Understanding Consumer Privacy: A Review and Future Directions

Clinton D. Lanier, Jr.
University of Nebraska-Lincoln

Amit Saini
University of Nebraska-Lincoln

Clinton D. Lanier, Jr. is a Ph.D. Candidate and Amit Saini is an Assistant Professor at the University of Nebraska-Lincoln, Department of Marketing, CBA 310, P.O. Box 880492, Lincoln, NE 68588-0492. Mr. Lanier can be reached by phone (402) 472-2316, fax (402) 472-9777, or email: cdlanier@unlserve.unl.edu. Dr. Saini can be reached by phone (402) 472-2344, fax (402) 472-9777, or email: asaini@unlnotes.unl.edu.

EXECUTIVE SUMMARY

With the rise of the marketing concept and the institutionalization of various market orientation approaches, marketers have increasingly focused on understanding the consumer. For businesses, this has led to the collection of vast amounts of consumer information. Although most consumers welcome the increased convenience and personalization that these approaches provide, many are concerned about how these practices affect their privacy. The purpose of this article is to provide an understanding of the general concept of privacy, to review and summarize the literature on consumer privacy, and to suggest future research directions that will both synthesize and expand our understanding of consumer privacy.

Privacy

Although it is tempting to think of privacy as a modern concern brought forth by industrialization, urbanization, and mechanization, the desire for privacy has roots in both the animal world and "primitive" societies (Westin 1967). It has been found that both animals and humans seek a balance between seclusion and social interaction. For humans, this often takes the form of controlling disclosure of personal information. Most humans exist in some form of society. Societies, though, differ in the degree to which they balance the desire of their citizens to control disclosure of their personal information with the need to engage in surveillance to maintain the proper functioning of the society. Although many citizens of the U.S. believe they have a right to privacy, the U.S. Constitution does not explicitly grant this right. The U.S. Supreme Court has interpreted various amendments of the Constitution as implicitly granting the right to privacy. Early definitions of the right to privacy focused on the right to be left alone. Later definitions focus on issues of control and access (Altman 1975; Westin 1967). Given the lack of an agreed upon privacy definition, privacy law in the U.S. has followed Prosser's four torts of privacy: intrusion, appropriation, disclosure, and false light (Prosser 1960). While outlining specific causes of action, most business practices that involve the analysis, use, and sharing of consumer information do not violate these four torts (Nowak and Phelps 1997). The U.S. Federal government has passed a limited number of laws to protect specific types of consumer information (e.g., health records and credit information), but allows the majority of firms to self-regulate the privacy protection of most forms of consumer information.

Consumer Privacy Literature Review

The review is based on consumer privacy articles published from 1989 to 2007 in a variety of academic journals. This review is meant to help the reader understand the current state of consumer privacy research. The review is divided into three main areas: 1) conceptualizations of consumer privacy, 2) consumer-related privacy issues, and 3) firm-related privacy issues.

Conceptualizations of Consumer Privacy – Early definitions of consumer privacy focus on two forms of control: 1) control of presence of others in the marketing environment and 2) control of transactional information (Goodwin 1991; Jones 1991). These early definitions of privacy have been expanded to include consumer knowledge, or the degree to which

consumers are informed about and understand a firm's information practices and privacy policies (Foxman and Kilcoyne 1993; Nowak and Phelps 1995). Although consumers maintain that they have a right to privacy in marketing situations, consumer privacy is not considered absolute for three main reasons: 1) consumer privacy often conflicts with other consumer and marketer rights, 2) what constitutes consumer privacy is culturally, situationally, and individually determined, and 3) marketers and consumers differ in terms of who "owns" consumers' private information (Foxman and Kilcoyne 1993; Milne and Gordon 1993). Likewise, the ethical dimensions of consumers' right to privacy and marketers' information practices have been explored in the literature. Researchers have examined the teleological and deontological justifications of information control, the privacy trade-offs that consumers make with a firm based on social contract theory, and the application of various theories of justice to explain perceptions of power, trust, and fairness regarding a firm's information practices.

Consumer-Related Privacy Issues – Many factors have a direct bearing on consumers' privacy concerns including awareness, information usage, information sensitivity, familiarity with the entity, and compensation (Sheehan and Hoy 2000). Demographic variables such as gender, age, and income also affect consumers' views of various privacy issues (Culnan and Armstrong 1999; Sheehan 1999). Some of the ways that consumers self-manage their privacy concerns include reading privacy notices, avoiding collection of information, engaging in name removal, exercising their legal rights, and managing their online identities (Milne and Rohm 2000; Zwick and Dholakia 2004). Research suggests that if concerns about consumer privacy are not mitigated, they can have negative consequences on decision-making, purchasing, and firm/brand trust (Eastlick, Lotz, and Warrington 2006; Phelps, D'Souza, and Nowak 2001).

