research on privacy in the e-commerce context has contributed to our understanding of privacy issues in e-commerce, but there are still many research areas that need to be explored. In this section, we discuss research opportunities for the MIS and AIS research community.

Company Perspective

The most researched area in connection with the company perspective on e-commerce privacy has been disclosure of privacy policies, but research opportunities abound in areas related to all four objectives pertaining to companies' privacy risk management as discussed below.

Strategic Objectives

Prior research has suggested that privacy constitutes one of the four main dimensions by which customers evaluate e-commerce sites (Ranganathan and Ganapathy 2002). This makes privacy protection a strategic asset (Ashworth and Free 2006) that should lead companies to consider privacy protection as a means for growing revenues and achieving other strategic objectives (e.g., avoiding regulation) and should, thus, encourage them to proactively manage their privacy policies for this purpose. However, many companies' strategic objectives regarding privacy are defined by existing and pending legislation (Sarathy and Robertson 2003). In other words, privacy policies are often designed to protect companies from potential privacy litigation (Earp et al. 2005; Papacharissi and Fernback 2005; Pollach 2007) rather than to enhance revenues. Research is needed to investigate the factors and conditions that lead some companies to take a proactive approach toward developing privacy policies to respond effectively to customers' privacy concerns as well as legal requirements, while others focus primarily on regulatory compliance. Sarathy and Robertson's (2003) model of factors influencing privacy strategy, which incorporates the environmental context, ethical perspective, and firm-specific considerations, has not been empirically tested; thus, it represents an important research opportunity, albeit a challenging one.

Furthermore, research could examine the relationship between privacy practices and trust in e-commerce. Prior studies showed that customers' privacy concerns negatively affect their trust, which, in turn, negatively influences their purchase intent toward the company (Eastlick et al. 2006; Liu et al. 2005; Kaplan and Nieschwietz 2003). Since individuals may have various dimensions of trust, future research could examine how factors such as firm reputation, prior

experience, and third-party assurance seals contribute to the development of trust in e-commerce companies' privacy practices and influence their commitment toward doing business with those companies.

Although there have been several studies of the impact on company share price of security breaches that compromised the confidentiality of company information (e.g., Campbell et al. 2003; Anthony et al. 2006), there has been no parallel study of the impact of failures to protect personal information. A study of public company privacy breaches such as Google (Hughes 2010) and Twitter (Efrati 2010) would be a welcome addition. A related question is whether investing in good privacy practices yields an ROI that demonstrates that such an investment adds more value than treating privacy as a compliance (cost-generating) activity. Research is also needed to examine how effectively the inclusion of privacy protection among a company's strategic goals affects the company's actual privacy practices.

Operations Objectives

Prior studies have focused on privacy policy disclosures, rather than actual privacy practices in terms of the collection and use of personal information, and their impact on customers' privacy behavior. Research is needed to examine actual privacy-related operations (e.g., use of cookies, data retention practices, and privacy complaint-handling processes) and investigate their impact on customers' privacy concerns. Researchers should also study whether and how companies' use of new technologies, such as RFID and GPS, encroaches on their customers' privacy and what measures companies take to obtain the strategic benefits from such technologies without undermining customers' trust that their personal information is protected.

In addition, various privacy-enhancing technologies (e.g., encryption, digital signatures, steganography, and DRM) have been developed to protect privacy, but few studies have examined them in an e-commerce setting. Researchers should study how and how well companies use privacy-enhancing technologies to protect their customers' privacy, the drivers or conditions that lead some companies to adopt privacy-enhancing technologies when others do not, and the related costs and benefits.

Disclosure Objectives

Prior studies suggest that an organization's privacy policies help build trust and promote the disclosure of personal information (Culnan and Armstrong 1999; Milne and Boza 1999). Indeed, many studies have shown that a growing number of companies are disclosing their privacy policies to communicate their efforts to protect customers' privacy and reduce their customers' privacy concerns. However, a growing body of literature suggests that the content of privacy policies does not match the information wanted by customers. Also, companies' privacy policy statements are often written to serve as legal protection for companies, more than to inform and protect customer privacy (Earp et al. 2005; Papacharissi and Fernback 2005; Pollach 2007). Several studies have shown that most customers do not read companies' privacy policies and that many privacy policies are unreadable because of their length and the educational level required to understand them (Antón et al. 2004; Milne and Culnan 2004; Milne et al. 2006; Pollach 2007). It would be useful to investigate why companies do not match the content of their privacy policies to customer preferences, and how companies can better communicate their privacy efforts to customers without requiring them to read the legalese of current privacy notices.

Also, research should investigate the differences between websites that post privacy policies and sites that do not; whether the sites with and without privacy policies share common characteristics; and whether the websites with the best privacy disclosures have better IT

governance, better financial performance, better shareholder value, or better corporate social responsibility reputations.

Compliance Objectives

Past research addressing compliance has focused on the most-visited sites and has only addressed a limited set of privacy issues such as opt-out provisions. Also, as stated earlier, most studies have examined privacy disclosures rather than actual privacy practices of e-commerce companies. Thus, companies' compliance with privacy issues such as those listed by the OECD or GAPP has not been studied to the degree that it should be to reveal to what extent companies' actual collection and sharing of personal information comply with their stated privacy policies and applicable laws and regulations. For instance, a researcher could examine the actual privacy practices of companies by developing a software agent (i.e., software that can examine companies' actual privacy practices such as what personal information a company collects) and compare this against their privacy policy statements.

