Journal of the Association for Information Systems

IS RESEARCH ARTICLE

Theoretical Explanations for Firms' Information Privacy Behaviors*

Kathleen E. Greenaway
Queen's School of Business
Queen's University
kgreenaway@business.queensu.ca

Yolande E. Chan
Queen's School of Business
Queen's University
ychan@business.queensu.ca

Abstract

Information privacy is an important information management issue that is increasingly challenging managers and policy makers. While many studies have investigated information privacy as an individual, sectoral, or national level phenomenon, there is a gap in our understanding of organizational approaches to developing and implementing policies and programs to manage customer information privacy. Information systems research lacks theory to explain firm level information privacy behaviors. This article argues for an expanded repertoire of theories to be applied to investigating information privacy, especially the role that the pursuit of competitive necessity versus competitive advantage plays in explaining organizational level behavior. The authors outline how the Institutional Approach (IA) and the Resource-Based View (RBV) of the firm offer compelling theoretical explanations for firms' behaviors and should be applied to privacy research within the information systems area.

Keywords: privacy, information privacy, institutional theory, resource-based view

* Sirkka Jarvenpaa was the accepting senior editor. Mary Culnan and Jeff Smith were reviewers for this paper.

Introduction

Information privacy[1] is an information management issue that increasingly is of importance to managers and policy makers [Culnan and Armstrong, 1999; Davison et al., 2003; Mason, 1986; Milberg et al., 2000; Smith, 1993]. As organizations invest in interconnected information and communications technologies that provide the means to capture, store, and process vast amounts of data quickly and efficiently, the privacy implications of these investments for customers, employees, organizations, industries, and society grow in significance. However, studies on privacy appear not to be keeping pace with the growing interest in privacy [Davison et al., 2003]. There is a limited amount of organizational level research in this area.

Research examining information privacy behaviors as an organizational phenomenon is underrepresented in the privacy literature, which is dominated by consumer [e.g., Culnan, 1993; Culnan and Armstrong, 1999; Smith et al., 1996; Stewart and Segars, 2002] and sectoral/national studies [e.g., Culnan, 1999a, 1999b; Earp et al., 2002; FTC, 1998, 2000]. In addition, theory is needed to assist in understanding similarities and differences in information privacy approaches among firms [Milne and Culnan, 2002]. The sectoral/national studies demonstrate that information privacy policies vary among firms, but do not explain why. Information systems researchers have used a limited repertoire of theories to explain organizational information privacy actions. We argue that the Institutional Approach (IA) and the Resource-Based View (RBV) offer powerful theoretical explanations for firms' behaviors, and should also be applied to information privacy research.

The purpose of this article is to address the organizational-level gap in information privacy research. We argue that a single theory cannot explain the range of behaviors. Instead, we examine the potential contributions of the IA and RBV paradigms. We contend that the IA paradigm explains the behavior of firms that view information privacy in terms of competitive necessity. However, the RBV paradigm is useful for exploring the reasons for the behavior of firms seeking to advance information privacy programs in pursuit of competitive advantage.

Definitions and Concepts

We provide a brief review of key information privacy definitions and concepts to assist readers. *Information Privacy* is defined as "*the ability of the individual to personally control information about oneself*" [Stone et al., 1983:460 based on Westin, 1967]. We further distinguish between customer information privacy (CIP) and employee information privacy (EIP) as distinct concepts. (We acknowledge the importance of employee privacy as an area for ongoing research. However, our concern in this article is with the privacy of customer information.) We define *Customer Information Privacy* as *the ability of the customer to control the collection, use, reuse and disposal of his personally identifiable information*

We use the term *Organizational Privacy Behaviors* to define *how firms treat their customers' personally identifiable information*. Typically, business researchers have defined

[1] This article focuses on issues of *information* privacy that arise primarily as a consequence of commercial transactions. We acknowledge that issues concerning "privacy of the body" [Clarke, 1999] such as the use of biometric identification systems are of increasing concern and merit significant research attention. However, these concerns are beyond the scope of this paper.

organizational privacy behaviors as fair information practices (FIP) [Bennett and Grant, 1999; Culnan and Bies, 1999; Mason et al., 2000.] Fair information practices in the U.S. include notice that information is being gathered, choice with regard to information tracking and use, access to personal information records, and security for these records [Culnan, 1993; Milne, 2000]. FIP form the core of privacy regulation in jurisdictions such as the European Community and Canada (which operate with all encompassing data protection regimes) as well as act as guiding principles in jurisdictions such as the United States (that offer a combination of sectoral and self regulation).[2] For example, FIP form the basis for the provisions of both the BBB Online and TRUSTe self-regulatory webseal programs. In Appendix A, we provide specific examples of privacy behaviors for each of the basic four principles we defined above.

An *information privacy program* is the term we use to describe *the collection of policies and procedures that firms implement with respect to the collection, use, reuse, security, storage, and disposal of their customers' personally identifiable information.* A program is thus more than a collection of behaviors, but also includes the organizational reasons for the behaviors. These "organizational reasons" are one way to think about the theoretical explanations for firms' information privacy behaviors.

Overview of Article

The article is organized as follows. First, we motivate this article with a brief overview of the information privacy research literature and demonstrate the empirical and theoretical gaps that exist at the organizational level of analysis. Next, we consider two theories, the Institutional Approach and the Resource-Based View,[3] and discuss why these particular theories are useful for examining firm-level differences in privacy behaviors that affect customer information. We present a detailed consideration of how these theories offer different and compelling explanations for firms' information privacy behaviors. We conclude with a discussion of research opportunities posed by these different theories.

[2] Different jurisdictions delineate different sets of fair information principles. For example, the first set of FIP were articulated by the U.S. Department of Health, Education and Welfare in 1972 and include four principles (notice, choice, access and security). The Organization for Economic Cooperation and Development (OECD) expanded this concept to eight principles (limitation, data quality, purpose, use, security, openness, participation and accountability). Canada's federal statute, the Protection of Information Privacy and Electronic Documents Act (PIPEDA), articulates 10 inter-related principles (accountability; identifying purposes; consent; limiting collection; limiting use, disclosure and retention; accuracy; safeguards; openness; individual access; and challenging compliance.) Regardless of how the fair information principles are specifically articulated, there is a "basic and common understanding of how the responsible organization should treat the personal data that it collects, stores and processes … The historical and cultural sources of concerns about privacy may differ … but the definition of what it means to be 'responsible' has increasingly converged" [Bennett and Grant, 1999:6].

[3] We do not provide a detailed exposition of the different facets of these paradigms. Rather, we select those elements of most salience to a discussion of organizational level information privacy behaviors. We refer interested readers to *inter alia* Orlikowski and Barley [2001], Robey and Boudreau [1999], and Tingling and Parent [2002] for further discussion of the Institutional Approach. Likewise, readers are directed to Mata et al. [1995], Jarvenpaa and Leidner [1998] and Wade and Hulland [2004] for further discussion of the Resource Based View of the firm.

Background and Motivation

A review of the privacy research published in leading outlets for IS research such as *Communications of the ACM*, *Information Systems Research, Journal of the AIS, Journal of Management Information Systems, Management Information Systems Quarterly*, and *Organization Science* shows that information privacy research is arguably most easily distinguished by level of analysis. For our purposes, we distinguish three levels of analysis – individual (consumer/employee), organizational, and sectoral/national.

Individual-Level Research

Much of the contemporary privacy research focuses on information privacy as a multidimensional individual level construct [Smith et al., 1996]. Studies have addressed the issues of consumer attitudes about privacy generally [Culnan, 1993; Culnan and Armstrong, 1999; Rohm and Milne, 2004; Tam et al., 2002]; consumer responses to organizations' privacy-violating behaviors [Smith et al., 1996; Stewart and Segars, 2002]; and consumer responses to incentives when choosing between withholding and sharing personal information [Dinev and Hart, 2003; Hann et al., 2002; Tam et al., 2002]. Culnan and Bies [1999] propose that consumers invoke a "privacy calculus" to weigh the potential risks and benefits of providing personal information in exchange for economic or social gains. At the same time, Dhillon et al. [2002] argue that individuals make "value focused" privacy-based assessments about the firms with which they do business.

Marketing research also informs our understanding of consumer-level privacy issues [Jones, 1991; Milne, 2000] especially in online environments [e.g., Milne et al., 2004; Milne and Rohm, 2000; Miyazaki and Fernandez, 2000; Sultan and Mooraj, 2001].
A persistent theme across both the IS and marketing-based privacy literatures is the important relationship between privacy and trust manifested in consumers' willingness to disclose personal information [e.g., Culnan, 2000; Gefen et al., 2003; Hoffman et al., 1999; McKnight et al., 2002; Milne and Boza, 1999; Schoenbachler and Gordon, 2002; Sheehan and Hoy, 2000].