Schwaig et al. (2006) showed that B2C companies complied more often with the FTC's FIPs than B2B companies did. Considering the relative magnitude of B2B e-commerce relative to B2C e-commerce, this is both a concern and a topic for research. In addition, cloud computing may intertwine B2C and B2B e-commerce activities. Personal information originated at the customer-facing B2C website may be exchanged in a cascading manner among business partners and service providers in a supply chain. Research is needed to provide insights into privacy practices at B2B companies, especially in a cloud computing environment.

Company-Customer Interaction

Companies that address customers' privacy concerns should influence customers' propensity to visit their websites more often, to share personal information, and to transact more. Companies are more likely to address customers' privacy concerns if they realize significant benefits from doing so, such as obtaining a competitive advantage through building strong customer relationships. Therefore, an issue worthy of research attention is whether companies actually do benefit by addressing customers' privacy concerns. Longitudinal research could help to assess the impact of companies' privacy practices on customer relationships (e.g., customer acquisition, retention, and profitability). As noted earlier, individuals are often willing to give up some degree of privacy for certain rewards (Caudill and Murphy 2000; Shapiro and Baker 2001).

Although companies like Google (Claburn 2010) try to reduce online users' privacy concerns by simplifying their privacy policies and providing privacy tools, research has not yet identified the most efficient and effective ways for companies to lessen key customer concerns. It may be that companies are not differentiating their privacy messaging sufficiently to address the differential privacy concerns of distinct categories of privacy concerns among their actual and potential customer base. Taking a one-size-fits-all approach to privacy communications may not satisfy the diverse privacy concerns of distinct customer categories identified in prior research (e.g., Sheehan 2002; Milberg et al. 2000). Differential privacy messaging has not, hitherto, been investigated. To what extent are various classes of customers willing to provide their personal information for rewards, such as discount coupons and free gifts, and do they perceive such trade-offs as fair? How can privacy disclosures posted on a central e-commerce site effectively inform and satisfy customers located in various geographical and cultural regions? How should such disclosures vary as the nature of the e-commerce activities (e.g., health care-related products and services, financial services, general merchandise sales) varies?

Social networking has become very popular among online users. Social networking sites like Facebook, MySpace, and Twitter are online communities where individuals communicate and share

personal content (e.g., profiles, journals, and photos) with other users. Since such sites store a huge amount of possibly sensitive personal information on users and their interactions, there are growing concerns about privacy in social networking sites (Lippman 2010; Steel and Vascellaro 2010; Goldie 2009). Models of trust in an e-commerce setting have not yet incorporated the impact of social networking on customers' trust in e-commerce and their related privacy behavior. Thus, researchers should investigate the differences between privacy-related concerns, behaviors, and practices in a social networking environment versus a standard e-commerce environment.

Company-Privacy Solution Provider Interaction

GAPP provides a control framework for addressing e-commerce privacy. There is virtually no research on how GAPP are being used by companies, even though the accounting profession (through the AICPA/CICA Trust Services Task Force) has devoted significant resources to developing privacy consulting and assurance services around GAPP. Research is needed to examine to what extent and how GAPP and related Trust Services are being used in e-commerce and how they compare to other privacy principles such as the U.S. FTC's FIPs and OECD guidelines. Also, the GAPP model appears to focus on a company's compliance with the commitments made in its own privacy notices rather than its compliance with FIPs. Is this a viable approach for addressing customers' privacy concerns?

Prior studies have shown that privacy seals are not popular among companies. Research is needed to investigate why privacy seals are not popular and why privacy seals currently posted on websites are not effective in dealing with customers' privacy concerns. It would also be interesting to examine whether there are specific situations in which privacy seals are perceived as useful. Without such research, e-commerce companies are understandably reluctant to expend resources to participate in privacy seal programs.

Privacy-enhancing technologies, such as access controls and encryption, are widely used in e-commerce for selected information such as credit card information transmitted over the Internet as part of an e-commerce transaction. However, other privacy technologies (e.g., P3P agents and DRM) have not been adopted as widely. Furthermore, many online users are not eager to purchase privacy software (Tuna 2010). There is little evidence to indicate that privacy-enhancing technologies improve customer privacy and that companies and individuals benefit from adopting such technologies. Therefore, it would be worth investigating whether privacy-enhancing technologies are more effective and efficient ways to enhance privacy, compared to alternatives such as government regulations and third-party assurance.

Company-Government Interaction

Making new regulations that balance companies' needs for personal information and customers' concerns about privacy requires taking into account companies' information-gathering activities and the context in which the information is used. It is generally assumed that existing and pending regulations influence companies' privacy practices, but research indicates that the degree of compliance with regulations is not very high in some jurisdictions. This may be due to companies' perceptions that privacy protection does not add value, which has been previously identified as an important topic for research to address. Another area for research is to examine how companies respond to new or pending regulations and whether and how these regulations enhance companies' privacy practices, reduce customers' privacy concerns, and, in turn, reduce pressure on governments to regulate privacy practices.

The differences in privacy regulations of each country may pose a significant regulatory challenge for companies looking to operate in multiple markets around the world. It would be interesting to learn whether companies operating in less strictly regulated countries have less-

comprehensive privacy practices than companies in more strictly regulated countries; or whether they create one policy and export it to weaker jurisdictions. Cultural values can also influence privacy concerns, practices, and regulations, but there has been no research on the impact of cultural values on privacy practices in an e-commerce setting. E-commerce websites from various cultural regions provide windows into privacy practices that could be used to gather research data for cross-cultural comparisons.

Finally, governments have the power to demand information from companies about themselves and their customers. For example, governments have sought disclosure of user identities and other personal information from Internet service providers (ISPs) to combat tax evasion, online gambling, copyright infringements, child pornography, and other infractions of local laws.[13] This is an area that has not been researched and where future work related to all four stakeholders and interactions among them is needed.

V. SUMMARY AND CONCLUSION

The spread of e-commerce and related technologies has enabled and encouraged companies to collect and store customers' personal information. E-commerce represents a potentially different context than other information privacy settings because participation in e-commerce has a built-in trade-off required between the necessity of providing at least some personal information to consummate a beneficial online transaction and the risk of negative consequences from providing personal information in the process. Of course, many companies are not satisfied with gathering the minimum amount of personal information required to process a transaction, but rather opt for gathering additional information to support their e-commerce strategies. As a result, the privacy of accumulated customer information is an issue of growing importance for customers, companies, PSPs, and governments.

The purpose of this paper is to review and summarize the literature on privacy in e-commerce and to suggest future research opportunities that will expand our understating of privacy issues in e-commerce. In this paper, we use a simple framework (see Figure 1) that identifies the key stakeholders and their interactions and helps to structure our review of prior research on privacy in an e-commerce setting around those stakeholders and their interactions. Table 1 summarizes the reviewed studies by year according to their contributions to the major research areas in e-commerce privacy identified in our framework. The most-researched area has been the customer perspective, possibly because e-commerce privacy issues arise from companies' desire to take advantage of customers' personal information and data relating to this area are easy for researchers to obtain through surveys. Interestingly, the company perspective has been much less researched, with most of the research addressing disclosure or compliance issues, leaving strategic and operations issues virtually unexplored. There has been virtually no empirical work relating companies' privacy behavior to factors such as their corporate and IT governance practices, financial performance, and market reactions. The government perspective appears to be significantly under-researched, given the amount of government regulation of privacy around the world. Again, this may be due to lack of access to data.

Reflecting on our review findings, we observe that most of the studies have relied on surveys of stakeholder groups; thus, they reflect opinions and attitudes rather than actual behaviors. Some studies have involved examinations of website content and have correlated this content with various factors. In many cases, the associations could be tenuous, since many factors and potential self-selection

[13] Canada is considering legislation allowing police and intelligence officers to access the online communications and the personal information of ISP subscribers (CBC News 2009). To monitor Internet and telephone communications, the British government plans to force telecommunication companies and ISPs to keep all their customers' personal communications and Internet traffic (Espiner 2008).

biases that are not controlled for are at play in companies' choices of website content. There is a need for research that uses experiments and other controlled observations as well as archival data. For these reasons, it would be desirable to see additional research employing other research methods such as studying actual behaviors rather than attitudes and opinions alone. For example, company privacy practices can be coded and correlated with governance metrics, performance metrics, and stock prices. Another reason for encouraging additional research is that e-commerce and attitudes about privacy are evolving. The issues surveyed in the early days of e-commerce are evolving with the passage of time, and the changes brought about by technological advances such as Internet access through mobile devices and the growth of social networking. Both of these have created new threats to privacy that have generated public debate about privacy issues that could be addressed by research. Therefore, there is a need for research on current attitudes and behaviors rather than relying solely on studies done during the infancy of the Internet and e-commerce.

Most of the studies that we found have examined privacy issues solely in a B2C e-commerce context. This is natural, since privacy pertains to personal information. However, there are significant privacy issues in the exchange of information in B2B settings, since B2B e-commerce can involve the transfer of personal information among business partners with different privacy practices and across jurisdictional boundaries with different privacy regulations (e.g., a cloud computing environment). Potential research questions include how the concept of privacy extends to the B2B environment; how privacy protection differs from confidentiality protection in a B2B context; and whether B2B firms consider privacy protection as a strategic issue or merely an operational or compliance concern.

In conclusion, we hope that this paper has effectively, albeit briefly, summarized the extant research on privacy in an e-commerce setting, and that it has identified interesting research opportunities for MIS and AIS researchers.

REFERENCES

Ackerman, M. S. 2004. Privacy in pervasive environments: Next generation labeling protocols. *Personal and Ubiquitous Computing* 8 (6): 430–439. doi:10.1007/s00779-004-0305-8

Ackerman, M. S., L. F. Cranor, and J. Reagle. 1999. *Privacy in E-Commerce: Examining User Scenarios and Privacy Preferences*. Paper Read at 1st ACM Conference on Electronic Commerce, Denver, CO, November 3–5.