Collectively, these studies provide important insights into consumer attitudes and behaviors. However, they do not explain what motivates the information privacy protecting or violating behaviors of the *organizations* with which consumers conduct business.

Sectoral/National-Level Research

A second group of studies examines information privacy policies posted to firms' websites across industry sectors and jurisdictions. This research particularly informs our understanding of how well organizations meet the basic privacy principles articulated as fair information practices (FIP) and previously described. Studies based in the U.S. have examined the extent to which FIP are present in the privacy policies posted on the websites of consumer-oriented firms [FTC, 1998, 2000]; the business-to-business and business-to-consumer websites of high technology firms [Ryker et al., 2002]; and the most heavily trafficked and popular sites on the Internet [Culnan, 1999a, 1999b]. A recent Canadian study examined privacy policies as they related to the then-proposed federal privacy legislation [Geist and Van Loon, 2000].

While these studies have provided important information about privacy trends across industries and countries, their usefulness for the purpose of this review is limited. First,

counts of the frequency of policies do not *explain* individual firm behavior. Second, these studies tend to emphasize the Internet-based commercial experience and overlook the totality of ways in which organizations track their customers across a range of commercial exchanges [Culnan and Bies, 1999; Smith, 2001]. Third, with few exceptions, these studies treat all firms equally, as simply announcers of privacy policies rather than implementers of privacy strategies. We echo Milne and Culnan's [2002] contention that these studies provide limited insight into the complexity of the information privacy phenomenon within organizations.

Organizational-Level Research

Three broad themes are prevalent in the organizational-level privacy research: information privacy as organizational liability, information privacy as an organizational decision outcome, and information privacy as an organizational ethical imperative. (We acknowledge that these three themes are not mutually exclusive, but we treat them as such for the purposes of clarity in the following discussion.) Within these three themes, information privacy is often treated as an organizational concern within broader contexts such as global IT management [Ives and Jarvenpaa, 1991] or corporate social responsibility [Straub and Collins, 1990]. Most researchers assert a narrow perspective of privacy as a source of legal liability [Bordoloi et al., 1996] or having to do more with systems security than with privacy actions [Srivatava and Mock, 2000]. Few authors have examined information privacy as a senior management issue requiring organizational action [Cadogan, 2001; Earp et al., 2002; Smith, 1990] despite calls for such investigations [e.g., Chan, 2003; Milne, 2000].

Information privacy has also been characterized as an organizational ethical imperative [e.g., Laudon, 1995; Mason, 1986], but the ethical theories to support these assertions are frequently underdeveloped. Examples of IS privacy research using ethical theory include Smith [1993] (seven case studies of the information privacy actions of U.S. financial firms) and Culnan and Smith [1995] (an examination of the ethics and privacy implications of Lotus: Marketplace). Marketing researchers have also studied organizational-level privacy issues from an ethical perspective [e.g. Caudill and Murphy, 2000; Foxman and Kilcoyne, 1993; Hoffman et al., 1999].

Despite apparent researcher interest in the issue of privacy in organizations, there is limited theory to guide us in understanding organizational information privacy behaviors. Especially lacking are explanations for why there are similarities and differences in privacy behaviors among firms within the same industry. Our contribution is to demonstrate that it is insufficient to rely on a single paradigm to explain all organizational-level privacy behaviors across all firms. This article argues for an expanded repertoire of theories to provide rich and nuanced explanations of firms' information privacy behaviors. In the next section, we introduce the Institutional Approach (IA) and the Resource-Based View of the firm (RBV) and demonstrate how they offer important insights into the reasons for information privacy behaviors at the organizational level of analysis.

Theoretical Explanations For Information Privacy Behaviors

Both the Institutional Approach and the Resource-Based View of the firm are paradigms [Jarvenpaa and Leidner, 1998:344] that offer broad bases from which to assess organizational operations and compare practices among firms and across industries. However, these theories offer fundamentally different explanations for organizations' privacy

behaviors.[4] If the Institutional Approach provides a means for considering the activities of the firm from the "outside-in," the Resource-Based View takes an "inside-out" perspective [Srivastava et al., 2001]. In considering privacy behaviors, institutional theory suggests that firms are constrained by external forces while the RBV argues that firms choose how they will treat their customer information as an organizational resource. In this section, we briefly describe each theory. Then we apply the theories to a consideration of firms' information privacy behaviors. We present high level propositions to guide research and include hypothetical scenarios to illustrate key points.

The Institutional Approach (IA)

Institutional theory is part of a stream of research that examines relationships between organizations and their environments. This approach considers the effects on organizations of "broad social and historical forces ranging from explicit laws to implicit cultural understandings" [Orlikowski and Barley, 2001:153]. The institutional tradition [Hannan and Freeman, 1989] sees organizations not solely as rational, efficiency-seeking entities, but also as social, political, and cultural ones [Scott, 1987]. In contrast to economic models of organizational behavior, institutional theory locates rationality within firms' external environments [DiMaggio and Powell, 1983; Pfeffer, 1997; Tolbert and Zucker, 1996]. The rationality is one of conformance to social norms in a search for legitimacy rather than conformance to a rent-seeking model of economic behavior. The Institutional Approach argues that organizational survival may depend more on conforming to the norms of external groups and less on succeeding as efficient producers of goods and services [DiMaggio and Powell, 1983].

Institutional theory has been identified as a potential alternative research perspective for IS researchers [Ang and Straub, 1998; Deveraj and Kohli, 2000; Kumar et al., 1998; Orlikowski and Barley, 2001]. Robey and Boudreau [1999:177] suggest that the institutional approach is particularly well suited to addressing the "question of information technology and organizational change… [including] conflicts among normative pressures such as efficiency, *rights to privacy*, and autonomy, and deeply embedded notions of bureaucratic and hierarchical structure" [our emphasis].

We argue that most organizations' information privacy behaviors are primarily responses to external pressures or "institutional" forces. That is, we believe that most firms do not choose to differentiate themselves competitively through their information privacy programs. We have identified four theoretical elements of particular interest to this discussion: organizational goals, the sources for pressures to act, the ability to act, and response strategies. In this section we outline the relevant attributes of the institutional theory and apply them to information privacy. We offer propositions to guide research. Table 1 summarizes our discussion of these elements.

[4] We refer to both the Institutional Approach and Resource-Based View as theories for ease of discussion. However, Jarvenpaa and Leidner [1998] argue that RBV is, technically, a paradigm, not a theory. We argue that a similar characterization can be applied to Institutional theory.

Table 1. The Institutional Approach to Explaining Information Privacy Behaviors

Element	Explanation	Application to information privacy in organizations	
		Acquiescent Approach	**Proactive Approach**
Organizational goals	Survival through the search for legitimacy	• Pragmatic • Managerial	• Social • Technical
Ability and willingness to respond to pressure	Influence of social network	Embeddedness	Agency
Responses to pressures	Compliance with established norms	Imitation of peer organizations	Impression management to yield "constrained leadership"

IA: Organizational Goals

The institutional approach assumes that the overriding organizational goal is to achieve legitimacy as a means of ensuring survival. *Legitimacy* is defined as:

> A generalized perception or assumption that the actions of an entity are desirable, proper or appropriate within some socially constructed system of norms, values, beliefs and definitions [Suchman, 1995:574].

The Institutional Approach literature identifies several forms of legitimacy. *Pragmatic legitimacy* refers to short term, self-interested perceptions by external audiences (such as customers) that indicate a transactions-oriented focus on legitimacy. In contrast, *social legitimacy* [Handelman and Arnold, 1999] or *moral legitimacy* [Suchman, 1995] refers to perceptions grounded in a longer term, pro-social logic that considers actions in light of their impact on community and society. Others distinguish between managerial and technical legitimacy. *Managerial legitimacy* involves "normative support for organizational mechanisms" while *technical legitimacy* is concerned with the core activities of the firm [Ruef and Scott, 1998: 883]. We characterize managerial legitimacy as incorporating key back-office functions such as human resources, accounting, finance, and IS/IT. In contrast, we suggest that technical legitimacy involves activities most concerned with the firm's direct economic activities, such as manufacturing, marketing and sales.[5]

Organizations choose, however consciously or not, the type of legitimacy they seek to obtain through their privacy practices. Within an institutional explanation for information privacy behaviors, some organizations are more concerned with seeking a combination of pragmatic and managerial forms of legitimacy, while others are more interested in pursuing a combination of social and technical legitimacy. Pragmatic legitimacy in information privacy

[5] These latter definitions are adapted from Ruef and Scott [1998:883]. Their study focused on hospitals which have typically well-defined managerial (non-medical) and technical (medical) functions. The adaptation we have made approximates Porter's [1985] value chain distinction between a firm's primary and support activities.

terms involves conforming to the legal environment (basic legal compliance) by making the minimum changes to organizational processes necessary to avoid potential legal problems (such as increasing IT security). Managers would make these changes in the firm's back office operations to demonstrate compliance, while attempting to mitigate the impact on the firm's key revenue generating activities.