Altman, I., 1975. *The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding*. Monterey, CA: Brooks/Cole.

American Institute of Certified Public Accountants/Canadian Institute of Chartered Accountants (AICPA/CICA). 2009. *Generally Accepted Privacy Principles*. New York, NY: AICPA/CICA. Available at: http://infotech.aicpa.org/Resources/Privacy/Generally+Accepted+Privacy+Principles/Generally+Accepted+Privacy+Principles.htm

Anthony, J. H., W. Choi, and S. Grabski. 2006. Market reaction to e-commerce impairments evidenced by website outages. *International Journal of Accounting Information Systems* 7 (2): 60–78. doi:10.1016/j.accinf.2005.10.002

Antón, A. I., J. B. Earp, H. Qingfeng, W. Stufflebeam, D. Bolchini, and C. Jensen. 2004. Financial privacy policies and the need for standardization. *IEEE Security & Privacy* 2 (2): 36–45. doi:10.1109/MSECP.2004.1281243

Arnold, V., and S. G. Sutton. 2002. *Researching Accounting as an Information Systems Discipline*. Sarasota, FL: American Accounting Association.

Ashley, P., S. Hada, G. Karjoth, and M. Schunter. 2002. *E-P3P Privacy Policies and Privacy Authorization*. Paper Read at the 2002 ACM Workshop on Privacy in the Electronic Society, Washington, D.C., November 21.

Ashworth, L., and C. Free. 2006. Marketing dataveillance and digital privacy: Using theories of justice to understand consumers' online privacy concerns. *Journal of Business Ethics* 67 (2): 107–123. doi:10.1007/s10551-006-9007-7

Bardeesy, K. 2009. Ottawa takes on social media giant for violating Canada's law. *The Globe and Mail* (July 17): A1–A4.

Baumer, D. L., J. B. Earp, and J. C. Poindexter. 2004. Internet privacy law: A comparison between the United States and the European Union. *Computers & Security* 23 (5): 400–412. doi:10.1016/j.cose.2003.11.001

Bellotti, V. 1997. Design for privacy in multimedia computing and communications environments. In *Technology and Privacy: The New Landscape*, edited by Agre, P. E., and M. Rotenberg, 63–98. Cambridge, MA: MIT Press.

Boritz, J. E. 2002. Information systems assurance. In *Research Accounting as an Information Systems Discipline*, edited by Arnold, V., and S. G. Sutton, 231–255. Sarasota, FL: American Accounting Association.

Boritz, J. E. 2005. *A Secure IT Infrastructure for E-Business*. Toronto, Canada: CICA.

Bowie, N. E., and K. Jamal. 2006. Privacy rights on the Internet: Self-regulation or government regulation? *Business Ethics Quarterly* 16 (3): 323–342.

Bustillo, M. 2010. Wal-Mart radio tags to track clothing. *Wall Street Journal* (July 23).

Campbell, K., L. A. Gordon, M. P. Loeb, and L. Zhou. 2003. The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. *Journal of Computer Security* 11 (3): 431–448.

Carr, N. 2010. Tracking is an assault on liberty, with real dangers. *Wall Street Journal* (August 6). Available at: http://online.wsj.com/article/SB10001424052748703748904575411682714389888.html

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

CBC News. 2009. ISPs must help police snoop on internet under new bill. *CBC News* (January 3). Available at: http://www.cbc.ca/technology/story/2009/06/18/tech-internet-police-bill-intercept-electronic-communications.html?ref=rss

Charters, D. 2002. Electronic monitoring and privacy issues in business-marketing: The ethics of the DoubleClick experience. *Journal of Business Ethics* 35 (4): 243–254. doi:10.1023/A:1013824909970

Claburn, T. 2010. Google trims privacy policy. *InformationWeek* (September 26 2010). Available at: http://www.informationweek.com/news/security/vulnerabilities/showArticle.jhtml?articleID=227300202

Committee of Sponsoring Organizations of the Treadway Commission (COSO). 1992. *Internal Control Integrated Framework*. New York, NY: AICPA.

Committee of Sponsoring Organizations of the Treadway Commission (COSO). 2004. *Enterprise Risk Management—Integrated Framework*. New York, NY: AICPA.

Cranor, L. F., M. Arjula, and P. Guduru. 2002. *Use of a P3P User Agent by Early Adopters*. Paper Read at Workshop on Privacy in the Electronic Society, Washington, D.C., November 21.

Cranor, L. F., S. Egelman, S. Sheng, A. McDonald, and A. Chowdhury. 2008. P3P deployment on websites. *Electronic Commerce Research and Applications* 7 (3): 274–293. doi:10.1016/j.elerap.2008.04.003

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 G. R. Milne. 2001. *The Culnan-Milne Survey on Consumers & Online Privacy Notices: Summary of Responses*. Washington, D.C.: FTC. Available at: http://www.ftc.gov/bcp/workshops/glb/supporting/culnan-milne.pdf

Desai, M. S., T. C. Richards, and K. J. Desai. 2003. E-commerce policies and customer privacy. *Information Management & Computer Security* 11 (1): 19–27. doi:10.1108/09685220310463696

Dhillon, G. S., and T. T. Moores. 2001. Internet privacy: Interpreting key issues. *Information Resources Management Journal* 14 (4): 33–37.

Dillard, J. F., and K. Yuthas. 2002. Ethics research in AIS. In *Research Accounting as an Information Systems Discipline*, edited by Arnold, V., and S. G. Sutton, 181–206. Sarasota, FL: American Accounting Association.

Earp, J. B., A. I. Anton, L. Aiman-Smith, and W. H. Stufflebeam. 2005. Examining Internet privacy policies within the context of user privacy values. *IEEE Transactions on Engineering Management* 52 (2): 227–237. doi:10.1109/TEM.2005.844927

Earp, J. B., and D. Baumer. 2003. Innovative web use to learn about consumer behavior and online privacy. *Communications of the ACM* 46 (4): 81–83. doi:10.1145/641205.641209

Eastlick, M. A., S. L. Lotz, and P. Warrington. 2006. Understanding online B-to-C relationships: An integrated model of privacy concerns, trust, and commitment. *Journal of Business Research* 59 (8): 877–886. doi:10.1016/j.jbusres.2006.02.006

Efrati, A. 2010. Google settles privacy lawsuit for $8.5 million. *Wall Street Journal* (September 3). Available at: http://online.wsj.com/article/SB10001424052748703946504575470510382073060.html

Espiner, T. 2008. Critics attack "dangerous" gov't comms-snooping plan. *ZDNet U.K.* (July 15). Available at: http://news.zdnet.co.uk/communications/0,1000000085,39447471,00.htm

Federal Trade Commission (FTC). 2000. *Privacy Online: Fair Information Practices in the Electronic Marketplace*. A Report to Congress, Washington, D.C.

Fowler, R., H. Bob, G. Kress, and T. Trew. 1979. Language and Control. London, U.K.: Routledge & Kegan Paul.

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

George, J. F. 2002. Influences on the intent to make Internet purchases. *Internet Research—Electronic Networking Applications and Policy* 12 (2): 165–180. doi:10.1108/10662240210422521

George, J. F. 2004. The theory of planned behavior and Internet purchasing. *Internet Research—Electronic Networking Applications and Policy* 14 (3): 198–212. doi:10.1108/10662240410542634

Goldie, L. 2009. Twitter's rapid growth raises regulation issues. *New Media Age* (February 25). Available at: http://www.nma.co.uk/news/twitters-rapid-growth-raises-regulation-issues/41620.article

Gray, G. L., and R. Debreceny. 2002. Research opportunities in electronic commerce. In *Research Accounting as an Information Systems Discipline*, edited by Arnold, V., and S. G. Sutton, 209–230. Sarasota, FL: American Accounting Association.

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

Grimm, R., and A. Rossnagel. 2000. *Can P3P Help to Protect Privacy Worldwide?* Paper Read at the 2000 ACM Workshops on Multimedia, Los Angeles, CA, October 30–November 3.

Gurau, C., A. Ranchhod, and C. Gauzente. 2003. "To legislate or not to legislate": A comparative exploratory study of privacy/personalization factors affecting French, U.K. and U.S. websites. *Journal of Consumer Marketing* 20 (7): 652–664. doi:10.1108/07363760310506184

Harper, J. 2010. It's modern trade: Web users get as much as they give. *Wall Street Journal* (August 7). Available at: http://online.wsj.com/article/SB10001424052748703748904575411530096840958.html

Harris Interactive. 2003. *Most People Are "Privacy Pragmatists" Who, While Concerned about Privacy, Will Sometimes Trade It Off for Other Benefits*. New York, NY: Harris Interactive. Available at: www.harrisinteractive.com/harris_poll/index.asp?PID=365

Harris, L., and Associates, and A. F. Westin. 1995. *Equifax-Harris Mid-Decade Consumer Privacy Survey*. Atlanta, GA: Equifax, Inc.

Hochheiser, H. 2002. The platform for privacy preference as a social protocol: An examination within the U.S. policy context. *ACM Transactions on Internet Technology* 2 (4): 276–306. doi:10.1145/604596.604598

Hoffman, D. L., T. P. Novak, and M. A. Peralta. 1999. Information privacy in the marketspace: Implications for the commercial uses of anonymity on the web. *The Information Society* 15 (2): 129–139. doi:10.1080/019722499128583

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

Hofstede, G. H. 1991. *Cultures and Organizations: Software of the Mind*. London, U.K.: McGraw-Hill.

Hoover, J. N. 2010. Federal CIOs issue cloud computing privacy framework. *InformationWeek* (August 25). Available at: http://www.informationweek.com/news/government/cloud-saas/showArticle.jhtml?articleID=227001084

Horton, R. P., T. Buck, P. E. Waterson, and C. W. Clegg. 2001. Explaining intranet use with the technology acceptance model. *Journal of Information Technology* 16 (4): 237–249.

Hoy, M. G., and J. Phelps. 2003. Consumer privacy and security protection on church Web sites: Reasons for concern. *Journal of Public Policy & Marketing* 22 (1): 58–70. doi:10.1509/jppm.22.1.58.17619

Hughes, D. A. 2010. Twitter settles FTC privacy charges. *Wall Street Journal* (June 25). Available at: http://online.wsj.com/article/SB10001424052748704911704575326774191987024.html

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

Ingram, M. 2009. Welcome to the social network, where your privacy has to be flexible. *The Globe and Mail* (July 17): A1–A4.