Other organizations with a greater concern for achieving social legitimacy (by appealing to customer concerns about trust) are more likely to appeal to perceived norms about information privacy and to emphasize changes to their technical cores (such as how marketing campaigns are conducted) to substantiate these claims.

To illustrate these distinctions, let us think about two firms in the retail banking industry. Assume that both wish to respond to perceived growth in demand for customer information privacy. Both communicate to their customers that they are engaged in privacy programs. However, Bank A states that the purpose of the privacy program is to comply with the law (pragmatic legitimacy) and that polices and procedures are in place across the bank (managerial legitimacy). Little specific detail is provided. The language employed in the "minimal privacy behavior" column of Appendix A reflects Bank A's approach.

In contrast, consider Bank B's statement that its customers have an inherent right to privacy as well as to appropriate conduct (by their financial institution). The purpose of the privacy program, therefore, is to meet the bank's legal and ethical obligations. These statements are indicative of the pursuit of social legitimacy. Bank B, in contrast to Bank A, provides considerable detail about information collection, use, security, and other activities that may impinge upon or support customer information privacy. For example, the firm has developed policies and procedures to: protect personal information, receive and respond to complaints and inquiries, train staff regarding the policies and procedures, and communicate the policies and procedures to its customers. Furthermore, the bank has instituted internal policies that affect the collection of data from customers. All new data-driven initiatives (such as a marketing program) are vetted through an internal committee (including marketing, IT, security, and privacy personnel) and must be signed off by both the functional head (in this case a senior marketing executive) as well as the senior privacy executive. These actions suggest that Bank B is pursuing technical legitimacy through its customer information privacy program. The "enhanced privacy behavior" column of Appendix A is illustrative of Bank B's approach.

In summary, we argue that firms pursue different forms of organizational legitimacy through their choice of information privacy behaviors.

IA: Organizational Ability to Respond

Organizational ability to respond to external pressures depends on the degree to which organizations are embedded within their social networks, coupled with their ability and willingness to exercise agency. *Social embeddedness* refers to the extent to which organizations are linked within larger networks, both economic and social [Dacin et al., 1999]. These networks, comprised of other organizations (including competitors, regulators, customers, and similar stakeholders), enable and constrain organizational activity [Orlikowski and Barley, 2001]. However, organizations are not passive victims of their environments [Pfeffer, 1997] because they can exercise agency. *Agency* is the extent to which organizations are able and willing to operate beyond the norms and restrictions contained

within their networks. Organizations can choose, albeit to greater or lesser extents, whether or not to engage their environments and respond to pressures [Scott, 2001].

We argue that firms that perceive themselves to be strongly embedded in networks (such as industry associations) will either be more willing to conform to what the network establishes as appropriate information privacy behaviors, or less willing to extend themselves in an independent search for alternatives.

On the other hand, we contend that some other firms, while still operating within their overall network, will exercise agency to develop different information privacy policies (in comparison with the network's policies) but not to the extent that this action would undermine other important goals such as legitimacy. These firms will perceive that information privacy is a source for apparent but not substantive differentiation.

Again, for the sake of illustration, let us return to Banks A and B. Let us assume that both banks are members of the same national industry association. This association has a model customer information privacy code, which was developed when the public's concern for information privacy was gaining government attention. In our scenario, Bank A did not participate in the discussions to develop the model code. Rather it adopted the code when it became apparent that the majority of its peers were doing so. As a further indication of its embeddedness, Bank A essentially "cut and pasted" the model code onto its website and declared itself privacy compliant with its industry's privacy standards.

In contrast, Bank B exercised agency. The bank had campaigned within the industry association to create the awareness of the need for a model code. It was a principle architect of the final product. Bank B's privacy policies derive from the model code, but the bank has tailored its approach to meet the specific needs and expectations of its customers. Bank B developed the approach after an extensive independent assessment of the available privacy "best practices" within the global banking industry. Bank B provides a summary of its privacy policies on its home page and provides a link to a repository of privacy information. Included in the repository are a PDF of its corporate privacy policy document, privacy FAQs, and an email contact link to the privacy office. Customer service representatives in the bank's call center have been trained to respond to privacy questions generated through the online banking SMS capability and the telephone banking system.

IA: Response Strategies

Oliver [1991] combined institutional and resource-dependence theories[6] to develop a repertoire of strategies from which organizations choose to respond to institutional pressures. These responses are based on how organizations manage their "technical activities" (the activities used to derive economic returns) as opposed to the institutional environment [Meyer and Rowan, 1977].

[6] Resource-dependence theory is not the same as the resource-based view of the firm. Resource-dependence theory [Pfeffer and Salancik, 1978] argues that organizations exist within and depend upon uncertain external environments for their survival. The "dependence" involves needing economic and other resources from the external environment in order to continue operating. Power relationships are an important aspect of the theory such that "organizations tend to comply with the demands of those interests in their environment which have relatively more power" [Pfeffer, 1987:26-7 as quoted in Pfeffer, 1997:63].

One of Oliver's strategies, acquiescence (conforming through imitation of model organizations), is particularly associated with the pursuit of organizational legitimacy [Scott, 2001]. Tingling and Parent [2002] demonstrated that "peer influence" could override managers' rationally-based, internally produced assessments of technology alternatives. Managers selected less appropriate or inferior technologies when informed that competitors had chosen a particular technology. Another study found that firms' decisions to outsource their IS functions were influenced by whether the pressure came from federal regulators or competitive peers. The "acquiescence" strategy was most likely to be invoked in the face of regulatory pressure in order for firms to achieve "certainty, stability and predictability" in their environments [Ang and Cummings,1997:249]. A broader range of responses distinguished competitive pressures.

An alternative institutional response is offered by Cashore and Vertinsky [2000:4], in which firms are "more advanced than societal pressure, leading the way with innovation and proaction." They argue that firms can seek to provide leadership and innovation in their operations while, at the same time, conforming to institutional norms. Their case study demonstrated that this category of response appeared to explain the actions of firms who sought industry leadership through their corporate environmental (so called "green") initiatives.

Overall, we argue that the majority of firms are likely to adopt an acquiescence strategy in the face of institutional pressures to address information privacy. However, even within this strategy, we conclude that there can be discernible differences among firms, primarily based on the rationale for the responses employed. An acquiescence strategy would be pursued for either of two (not necessarily mutually exclusive) reasons: either the firms will acquiesce for reasons of conformity to a defined legal model, or they will imitate the privacy behaviors of similar firms with minimalist privacy regimes. Their rhetoric will involve appeals to "having to do what the law requires" and "being just as good as other firms in the industry or jurisdiction."

"Proactive" firms would use organizational impression management[7] tactics [Mohamed et al., 1999] to demonstrate a difference in approach to information privacy. Pfeffer [1981:26] argued that an organization would use impression management to "define reality for its key constituents" in order to be perceived as legitimate. Recent work by Winter et al. [2003:318] showed that websites can influence customers' impressions of organizations, including perceptions of legitimacy. In the case of information privacy, we would expect proactive firms, on one hand, to employ a bounded language of leadership that would imply "good" differences in their information privacy practices. At the same time, these firms would want to avoid two problems that could be created if they were perceived to be "too different." First, appearing extreme in their information privacy behaviors could jeopardize their claims to legitimacy by appearing to be outside the norms of their industry network. Second, overplaying claims to superiority might undermine perceptions of the overall legitimacy of the industry. Neither situation would serve a proactive firm well. As a result, proactive firms must constrain their information privacy leadership to avoid undermining the industry's basic legitimacy claims.

[7] Impression management "includes attempts to control the perceptions that others form of an individual or firm by influencing the likelihood that a perceiver will make certain attributions." [Winter et al., 2003:310]

For example, Bank A does not claim privacy leadership. It argues simply that its policies conform to [an unspecified] code concerning the protection of personal information. Further, it asserts that it complies with some unspecified law in order to ensure that its customers' rights are fully respected. However, few details are provided to support these claims.

In contrast, Bank B not only references the model code but provides a link to the specific text of the code and offers explanatory notes. In addition, it references the banking industry's long tradition of confidentiality to support legitimacy claims for the industry. At the same time, Bank B demonstrates leadership through impression management tactics such as providing the name and contact information for its privacy manager, an explanation of its access processes and a form for requisitioning personal information, and links to a glossary of privacy and security terms. In its branches, the bank has placed posters in prominent positions and provided literature drawing attention to its privacy policies. A senior staff member is publicly identified as a privacy champion who acts as a resource for staff and customers with privacy questions. The head office executive with privacy responsibility makes speeches in public forums about privacy and is frequently contacted by the media to comment on privacy incidents in the news.

In summary, we offer the following high-level propositions to assist future research.

> (P1) *The behaviors of firms that do not seek to differentiate themselves using their information privacy programs can be explained using the Institutional Approach such that:*
>
> *(P1a) Firms with a compliance perspective on information privacy will adopt privacy behaviors that demonstrably conform to industry norms; OR*
>
> *(P1b) Firms with a prosocial perspective on information privacy will adopt privacy behaviors that appear to be differentiated from others but are grounded in impression management.*

The Institutional Approach offers a comprehensive way to think about information privacy behaviors in firms that view information privacy as "table stakes." These firms offer some differences at the margins in their information privacy behaviors but fundamentally do not offer anything unique. These firms prefer to tread the common ground of not appearing to be too different from their peers in an attempt to prevent information privacy from becoming a competitive issue within their referent group.

We now turn our attention to how the resource-based view of the firm can be applied to explain why certain firms have pursued different organizational responses to the pressures to implement information privacy programs.

Resource-Based View Of The Firm (Rbv)

In contrast to the "social approach" that characterizes institutional theory, the RBV is grounded in an economic tradition. This tradition argues that firms are rent-seeking entities that pursue sustainable competitive advantage through the development and deployment of firm resources. Owning or having access to resources, however, is not sufficient in and of itself to confer competitive advantage, whether sustained or temporary. The resource-based approach is premised on four *attributes of sustainability* [Barney, 1991]. These attributes

describe a resource's degree of value (*valuable* or not) and degree of idiosyncrasy (*rareness*, *imitability*, *substitutability*) [Brumagin, 1994].

The Resource-Based View has been used as a theoretical lens in information systems research particularly to explore the contribution of IT to firm performance [Wade and Hulland, 2004]. Zhang and Lado [2001] theorized that firms can cultivate IT-based "organizational competencies." Jarvenpaa and Leidner [1998] argued that firms can cultivate dynamic capabilities in anticipation of changes in their environment. We believe that the RBV emphasis on the ability of firms to select unique combinations of resources and to behave independently provides an important counterpoint to the IA emphasis on reaction, imitation, and impression management.

In contrast to the arguments laid out in the previous discussion on the Institutional Approach, we suggest that some firms' information privacy behaviors do not result from responding to externally derived "institutional" forces. Rather, these behaviors are the outcome of deliberate choices made to differentiate the firm in privacy terms [Chan, 2003; Culnan and Bies, 2003]. We argue that certain firms choose to develop their customer information resource as an important source for achieving competitive advantage, either as a customer knowledge capability or customer relationship-based capability.

In this section, we define the salient aspects of the RBV paradigm as a lens for considering information privacy behaviors (which we summarize in Table 2). We discuss how resources and capabilities can contribute to achieving sustainable competitive advantage. We also adapt a corporate resource hierarchy framework to demonstrate how this theoretical approach can be applied to information privacy orientation and suggest high-level propositions to encourage future research.

Table 2. The Resource-Based Approach to Explaining Information Privacy Behaviors

Element	Explanation	Application to information privacy in organizations	
		Information Focus	**Customer Focus**
Organizational goal	Sustainable competitive advantage	Strategic differentiation based on superior customer insight	Strategic differentiation based on superior customer trust
Resource	Customer information as a resource to support innovation and change	Support efficiency focused internal innovation	Support effectiveness focused external innovation
Process	Privacy policies and practices	Information privacy as an intellectual/knowledge management process	Information privacy as a social/relationship management process
Dynamic capability	Information privacy as a source of information and innovation	Customer knowledge capability	Customer relationship capability

RBV: Organizational Goals

The organizational goal within the resource-based paradigm involves the search for competitive advantage based on strategic differentiation [Barney, 1991]. This differentiation can be pursued through two distinct approaches to information privacy. In the first instance, firms can strive for differentiation by emphasizing the development and use of detailed customer information to deliver superior customer insight. We argue that to implement this strategy would require these firms to focus on obtaining as much detailed information as possible by whatever means. They would justify their actions based on the need for inputs to their decision models.

In the second instance, we contend that certain firms could pursue strategic differentiation by cultivating superior customer trust in either of two ways. On the one hand, these firms could simply gather less information in order to avoid alienating their customers. On the other hand, the firms could gather as much information as others, but with much greater attention to the conditions under which the information is gathered and used, the means and thoroughness of communicating their actions to their customers, and the extent to which they cultivate privacy practices to protect their customers' interests.

However, selecting an organizational goal depends largely on the definition of the resource upon which the differentiation strategy is built. This is the subject of our next section.

RBV: Resources

We identify the key resource as "customer information." However, the specific differentiation strategy to be pursued depends on how the customer information resource is characterized. The RBV literature provides several approaches to defining resources [e.g., Barney, 1991; Grant, 1991; Miller and Shamsie, 1996]. For our purposes, we combine Srivastava et al.'s [1998] approach to market-based assets and Brumagin's corporate resource hierarchy [1994] to develop a useful information privacy resource typology.

Srivastava et al. [1998] define "market-based assets"[8] as assets that result from the organization's externally-oriented activities and distinguish two types of market-based assets – intellectual and relational. *Intellectual market-based resources* are the "types of knowledge a firm possesses about the environment, such as the emerging and potential state of market conditions and the entities in it, including competitors, customers, channels, suppliers, and social and political interest groups," while *relational market-based resources* are "outcomes of the relationship between the firm and key external stakeholders, including distributors, retailers, end customers, other strategic partners, community groups, and even governmental agencies" [Srivastava et al.,1998] :5]. This distinction supports our contention that firms choose between valuing information-based resources (intellectual) and customer relationship-based resources (relational). These choices are based on the firms' different perspectives on the value of information privacy.

Brumagin [1994] theorized a hierarchy of corporate resources in which not all resources are accorded an equal role in pursuing competitive advantage.[9]

[8] Barney [1991] and Srivastava et al. [2001] use the terms assets and resources interchangeably.

[9] Brumagin's [1994:90] hierarchy included four levels of corporate resources distinguished by the extent to which they supported strategic differentiation as opposed to supporting improvements to internal processes.

Consistent with this approach to resource categorization, we view customer information as a resource "that supports learning (Innovation and Change) throughout the organization directed to better utilization of corporate assets" [Brumagin, 1994:90]. We contend that firms gather detailed customer information in order to learn something that they otherwise would not know and that this learning is applied to achieving other important goals (beyond the mere gathering of data). It is the application of the customer information resources to the achievement of these different goals that is the important consideration.

We believe that certain firms will emphasize the customer information resource as a means to support efficiency-focused, internally-oriented learning. These firms will be more concerned to gather as much customer information as possible in order to better target their marketing offerings or to more efficiently deploy their customer systems to achieve, for example, their cost minimization or profitability improvement goals. If considering privacy at all, these firms would seek to minimize its interference with the collection and processing of data.

In contrast, other firms might use the customer information resource as a means to learn about better ways to address immediate or anticipate future customer preferences. Brumagin [1994] characterizes this learning as effectiveness-focused learning that emphasizes the firm's ability to improve its adaptive capacity in the face of a changing external environment. These firms would be more interested in treating the customer information resource as a unique asset important unto itself, rather than as merely an input to other firm processes and systems. The customer information resource would be used to improve understanding of particular segment needs, develop insight into emerging trends, and provide the basis for future offerings. Privacy considerations would be extended to ensure that the information being collected is relevant, useful, and timely.

RBV: Information Privacy and Processes

We suggest that firms will have different information privacy policies according to whether they desire to emphasize the intellectual/knowledge aspect or the social/relationship aspect of their information privacy activities. Firms that emphasize the information aspect of information privacy will be more likely to implement privacy regimes that closely align with their information management regimes. For example, they will try to maximize the efficiencies they can obtain from the deployment of their customer relationship management systems. An information rule of thumb would be "if in doubt, collect it and we'll find a way to use it" as, after all, data storage costs are low.

In contrast, we would expect other firms to emphasize the customer relationship aspect of information privacy. These firms would attempt to maximize the effectiveness of their privacy processes such that, for example, only the minimum necessary information is collected. In this case, the rule of thumb would be more along the lines of "if in doubt, don't collect," reflecting two main considerations. First, this approach would help to preserve the firm's reputation and social ties with its customers. Second, this would support a disciplined approach to data collection that recognizes the use of Fair Information Principles as an effective information discipline.

For example, let us consider the different approaches taken by Banks C and D. Bank C takes the view that it will compete on the basis of having extensive, detailed customer profiles. Its approach is that more data, even data whose application is not immediately apparent,

improves decision-making. This firm asks customers for great amounts of personal information about, for example, "lifestyle" (such as recreational preferences) and "aspirations" (such as retirement goals) as a matter of routine. The collected information may not be used immediately, but the questions are built into routine transaction processes, and staff is trained to ask the questions. In addition, the firm cross references transaction data from multiple sources (such as checking and credit card accounts).The use of the information for new purposes is not disclosed to customers, and customer information is routinely sold to third parties. In this manner, Bank C pursues an efficient use of the customer information resource through internal reuse and revenue-raising from external groups.