Jamal, K., M. Maier, and S. Sunder. 2003. Privacy in e-commerce: Development of reporting standards, disclosure, and assurance services in an unregulated market. *Journal of Accounting Research* 41 (2): 285–309. doi:10.1111/1475-679X.00104

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

Johnson-Page, G. F., and R. S. Thatcher. 2001. B2C data privacy policies: Current trends. *Management Decision* 39 (4): 261–271. doi:10.1108/00251740110391420

Kane, M., and M. Hines. 2005. ChoicePoint faces inquiry, will curtail data sales. *CNET* (March 4). Available at: http://news.cnet.com/ChoicePoint-faces-inquiry,-will-curtail-data-sales/2100-1029_3-5599516.html

Kaplan, S. E., and R. J. Nieschwietz. 2003. A web assurance services model of trust for B2C e-commerce. *International Journal of Accounting Information Systems* 4 (2): 95–114. doi:10.1016/S1467-0895(03)00005-8

Katzan, H., Jr. 2010. On the privacy of cloud computing. *International Journal of Management and Information Systems* 14 (2): 1–12.

Kauffman, R. J., Y. J. Lee, M. Prosch, and P. J. Steinbart. 2011. A survey of consumer information privacy from the Accounting Information Systems research perspective. *Journal of Information Systems* 25 (2): 47–79.

Kaya, S. V., E. Savas, A. Levi, and Ö. Erçetin. 2009. Public key cryptography based privacy preserving multi-context RFID infrastructure. *Ad Hoc Networks* 7 (1): 136–152. doi:10.1016/j.adhoc.2007.12.004

Kenny, S., and L. Korba. 2002. Applying digital rights management systems to privacy rights management. *Computers & Security* 21 (7): 648–664. doi:10.1016/S0167-4048(02)01117-3

Kovar, S. E., K. G. Burke, and B. R. Kovar. 2000. Consumer responses to the CPA WebTrust assurance. *Journal of Information Systems* 14 (1): 17–35. doi:10.2308/jis.2000.14.1.17

Koyuncu, C., and D. Lien. 2003. E-commerce and consumer's purchasing behaviour. *Applied Economics* 35 (6): 721–726. doi:10.1080/0003684022000020850

Lala, V., V. Arnold, S. G. Sutton, and L. Guan. 2002. The impact of relative information quality of e-commerce assurance seals on Internet purchasing behavior. *International Journal of Accounting Information Systems* 3 (4): 237–253. doi:10.1016/S1467-0895(02)00069-6

LaRose, R., and N. Rifon. 2007. Promoting i-safety: Effects of privacy warnings and privacy seals on risk assessment and online privacy behavior. *The Journal of Consumer Affairs* 41 (1): 127–149. doi:10.1111/j.1745-6606.2006.00071.x

Laudon, K. C. 1996. Markets and privacy. *Communications of the ACM* 39 (9): 92–104. doi:10.1145/234215.234476

Laufer, R. S., and M. Wolfe. 1977. Privacy as a concept and a social issue: A multidimensional developmental theory. *The Journal of Social Issues* 33 (3): 22–42. doi:10.1111/j.1540-4560.1977.tb01880.x

Lee, H.-H., and M. Stamp. 2008. An agent-based privacy-enhancing model. *Information Management & Computer Security* 16 (3): 305–319. doi:10.1108/09685220810893234

Lippmann, D. 2010. Half of social networkers worried about privacy: Poll. *Reuters* (July 15). Available at: http://www.reuters.com/article/idUSTRE66E41820100715

Liu, C., and K. P. Arnett. 2002. An examination of privacy policies in Fortune 500 Web sites. *Mid-American Journal of Business* 17 (1): 13–21.

Liu, C., J. T. Marchewka, J. Lu, and C.-S. Yu. 2005. Beyond concern—A privacy-trust-behavioral intention model of electronic commerce. *Information & Management* 42 (2): 289–304. doi:10.1016/j.im.2004.01.003

Lwin, M. O., and J. D. Williams. 2003. A model integrating the multidimensional developmental theory of privacy and theory of planned behavior to examine fabrication of information online. *Marketing Letters* 14 (4): 257–272. doi:10.1023/B:MARK.0000012471.31858.e5

Macavinta, C. 1999. RealNetworks faced with second privacy suit. *CNET* (November 10). Available at: http://news.cnet.com/2100-1001-232766.html

Meinert, D. B., D. K. Peterson, J. R. Criswell, and M. D. Crossland. 2006. Privacy policy statements and consumer willingness to provide personal information. *Journal of Electronic Commerce in Organizations* 4 (1): 1–17.