In contrast, Bank D operates on the basis that it can limit the amount of information it collects about its customers and still provide an appropriate level of customized service. To do this, it applies the fair information principles to its information management processes and, at each step, provides privacy protection as the decision rule. For example, every piece of information collected about customers is tied to a decision that has been identified as an immediate, relevant requirement. "Nice to have" information is not collected. Customer information is deemed too valuable to the firm to be sold to third parties. In this manner, Bank D pursues an effectiveness approach to the use of customer information.

In summary, we argue that the characterization and, hence, treatment of the customer information resource underpins a firm's approach to information privacy.

RBV: Information Privacy And Capabilities

If we accept that customer information is a resource that is managed through a process that renders a capability, then we can distinguish two types of capabilities that firms may pursue in order to achieve competitive advantage. We argue that firms that view customer information as an efficiency-focused internal learning resource and that pursue information privacy as a part of an overall information management regime are firms that are pursuing a customer knowledge capability. This approach is consistent with Bhardawaj's [2000] argument that advantage can be conferred on organizations that possess the ability to track and predict changing customer preferences, especially in volatile markets.

On the other hand, firms that treat their customer information resource as an effectiveness-focused external resource, and implement processes that rank customers' information privacy concerns higher in priority than organizational information gathering, could be seen to be pursuing a customer relationship capability. This approach arguably reflects the view that firms can pursue competitive advantage through the core competence of trustworthiness [Barney and Hansen, 1994; Jarvenpaa and Leidner, 1998].

For example, building on Bank C's "efficiency" approach to the customer information resource, all of its business units have access to its comprehensive customer profiles. This means that, for example, a basic mortgage customer with a certain threshold income level is identified for further marketing and cross-selling by the bank's wealth management or investment banking units. To the extent that Bank C addresses privacy concerns, its explanations are general and refer to using the information to improve products and services. Customers who choose not to provide additional, non-transaction-specific information may be denied access to particular products or services. To the extent that Bank C offers customers any control over the use of their personal information (i.e., consent to receive additional marketing information), customers that decline to participate are categorized unfavorably, and are excluded from receiving benefits that accrue to similarly profiled

customers who have agreed to participate in marketing programs. In this manner, Bank C emphasizes the internally efficient use of its customer resource. Collecting detailed information from multiple sources and sharing it across multiple units provides it with a customer knowledge capability from which it aspires to achieve competitive advantage.

In contrast, Bank D operates with an external orientation that emphasizes its relationship with customers. Bank D explains its privacy practices whenever it needs to ask customers for information. It invites customers to participate in information-based programs (such as building comprehensive profiles for long term financial planning) and explains how different categories of information assist in developing useful profiles. It seeks permission to share information with other internal business units but does not discriminate against customers who decline. It offers specific examples about how it uses customer information internally and the circumstances under which the information would leave the firm (such as for market research purposes). The staff is trained to answer privacy enquiries and to explicitly emphasize privacy actions in their dealings with customers.[10] Customers may be provided with tools to control their information. For example, customers might have access to privacy-protecting software when engaged in online banking and other ecommerce transactions.[11] In this manner, Bank D emphasizes its approach to privacy as integral to trust building within its customer relationship capability.

We acknowledge that we have made a distinction between capabilities that do not have to be mutually exclusive. However, we believe that a case can be made for the existence of a practical hierarchy in which firms operationalize preferences for privacy-invasive information practices over their customers' information privacy concerns, and vice versa.
We offer the following high-level propositions to guide research.

> (P2): *The behaviors of firms that seek competitive advantage through the use of their customer information resource can be explained using the Resource-Based View such that:*
>
> *(P2a): Firms that emphasize customer information as an efficiency-based internally-focused learning resource will subordinate privacy concerns and emphasize information collection and reuse behaviors;* OR
>
> (*P2b*)*: Firms that emphasize customer information as an effectiveness based, externally-focused learning resource will accord customer privacy concerns priority over their information gathering opportunities.*

We contend that the information privacy activities of certain firms can be explained using the Resource-Based View. These firms pursue competitive advantage through the development of capabilities that reveal an organizational preference for competing on the basis of differentiation through a customer knowledge capability or a customer relationship capability. What distinguishes these firms from those discussed in the section on the Institutional Approach is that RBV firms view privacy as a competitive issue.

We summarize our theoretical explanations for firms' information privacy behaviors in Table 3.

[10] For example, see Cocheo [2003].
[11] For example, see Middlemiss [2001].

Table 3. Summary of Theoretical Explanations for Information Privacy Behaviors

Theory / Theory attributes	Institutional Approach		Resource-based View	
	Acquiescence strategy	**Proactive strategy**	**Customer knowledge capability**	**Customer relationship capability**
Organizational goal argued by theory base	Survival		Competitive advantage	
Information privacy role in achieving organizational goal	Source for pragmatic legitimacy	Source for social legitimacy	Support for differentiation through intellectual resource	Support for differentiation through social resource
Focus of firm information privacy activities	Internal	External	Internal	External
Information privacy as a mechanism for achieving the goal	Isomorphism within industry privacy practice	Impression management to suggest differentiation	Evolution of organizational information management processes	Evolution of organizational privacy management processes

We have proposed that firms' behaviors can be partly explained by the role that information privacy plays in either securing survival through legitimacy (Institutional Approach) or in pursuing competitive advantage through the use of the customer information resource (RBV). The Institutional Approach paradigm offers two views of firms that have limited interest in differentiating themselves through information privacy. Firms with a lesser concern for or commitment to information privacy would be more likely to exhibit an acquiescent strategy, be internally focused, and reactively imitate industry privacy practices. Firms with a greater concern for appearing to respond to pressures to adopt information privacy programs would be more likely to adopt a proactive strategy, be externally focused, and employ impression management techniques to suggest a level of privacy differentiation from competitors that is more style than substance. However, this differentiation would appear as a form of leadership that remains essentially constrained within a concern to be seen to not be out of step with institutional privacy norms.

In contrast, RBV would help to explain the behavior of firms that seek to use the customer information resource as a vehicle for achieving competitive advantage. Again, we argue for two different responses that are consistent with the attributes of the RBV theory. Some firms will seek to differentiate by treating customer information as an input to internally-focused information management regimes to achieve superior customer insight. These firms would downplay information privacy by emphasizing the importance of customer information for organizational decision-making. We have labeled this approach "Customer Knowledge Capability." However, we believe that other firms' actions can be characterized by

differentiation on the basis of an externally-focused and proactive treatment of customer information privacy as an important aspect of managing a key social relationship. We have characterized this approach as the "Customer Relationship Capability."

We now turn to the important question of how our discussion of organizational-level customer information privacy can shape an information systems research agenda.

Research Opportunities

Our review of the privacy literature has led us to conclude that there is likely not one best explanation for firms' information privacy behaviors. Rather, we expect that there are different theoretically sound explanations for differences in information privacy behaviors within and across industries.

We have argued that institutional theory and the resource-based view of the firm offer compelling explanations for different firms' information privacy behaviors. We believe that these two theoretical approaches provide fresh insights into organizational-level information privacy behaviors. In addition, we have offered a set of high-level propositions to assist researchers in framing their inquiries. These propositions reflect the different organizing logics of these theoretical lenses. Clearly, more detailed exploration and empirical testing of these propositions is required.

To the best of our knowledge, neither the Institutional Approach nor the RBV has been used previously to examine information privacy as an organizational-level phenomenon. We argue that both the institutional approach and the resource-based view of the firm offer important theoretical insights into firms' information privacy behaviors. Incorporating these paradigms into privacy enquiries will also have the benefit of broadening the application of these underutilized theories in MIS research [Jarvenpaa and Leidner, 1998; Orlikowski and Barley, 2001; Robey and Boudreau, 1999; Wade and Hulland, 2004].

We expect that researching the institutional approach and resource-based view of information privacy practices in organizations will present significant challenges to researchers. First, this research will require intensive fieldwork in order "to gain an in-depth knowledge and understanding of the organization and its processes" [Rouse and Daellenbach, 1999:489]. In addition, this fieldwork will be required in more than one location in order to identify industry norms (IA) as well as competitive strategies (RBV). This approach represents both a resource and an ingenuity challenge to investigators. How will researchers identify likely candidates and secure the cooperation of organizations sufficient to the task? We suggest that the sectoral studies approach pioneered by Milne and Culnan [2004] represents a useful starting point for this work.

Second, there are significant design challenges associated with completing studies within the paradigmatic traditions of both theories. Identifying and understanding the sources for institutional pressures versus the seizing of competitive opportunities will not necessarily be apparent from a review of privacy policies posted on websites. In addition to that necessary work, researchers will have to engage in dialogue with employees in the various firms. Discerning the existence and role of the different elements attached to each theoretical lens will not only require attention to nuances and perceptions, it will demand vigilance and thoroughness. It is unlikely that any research site will have organized its privacy program

along recognizably "institutional" or "RBV" lines. Despite the anticipated difficulties, we believe a carefully crafted program of case-based research should yield useful results. We suggest strongly that the approach taken involve triangulation across multiple methods (especially documentary and interview processes) as well as multiple informants. In our experience with privacy research, no single individual or organizational group (regardless of title or organizational position) understands the entirety of a firm's privacy initiatives. No single document summarizes all aspects of a firm's information privacy motivations and behaviors.

Third, the definition of the scope for research will require careful consideration. The proliferation of multinational and global enterprises suggests that issues concerning the level of analysis within the firm must be addressed. Different divisions within an enterprise may have different sensitivities attached to the customer information that is collected. For example, divisions collecting customer information about grocery shopping preferences may operate with privacy standards that differ from those dealing with customers' financial or health information. These decisions are complicated by jurisdictional issues. For example, whose laws or codes will serve the wider enterprise as the privacy benchmark? The influences on a firm's choice of reference jurisdiction provide another avenue for interesting research.

A fourth set of research issues is presented by the question of what exactly is being investigated. If we set the level of analysis as the organization and the object of analysis as the information privacy policies and behaviors, what questions do we ask to collect important information? We suggest that there are several phenomena or constructs worthy of investigation. For example, can we discern specific information privacy strategies? Are there measures of information privacy effectiveness? Can a privacy program ROI be established? Can we identify key relationships between information privacy and information security behaviors? Are there specific organizational contexts that lead firms to choose to address information privacy as table stakes versus competitive advantage? What is the influence of investments in customer relationship management systems on the approach to and selection of information privacy behaviors? What privacy leadership roles (Chief Privacy Officers, etc.) are helpful given various information strategies? Clearly, information privacy offers rich opportunities for IS research.

A final issue for researchers involves discerning the relationship between the institutional and resource-based paradigms. To what extent do they provide a competing or complementary explanation for firms' privacy behaviors? At this juncture, we argue only that the two approaches offer distinct, separate, and useful insights into information privacy behaviors.
Research using these theories would, in our view, also support practitioners' efforts to "get privacy right." Articles in the popular and business press tend to stress the "tactics" of information privacy. That is, they emphasize information privacy maxims such as "don't abuse customer trust" and "provide the ability to opt-out." These are useful guidelines for managers seeking fast answers to pressing problems. However, carefully constructed and theoretically grounded research has an important role to play in helping managers. It can assist them in choosing how they might fashion their information management and information privacy programs; think about the ramifications of their privacy initiatives for their operations and their customers; and, ultimately, identify the longer term potential for information privacy to alter, and potentially improve, how they do business. For example, organizational level information privacy research might offer new insights into the conditions under which firms may choose to (not) compete with privacy, and how that would influence firm processes. As Kurt Lewin [1951] noted, "There is nothing so practical as a good theory."

Conclusion

Organizations are increasingly required to develop and implement information privacy policies and programs. This circumstance poses a challenge to managers and researchers alike. In this article, we have argued for the expansion of the information privacy research agenda to attend to theory building at the organizational level of analysis. In particular, we have called for increased theoretically-grounded research using the institutional and resource-based paradigms. We have provided high-level propositions to guide future research in this area.

A recent Gartner Group report suggested that information privacy is a strategy and not simply a policy [Herschel, 2003]. We agree that this is the case for some, but not all, firms. There is no single "silver bullet" approach to this complex organizational phenomenon. Our examination of how the lenses of the Institutional Approach and the Resource-Based View can explain firms' information privacy behaviors is our contribution to what we hope will be a growing and productive IS research debate.

Acknowledgement

The authors thank the Social Sciences and Humanities Research Council of Canada for providing funding to support this research. The authors also thank Sirkka Jarvenpaa and the two anonymous reviewers, as well as Jane Webster and Peggy Cunningham of Queen's University, for their helpful comments on previous versions of this article.

References

Editor's Note: The following reference list may contain hyperlinks to World Wide Web pages. Readers who have the ability to access the Web directly from their word processor or are reading the paper on the Web, can gain direct access to these linked references. Readers are warned, however, that

1. these links existed as of the date of publication but are not guaranteed to be working thereafter.
2. the contents of Web pages may change over time. Where version information is provided in the References, different versions may not contain the information or the conclusions referenced.
3. the author(s) of the Web pages, not AIS, is/are responsible for the accuracy of their content.
4. the authors of this article, not AIS, are responsible for the accuracy of the URL and version information.

Ang, S. and L.L. Cummings (1997) "Strategic Response to Institutional Influences on Information Systems", *Organization Science*, (8)3, pp. 235-256.

Ang, S. and D.W. Straub (1998) "Production and Transaction Economies and IS Outsourcing: A Study of the U.S. Banking Industry", *MIS Quarterly*, (22)4, pp. 535-552.

Barney, J.B. (1991) "Firm Resources and Sustained Competitive Advantage", *Journal of Management*, (17)1, pp. 99-120.

Barney, J.B. and M.H. Hansen (1994) "Trustworthiness as a Source of Competitive Advantage", *Strategic Management Journal*, (15), pp. 175-190.

Bennett, C.J. and R. Grant (1999) "Introduction", in Bennett, C.J. and R. Grant (eds.) (1999) *Visions of Privacy,* Toronto: University of Toronto Press, pp. 3-16.

Bhardawaj, A.S. (2000) "A Resource-Based Perspective on Information Technology Capability and Firm Performance", *Management Information Systems Quarterly,* (24)1, pp. 169-196.

Bordoloi, B., K. Mykytyn, and P.P. Mykytyn (1996) "A Framework to Limit Systems' Developers Legal Liabilities", *Journal of Management Information Systems*, (12), pp. 161-185.

Brumagin, A.L. (1994) "A Hierarchy of Corporate Resources", *Advances in Strategic Management,* (10A), pp. 81-112.

Cadogan, R. (2001) "The Ethics of Data Privacy in an Electronic Marketplace: A Multiple Case Study of the Privacy Policy Notice and the Incorporation of Fair Information Practice Principles", Unpublished dissertation, Viterbo University.

Cashore, B. and I. Vertinsky (2000) "Policy Networks and Firm Behaviors: Governance Systems and Firm Responses to External Demands for Sustainable Forest Management", *Policy Sciences,* (33)1, pp. 1-30.

Caudill, E.M. and P.E. Murphy (2000) "Consumer Online Privacy: Legal and Ethical Issues", *Journal of Public Policy and Marketing,* (19)1, pp. 7-19.

Chan, Y. (2003) "Competing Through Information Privacy", in Luftman, J.N. (ed.) (2003) *Competing in the Information Age: Align in the Sand* (2nd ed.), New York: Oxford University Press, pp. 350-361.

Clarke, R. (1999) "Internet Privacy Concerns Confirm the Case for Intervention", *Communications of the ACM*, 42(2), pp. 60-67.

Cocheo, S. (2003). "Georgia Bank Turns Privacy into a Marketing Plus," *American Banking Association. ABA Banking Journal*, 95(10), pp. 26-30.

Culnan, M.J. (1993) "How Did They Get My Name? An Exploratory Investigation of Consumer Attitudes Toward Secondary Information Use", *Management Information* Systems Quarterly, (17)2, pp. 341-363.

Culnan, M.J. (1999a) *Georgetown Internet Privacy Policy Survey: Report to the Federal Trade Commission*.

Culnan, M.J. (1999b) *Privacy and the Top 100 Websites: Report to the Federal Trade Commission,* prepared for the Online Privacy Alliance.

Culnan, M. J. (2000) "Protecting Privacy Online: Is Self-Regulation Working?" *Journal of Public Policy and Marketing*, (19)1, pp. 20-26.

Culnan, M.J. and P. Armstrong (1999) "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation", *Organization Science,* (10)1, pp. 104-115.

Culnan, M.J. and R.J. Bies (1999) "Managing Privacy Concerns Strategically: The Implications of Fair Information Practices for Marketing in the Twenty-first Century", in Bennett, C.J. and R. Grant (eds.) (1999) *Visions of Privacy: Policy Choices for the Digital Age*, Toronto, ON: University of Toronto Press, pp. 149-167.

Culnan, M.J. and R.J. Bies (2003) "Consumer Privacy: Balancing Economic and Justice Considerations", *Journal of Social Issues,* (59)2, pp. 323-342.

Culnan, M.J. and H.J. Smith (1995) "Lotus Marketplace: Households–Managing Information Privacy Concerns" in Johnson, D.G. and H. Nissenbaum (eds.) (1995) *Computer Ethics and Social Values* Prentice Hall.

Dacin, T., M.J. Ventresca, and B.D. Beal (1999) "The Embeddedness of Organizations: Dialogue and Directions", *Journal of Management,* (25), pp. 317-356.