Milberg, S. J., S. J. Burke, H. J. Smith, and E. A. Kallman. 1995. Values, personal information privacy, and regulatory approaches. *Communications of the ACM* 38 (12): 65–74. doi:10.1145/219663.219683

Milberg, S. J., H. J. Smith, and S. J. Burke. 2000. Information privacy: Corporate management and national regulation. *Organization Science* 11 (1): 35–57. doi:10.1287/orsc.11.1.35.12567

Milne, G. R., and M.-E. Boza. 1999. Trust and concern in consumers' perceptions of marketing information management practices. *Journal of Interactive Marketing* 13 (1): 5–24. doi:10.1002/(SICI)1520-6653(199924)13:1<5::AID-DIR2>3.0.CO;2-9

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., and M. J. Culnan. 2004. Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. *Journal of Interactive Marketing* 18 (3): 15–29. doi:10.1002/dir.20009

Milne, G. R., M. J. Culnan, and H. Greene. 2006. A longitudinal assessment of online privacy notice readability. *Journal of Public Policy & Marketing* 25 (2): 238–249. doi:10.1509/jppm.25.2.238

Milne, G. R., and A. J. Rohm. 2000. Consumer privacy and name removal across direct marketing channels: Exploring opt-in and opt-out alternatives. *Journal of Public Policy & Marketing* 19 (2): 238–249. doi:10.1509/jppm.19.2.238.17136

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

Moores, T. T. 2005. Do consumers understand the role of privacy seals in e-commerce? *Communications of the ACM* 48 (3): 86–91. doi:10.1145/1047671.1047674

National Conference of State Legislatures (NCSL). 2009. *State Laws Related to Internet Privacy*. Washington, D.C.: NCSL. Available at: http://www.ncsl.org/default.aspx?tabid=13463

Nikitkov, A. 2006. Information assurance seals: How they impact consumer purchasing behavior. *Journal of Information Systems* 20 (1): 1–17. doi:10.2308/jis.2006.20.1.1

O'Neil, D. 2001. Analysis of Internet users' level of online privacy concerns. *Social Science Computer Review* 19 (1): 17–31. doi:10.1177/089443930101900103

Oppliger, R. 2005. Privacy-enhancing technologies for the World Wide Web. *Computer Communications* 28 (16): 1791–1797. doi:10.1016/j.comcom.2005.02.003

Palmer, J. W., J. P. Bailey, and S. Faraj. 2000. The role of intermediaries in the development of trust on the WWW: The use and prominence of trusted third parties and privacy statements. *Journal of Computer-Mediated Communication* 5 (3).

Papacharissi, Z., and J. Fernback. 2005. Online privacy and consumer protection: An analysis of portal privacy statements. *Journal of Broadcasting & Electronic Media* 49 (3): 259–281. doi:10.1207/s15506878jobem4903_1

Peltier, J. W., G. R. Milne, and J. E. Phelps. 2009. Information privacy research: Framework for integrating multiple publics, information channels, and responses. *Journal of Interactive Marketing* 23 (2): 191–205. doi:10.1016/j.intmar.2009.02.007

Peslak, A. R. 2005. An ethical exploration of privacy and radio frequency identification. *Journal of Business Ethics* 59 (4): 327–345. doi:10.1007/s10551-005-2928-8

Petty, R. D. 2000. Marketing without consent: Consumer choice and costs, privacy, and public policy. *Journal of Public Policy & Marketing* 19 (1): 42–53. doi:10.1509/jppm.19.1.42.16940

Phelps, J., G. Nowak, and E. Ferrell. 2000. Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy & Marketing* 19 (1): 27–41. doi:10.1509/jppm.19.1.27.16941

Pollach, I. 2007. What's wrong with online privacy policies? *Communications of the ACM* 50 (9): 103–108. doi:10.1145/1284621.1284627

Proctor, R. W., M. A. Ali, and K.-P. L. Vu. 2008. Examining usability of web privacy policies. *International Journal of Human-Computer Interaction* 24 (3): 307–328. doi:10.1080/10447310801937999

Prosch, M. 2008. Protecting personal information using Generally Accepted Privacy Principles (GAPP) and Continuous Control Monitoring to enhance corporate governance. *International Journal of Disclosure and Governance* 5 (2): 153–166. doi:10.1057/jdg.2008.7

Provos, N., and P. Honeyman. 2003. Hide and seek: An introduction to steganography. *IEEE Security & Privacy* 1 (3): 32–44. doi:10.1109/MSECP.2003.1203220

Public Company Accounting Oversight Board (PCAOB). 2004. *An Audit of Internal Control over Financial Reporting Performed in Conjunction with an Audit of Financial Statements*. Auditing Standard No. 2. New York, NY: PCAOB. Available at: http://pcaobus.org

Public Company Accounting Oversight Board (PCAOB). 2007. *An Audit of Internal Control over Financial Reporting That is Integrated with an Audit of Financial Statements*. Auditing Standard No. 5. New York, NY: PCAOB. Available at: http://pcaobus.org

Ranganathan, C., and S. Ganapathy. 2002. Key dimensions of business-to-consumer Web sites. *Information & Management* 39 (6): 457–465. doi:10.1016/S0378-7206(01)00112-4

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

Reay, I., S. Dick, and J. Miller. 2009a. An analysis of privacy signals on the World Wide Web: Past, present and future. *Information Sciences* 179 (8): 1102–1115. doi:10.1016/j.ins.2008.12.012