Davison, R.M., R. Clark, H.J. Smith, D. Langford, and F.-Y. Kuo (2003) "Information Privacy in a Globally Networked Society: Implications for Information Systems Research", *Communications of the Association for Information Systems,* (12), pp. 341-365.
Devaraj, S. and R. Kohli (2000) "Information Technology Payoff in the Health-Care Industry: A Longitudinal Study", *Journal of Management Information Systems,* (16)4, pp. 41-67.
Dhillon, G., J. Bardacino, and R. Hackney (2002) "Value Focused Assessment of Individual Privacy Concerns for Internet Commerce", *Twenty Third International Conference on Information Systems*, Barcelona, Spain, pp. 705-709.
DiMaggio, P.J. and W.W. Powell (1983) "The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields", *American Sociological Review,* (48), pp. 147-160.
Dinev, T. and P. Hart (2003) "Privacy Concerns and Internet Use – A Model of Trade-off Factors", Presentation to 2003 *Academy of Management,* Seattle, Washington, August 2003.
Earp, J.B., A.I. Antón, and O. Jarvinen (2002) "A Social, Technical, and Legal Framework for Privacy Management and Policies", *Eighth Americas Conference on Information Systems*, pp. 605-612.
Federal Trade Commission (FTC) (1998) "Privacy Online: A Report to Congress", http://www.ftc.gov/reports/privacy3/priv-23a.pdf (current May 1, 2004).
Federal Trade Commission (FTC) (2000) "Privacy Online: Fair Information Practices in the Electronic Marketplace – A Report to Congress", http://www.ftc.gov/reports/privacy2000/privacy2000.pdf, (current May 1, 2004).
Foxman, E.R. and P. Kilcoyne (1993) "Information Technology, Marketing Practice and Consumer Privacy: Ethical Issues", *Journal of Public Policy and Marketing,* (12)1, pp. 106-119.
Gefen, D., E. Karahanna, and D.W. Straub. (2003) "Trust and TAM in Online Shopping: An Integrated Model", *MIS Quarterly,* (27)1, pp. 51-90.
Geist, M. and G. Van Loon (2000) "Canadian E-Commerce and Privacy Study 2000: A Failure to Communicate." Obtained from the first author.
Grant, R.M. (1991) "The Resource-Based Theory of Competitive Advantage: Implications for Strategy Formulation", *California Management Review,* (33)3, pp. 114-135.
Handelman, J.M. and S.J. Arnold (1999) "The Role of Marketing Actions with a Social Dimension: Appeals to the Institutional Environment", *Journal of Marketing,* (63), pp. 33-48.
Hann, I., K. Hui, T.S. Lee, and I.P.L. Png (2002) "Online Information Privacy: Measuring the Cost-Benefit Trade-off", *Twenty-Third International Conference on Information Systems*, Barcelona, Spain, pp. 1-10.
Hannan, M.T. and J. Freeman (1989) *Organizational Ecology*, Cambridge, MA: Harvard University Press.
Herschel, G. (2003) "Customer Privacy is a Strategy, Not a Policy," Letter from the Editor, *Gartner Group Research Note (LE-20-6616, July 29, 2003)*, *http://gartner.business.queensu.ca*, (current Mar. 9, 2004).
Hoffman, D.L., T.P. Novak, and M. Peralta, (1999) "Building Consumer Trust Online", *Communications of the ACM,* (42)4, pp. 80-85.
Ives, B. and S. Jarvenpaa (1991) "Applications of Global Information Technology: Key Issues for Management", *Management Information Systems Quarterly,* pp. 33-49.
Jarvenpaa, S. L. and D.E. Leidner (1998) "An Information Company in Mexico: Extending the Resource-Based View of the Firm to a Developing Country Context", *Information Systems Research,* (9)4, pp. 342-361.

Jones, M.G. (1990) "Privacy: A Significant Marketing Issue for the 1990s". *Journal of Public policy and Marketing,* (10)1, pp. 133-148.
Kumar, K., H.G. van Dissel, and P. Bielli (1998) "The Merchant of Prato – Revisited: Toward a Third Rationality of Information Systems", *MIS Quarterly,* (22)2, pp. 199-226.
Laudon, K. (1995) "Ethical Concepts and Information Technology", *Communications of the ACM,* (38)12, pp. 33-39.
Lewin, K. (1951) *Field Theory in Social Science: Selected Theoretical Papers*. New York: Harper & Row.
Mason, R.O. (1986) "Four Ethical Issues of the Information Age", *Management Information Systems Quarterly,* (10)1, pp. 4-12.
Mason, R.O., M.J. Culnan, S. Ang and F. Mason (2000) "Privacy in the Age of the Internet" in Dickson, G.W. and G. DeSanctis (eds.) (2000) *Information Technology and the Future Enterprise* Upper Saddle River, NJ: Prentice Hall, pp. 208-238.
Mata, F.J., W.L. Fuerst, and J.B. Barney (1995) "Information Technology and Sustained Competitive Advantage", *Management Information Systems Quarterly,* (19)4, pp. 487-505.
McKnight, G.H., V. Choudury, and C. Kacmar (2002) "Developing and Validating Trust Measures for e-Commerce: An Integrative Typology", *Information Systems Research* (13)3, pp. 334-359.
Meyer, J.W. and B. Rowan (1977) "Institutionalized Ceremonies: Formal Structure as Myth and Ceremony", *American Journal of Sociology*, (83)2, pp. 340-363.
Middlemiss, J. (2001). "RBC Pilots Online Privacy Tools Program." *Bank Systems and Technology Online*, December 7, 2001, downloaded from http://www.banktech.com/story/BNK20011207S0004, accessed January 2003.
Milberg, S.J., H.J. Smith, and S.J. Burke (2000) "Information Privacy: Corporate Management and National Regulation", *Organization Science,* (11)1, pp. 35-57.
Miller, D. and J. Shamsie (1996) "The Resource-Based View of the Firm In Two Environments: The Hollywood Film Studios from 1936-1965", *Academy of Management Journal,* (39)3, pp. 519-543.
Milne, G.R. (2000) "Privacy and Ethical Issues in Database/Interactive Marketing and Public Policy: A Research Framework and Overview of the Special Issue", *Journal of Public Policy and Marketing,* (19)1, pp. 1-6.
Milne, G.R. and M. Boza (1999) "Trust and Concern in Consumers' Perceptions of marketing Information Management Practices", *Journal of Interactive Marketing*, (13)1, pp. 5-24.
Milne, G.R. and M. Culnan (2002) "A Longitudinal Analysis of the Privacy Web Sweep Data: Using Marketing Research to Inform Public Policy" *The Information Society* (18), pp. 345-359.
Milne, G.R. and M. Culnan (2004) "Strategies for Reducing Online Privacy Risks: Why Consumers Read (Or Don't Read) Online Privacy Notices", *Journal of Interactive Marketing*, (18)3, pp. 15-29.
Milne, G.R. and A. Rohm. (2000) "Consumer Privacy and Name Removal Across Direct Marketing Channels: Exploring Opt-in and Opt-out Alternatives." *Journal of Public Policy and Marketing.* (19)2, pp. 238-249.
Milne, G.R., A.J. Rohm and S. Bahl (2004) "Consumers' Protection of Online Privacy and Identity", *The Journal of Consumer Affairs*, (38)2, pp. 217-232.
Miyazaki, A.D. and A. Fernandez. (2000) "Internet Privacy and Security: An Examination of Online Retailer Disclosures", *Journal of Public Policy and Marketing,* (19)1, pp. 54-61.
Mohamed, A.A., W.L. Gardner and J.G.P. Paolillo (1999) "A Taxonomy of Organizational Impression Management Tactics", *Advances in Competitiveness Research* (7)1, pp.108-130.