Reay, I., S. Dick, and J. Miller. 2009b. A large-scale empirical study of P3P privacy policies: Stated actions vs. legal obligations. *ACM Transactions on the Web* 3 (2): 1–34. doi:10.1145/1513876.1513878

Reay, I., P. Beatty, S. Dick, and J. Miller. 2007. A survey and analysis of the P3P protocol's agents, adoption, maintenance, and future. *IEEE Transactions on Dependable and Secure Computing* 4 (2): 151–164. doi:10.1109/TDSC.2007.1004

Rendleman, J. 2001. Customer data means money. *InformationWeek* (August 20). Available at: http://www.informationweek.com/news/showArticle.jhtml?articleID=6506304

Rezgui, A., A. Bouguettaya, and M. Y. Eltoweissy. 2003. Privacy on the web: Facts, challenges, and solutions. *IEEE Security & Privacy* 1 (6): 40–49.

Rice, R. 1986. Privacy, freedom and public-key cryptography. *Information Age* 8 (4): 208–214.

Sarathy, R., and C. J. Robertson. 2003. Strategic and ethical considerations in managing digital privacy. *Journal of Business Ethics* 46 (2): 111–126. doi:10.1023/A:1025001627419

Schwaig, K. S., G. C. Kane, and V. C. Storey. 2005. Privacy, fair information practices and the Fortune 500: The virtual reality of compliance. *ACM SIGMIS Database* 36 (1): 49–63. doi:10.1145/1047070.1047075

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

Seničar, V., B. Jerman-Blažič, and T. Klobučar. 2003. Privacy-enhancing technologies—Approaches and development. *Computer Standards & Interfaces* 25 (2): 147–158. doi:10.1016/S0920-5489(03)00003-5

Shankar, V., G. L. Urban, and F. Sultan. 2002. Online trust: A stakeholder perspective, concepts, implications, and future directions. *The Journal of Strategic Information Systems* 11 (3–4): 325–344. doi:10.1016/S0963-8687(02)00022-7

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

Sheehan, K. B. 1999. An investigation of gender differences in online privacy concerns and resultant behaviors. *Journal of Interactive Marketing* 13 (4): 24–38. doi:10.1002/(SICI)1520-6653(199923)13:4<24::AID-DIR3>3.0.CO;2-O

Sheehan, K. B. 2002. Toward a typology of Internet users and online privacy concerns. *The Information Society* 18 (1): 21–32. doi:10.1080/01972240252818207

Sheehan, K. B., and M. G. Hoy. 1999. Flaming, complaining, abstaining: How online users respond to privacy concerns. *Journal of Advertising* 28 (3): 37–51.

Sivasailam, N., D. J. Kim, and H. R. Rao. 2002. What companies are(n't) doing about website assurance. *IT Professional* 4 (3): 33–40. doi:10.1109/MITP.2002.1008535

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

Smith, R., and J. Shao. 2007. Privacy and e-commerce: A consumer-centric perspective. *Electronic Commerce Research* 7 (2): 89–116. doi:10.1007/s10660-007-9002-9

Steel, E., and J. Scheck. 2010. Smartphone trackers raise privacy worries. *Wall Street Journal* (June 14). Available at: http://online.wsj.com/article/SB10001424052748704067504575304643134531922.html

Steel, E., and J. E. Vascellaro. 2010. Facebook, MySpace confront privacy loophole. *Wall Street Journal* (May 21). Available at: http://online.wsj.com/article/SB10001424052748704513104575256701215465596.html

Stone, D. L., and E. F. Stone. 1990. Privacy in organizations: Theoretical issues, research findings, and protection mechanisms. *Research in Personnel and Human Resources Management* 8: 349–411.

Swaminathan, V., E. Lepkowska-White, and B. P. Rao. 1999. Browsers or buyers in cyberspace? An investigation of factors influencing electronic exchange. *Journal of Computer-Mediated Communication* 5 (2).

Tuna, C. 2010. Slow-going for web-privacy software. *Wall Street Journal* (September 8). Available at: http://online.wsj.com/article/SB10001424052748703946504575469621089587394.html

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.S. Census Bureau. 2009. *E-Stats*. Washington, D.C.: U.S. Census Bureau. Available at: http://www.census.gov/econ/estats/2008/2008reportfinal.pdf

Vail, M. W., J. B. Earp, and A. I. Anton. 2008. An empirical study of consumer perceptions and comprehension of Web site privacy policies. *IEEE Transactions on Engineering Management* 55 (3): 442–454. doi:10.1109/TEM.2008.922634

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

Weise, J. 2001. *Public Key Infrastructure Overview*. Palo Alto, CA: Sun Microsystems, Inc. Available at: http://www.sun.com/blueprints/0801/publickey.pdf.

Westin, A. F. 1967. *Privacy and Freedom*. 1st edition. New York, NY: Atheneum.

Westin, A. F. 2003. Social and political dimensions of privacy. *The Journal of Social Issues* 59 (2): 431–453. doi:10.1111/1540-4560.00072

Zogby International. 2007. *Zogby Poll: Most Americans Worry about Identity Theft*. Utica, NY: Zogby International. Available at: http://www.zogby.com/NEWS/ReadNews.dbm?ID=1275