Oliver, C. (1991) "Strategic Responses to Institutional Processes", *Academy of Management Review,* (16), pp. 145-179.
Orlikowski, W.J. and S.R. Barley (2001) "Technology and Institutions: What Can Research on Information Technology and Research on Organizations Learn From Each Other?" *Management Information Systems Quarterly,* (25)2, pp. 145-165.
Pfeffer, J. (1981) "Management as Symbolic Action: The Creation and Maintenance of Organizational Paradigms" in L.L. Cummings and B.M. Staw (eds.) *Research in Organizational Behavior*, (3), pp. 1-52.
Pfeffer, J. (1997) *New Directions for Organization Theory,* New York: Oxford University Press.
Pfeffer, J. and G. Salancik (1978) *The External Control of Organizations*, New York: Harper and Row.
Porter, M.E. (1985) *Competitive Advantage,* New York: Free Press.
Robey, D.I. and M. Boudreau (1999) "Accounting for the Contradictory Organizational Consequences of Information Technology: Theoretical Directions and Methodological Implications", *Information Systems Research,* (10)2, pp. 167-185.
Rohm, A.J. and G.R. Milne (2004) "Just What the Doctor Ordered: The Role of Information Sensitivity and Trust in Reducing Medical Information Privacy Concern", *Journal of Business Research,* (57), pp. 1000-1011.
Rouse, M.J. and U.S. Daellanbach (1999) "Rethinking Research Methods for the Resource-Based Perspective: Isolating Sources of Sustainable Competitive Advantage", *Strategic Management Journal,* (20), pp. 487-494.
Ruef, M. and W.R. Scott (1998) "A Multidimensional Model of Organizational Legitimacy: Hospital Survival in Changing Institutional Environments", *Administrative Science Quarterly,* (43), pp. 877-904.
Ryker, R., E. Latteur, B. McManis, and K.C. Cox (2002) "Online Privacy Policies: An Assessment of the Fortune E-50", *Journal of Computer Information Systems,* (Summer), pp. 15-20.
Schoenbachler, D.D. and G.R. Milne (2002) "Trust and Consumer Willingness to Provide Information to Data-Driven Relationship Marketing", *Journal of Interactive Marketing*, (16)3, pp. 2-16.
Scott, W. R. (1987) "The Adolescence of Institutional Theory", *Administrative Science Quarterly,* (32), pp. 493-511.
Scott, W.R. (2001) *Institutions and Organizations* (2nd ed). Thousand Oaks, CA: Sage.
Sheehan, K.B. and M.G. Hoy (2000) "Dimensions of Privacy Concern Among Online Consumers", *Journal of Public Policy and Marketing* (19)1, pp. 62-73.
Smith, H.J. (1990) "Managing Information: A Study of Personal Information Privacy", Unpublished dissertation, Harvard Business School.
Smith, H.J. (1993) "Privacy Policies and Practices: Inside the Organizational Maze", *Communications of the ACM*, (36)12, pp. 105-122.
Smith, H.J. (2001) "Information Privacy and Marketing: What the U.S. Should (and Shouldn't) Learn from Europe", *California Management Review,* (43)2, pp. 8-33.
Smith, H.J., S.J. Milberg, and S.J. Burke (1996) "Information Privacy: Measuring Individuals' Concerns about Organizational Practices", *Management Information Systems Quarterly,* (20)2, pp. 167-196.
Srivastava, R.K., T. Shervani, and L. Fahey. (1998) "Market-Based Assets and Shareholder Value: A Framework for Analysis", *Journal of Marketing,* (62)1, pp. 2-18.
Srivastava, R.K., L. Fahey, and H.K. Christensen (2001) "The Resource-Based View and Marketing: The Role of Market-Based Assets in Gaining Competitive Advantage", *Journal of Management,* (27), pp. 777-802.

Srivatava, R.P. and T.J. Mock (2000) "Evidential Reasoning for WebTrust Assurance Services", *Journal of Management Information Systems,* (16)3, p. 11-32.

Stewart, K.A. and A.H. Segars (2002) "An Empirical Examination of the Concern for Privacy Instrument", *Information Systems Research,* (13)1, pp. 36-49.

Stone, E.F., D. G. Gardner, H.G. Gueutal, and S. McClure (1983) "A Field Experiment Comparing Information-Privacy Values, Beliefs and Attitudes Across Several Types of Organizations", *Journal of Applied Psychology*, (68)3, pp. 459-468.

Straub, D. and R.W. Collins (1990) "Key Information Liability Issues Facing Managers: Software and Proprietary Databases, and Individual Rights to Privacy", *Management Information Systems Quarterly,* (22)4, pp. 441-470.

Suchman, M.C. (1995) "Managing Legitimacy: Strategies and Institutional Approaches", *Academy of Management Review,* (20), pp. 571-610.

Sultan, F. and H.A. Mooraj (2001) "Designing a Trust-Based e-Business Strategy", *Marketing Management* (10)4, pp. 40-46.

Tam, E., K. Hui, and B.C.Y. Tan (2002) "What Do They Want? Motivating Consumers to Disclose Personal Information to Internet Businesses", *Twenty Third International Conference on Information Systems*, Barcelona, Spain, pp. 11-21.

Tingling, P. and M. Parent (2002) "Mimetic Isomorphism and Technology Evaluation: Does Imitation Transcend Judgment?" *Journal of the Association for Information Systems,* (3), pp. 113-143.

Tolbert, P.S. and L.G. Zucker (1996) "The Institutionalization of Institutional Theory" in Clegg, Stewart R., Cynthia Hardy and Walter R. Nord (eds.) (1996) *Handbook of Organizational Studies*, Thousand Oaks, CA: Sage, pp. 175-190.

Wade, M. and J. Hulland (2004) "The Resource-Based View and Information Systems Research: Review, Extension, and Suggestions for Future Research", *Management Information Systems Quarterly,* (28)1, pp. 107-142.

Winter, S.J., C. Saunders and P. Hart (2003) "Electronic Window Dressing: Impression Management with Websites", *European Journal of Information Systems*, (12), pp. 309-322.

Zhang, M.H. and A.A. Lado (2001) "Information Systems and Competitive Advantage: A Competency-Based View", *Technovation,* (21), pp. 147-156.

Appendix A: Fair Information Principles with Examples of Behaviors

The following table provides an explanation for and examples of the four main fair information practices. The examples are drawn from actual privacy policies. The "minimal privacy behavior" column includes examples address the most basic requirements while the "enhanced privacy behavior" exemplifies more specific and explicit disclosure of privacy practices.

Principle & Explanation	**Example of Minimal Privacy Behavior**	**Example of Enhanced Privacy Behavior**
Notice: Advising customers that their personal information is being collected	We collect your personal information to meet operational requirements.	We collect your personal information for the following reasons: • To verify your identity. • To provide the financial services you request. • To understand your financial and banking needs. • To develop and manage products and services to meet the needs of our customers. • To contact our customers directly for products and services that may be of interest. • To determine the eligibility of our customers for different products and services. • To meet regulatory requirements.
Choice: Allowing customers to choose the extent to which their information is tracked, used and reused.	By supplying your information you consent to our using it to meet our operational requirements.	You may choose: • not to receive marketing information. • to only receive marketing information specifically related to the services you have contracted with us. • to not permit us to share your information with other affiliated organizations within our corporate group. • not to permit us to share your information with other organizations affiliated with our corporate group. • not to provide information to us as long as that information is

		not required by law. • not required to fulfill our contract for certain products or services.
Access: Providing customers with access to their personal files	[No policy is provided.]	Upon request and within 45 days, we will provide for your review the specific personal information we have about you, what it is being used for, and to whom it has been disclosed. You may bring to our attention incorrect information in your personal file which we will review and amend as necessary.
Security: Ensuring that customers information cannot be accessed by unauthorized others	We treat your information with care.	We are committed to keeping your personal information safe in order to prevent its loss, theft, unauthorized access, disclosure, duplication, use, or modification. Depending on the sensitivity of the information, we will employ appropriate security measures to protect the information. The measures may include, for example, the physical security of offices and data centers, and electronic security measures such as passwords, encryption, and personal identification numbers. We will use appropriate security measures when disposing of your personal information. We will develop policies and procedures for the protection of personal information and employ the most up to date information protection technologies and procedures to ensure ongoing information security including authentication, non-repudiation, confidentiality and authorized access, and integrity processes.

Yolande E. Chan is Professor and E. Marie Shantz Research Fellow in MIS at Queen's University in Canada. She holds a Ph.D. from the University of Western Ontario, an M.Phil. in Management Studies from Oxford University, and S.M. and S.B. degrees in Electrical Engineering and Computer Science from MIT. Prior to joining Queen's, she worked with Andersen Consulting (now Accenture). Dr. Chan conducts research on information privacy, knowledge management, strategic alignment, and information systems performance. She has published her findings in journals such as *Information Systems Research*, *MIS Quarterly Executive, Journal of Management Information Systems, Journal of Strategic Information Systems, Information & Management*, *IEEE Transactions on Engineering Management, Communications of the AIS* and *The Academy of Management Executive.* Dr. Chan is a member of several journal editorial boards. She currently co-leads a $2 million research project on surveillance and privacy issues.

Kathleen E. Greenaway is a Post-Doctoral Fellow with the Globalization of Personal Data Project at Queen's University in Canada. She holds a Ph.D. in Management and an M.P.A from Queen's University, an M.B.A. from the University of Western Ontario, and a B.A in Canadian Studies from the University of Alberta. Dr. Greenaway has twenty years experience as a manager and consultant in the private, public and non-profit sectors. Her research interests include information privacy, knowledge management, organizational IT efficacy and business ethics. Dr. Greenaway's research has been presented at the *Academy of Management*, the *Americas Conference on Information Systems,* the *American Marketing Association Conference on Marketing and Public Policy,* the *Information Resource Management Association,* and the *Administrative Sciences Association of Canada.* Her work has been published in the *Communications of the AIS* and the *International Journal of Management Reviews.*

Journal of the Association for Information Systems
ISSN: 1536-9323