Firm-Related Privacy Issues – Three broad firm-level privacy issues have been addressed in the literature: 1) the extent to which firms follow the fair information practices (FIPs) in their privacy policies/notices, 2) the legal and business challenges that firms face when dealing with consumer privacy protection, and 3) the various alternatives available to firms in order to manage and communicate privacy protection while pursuing strategic and financial success in the marketplace. Several studies that investigated the self-regulation of online privacy by commercial businesses found that while the number of firms that collected some form of personal information was rather high, compliance with all of the FIPs was rather low. While later studies found that more firms were complying with the FIPs, the research suggests that more could and should be done by firms to protect consumer privacy (Hoy and Phelps 2003; Milne and Culnan 2002; Sheehan 2005). On the legal front, in addition to complying with the FIPs, firms need to be aware of both federal and state privacy legislation specific to their industries in crafting their privacy statements (Bloom, Milne, and Adler 1994). The primary business challenge is to deliver an optimal level of privacy protection that mitigates consumers' fears, as well as builds trust, while minimizing the cost of compliance to the firm (Milne and Boza 1999; Sarathy and Robertson 2002). In addition, research suggests that firms need to articulate an explicit, transparent, and readable privacy policy in order to empower consumers and mitigate their privacy fears (Milne, Culnan, and Greene 2006; Pollach 2005).

Future Research Directions

As evidenced by the literature review, research on consumer privacy has grown considerably in the past twenty years and has provided many insights to researchers, practitioners, and policy makers alike. While this research has made significant contributions towards highlighting consumer privacy as a critical business issue, it has addressed this matter primarily from a descriptive point of view and has focused less on developing consumer privacy from a theoretical perspective (Margulis 2003). In this section, we propose various directions that future consumer privacy research can take in order to develop a more theoretically-driven body of research. First, research should focus on operationalizing the dimensions of consumer privacy and examining their relationships. Second, more research needs to examine the conditions and situations that influence the trade-offs that consumers are willing to make between their perceived right to privacy and their other rights. Third, research into consumer privacy ethics needs to be extended by testing the relationship between various firm-level practices and their affects on consumers' privacy perceptions. Fourth, more research is needed that examines the firm-level strategy of managing consumer privacy. Research should focus on issues related to how firms should address privacy protection through their organizational structure and how market-oriented firms need to adapt or modify their strategies to efficiently and effectively manage consumer privacy in ways that benefit both the firm and their customers.

In addition, recent technological advances and changing perceptions of privacy need to be addressed in the literature. First, while the academic literature on identity theft is growing, it is one of the fastest growing white collar crimes in the United States and deserves more research attention. For instance, research should examine to what degree is marketing or other business practices responsible for this growing epidemic? Second, in spite of the growth of identity theft, more and more consumers are voluntarily posting large amounts of personal information online. Many consumers, especially younger consumers, as well as some business leaders and academics, argue that privacy is dead and that we have to accept that we now live in a world of surveillance. Research should examine these changing consumer perceptions and their affects on consumers' behaviors. Third, research needs to examine the business techniques of consumer profiling and electronic surveillance for both their ethical and practical implications. We feel that these categories represent the most critical and immediate privacy issues facing consumers, firms, and governments today.

Conclusion

Substantial progress has been made since the late 1980s to define consumer privacy and examine many of the issues related to this concept. However, more theoretically-driven research needs to be conducted in order to develop a working model of consumer privacy that specifies and defines this domain and that highlights the relationships between the relevant individual-level and firm-level dimensions, as well as their antecedents and consequences. In addition, more academic research is needed that addresses contemporary issues of consumer privacy from the changing perspectives of consumers and firms. Through this review, we have summarized the general concept of privacy, reviewed the current state of consumer privacy research, and have suggested ways to move this very important research area forward in the future. Consumer privacy is a continuing concern among many individuals and firms, and needs to be further developed in order to address these concerns in ways that efficient and effective for all those concerned.

Keywords: Consumer Privacy, Ethics, Fair Information Practices, Identity Theft, Online Privacy, Consumer Profiling, Privacy, Privacy Protection, Privacy Rights, Privacy Regulation, Surveillance.

Understanding Consumer Privacy: A Review and Future Directions

The evolution of marketing from a production orientation to a market orientation (Kieth 1960; Kotler and Zaltman 1971), as exemplified by the marketing concept (Barksdale and Darden 1971; Houston 1986; McKitterick 1957), has led to a dramatic increase in the need to understand the consumer. While application of this market orientation approach, especially in the forms of direct and relationship marketing, arguably brings multiple benefits to both consumers and firms (Kohli and Jaworski 1990; Narver and Slater 1990), it also requires a large amount of consumer information in order to deliver value (Nowak and Phelps 1997). The widespread adoption of information technology (IT) has allowed firms to meet this need for consumer information by vastly increasing the amount and types of information they collect (McCrohan 1989; Thomas and Maurer 1997). For firms, advances in IT have considerably enhanced the institutionalization and utilization of the market orientation approach by providing the technological infrastructure to capture, analyze, and maintain large quantities of consumer information (Winer 2001). For consumers, though, the collection and analysis of their personal information has led to an increase in privacy concerns (Foxman and Kilcoyne 1993; Phelps, Nowak, and Ferrell 2000).

While most consumers welcome the increased convenience and personalization that these various marketing orientation approaches provide, many are concerned about the collection, use, and protection of their personal information (Phelps et al. 2000; Rust, Kannan, and Peng 2002). Given the sharp increases in unsolicited promotions, incidences of identity theft, and the negligent loss of consumer information by firms, these fears are not altogether unwarranted (Levy and Stone 2005). For many consumers, major privacy concerns fall into three main categories: (1) notification, (2) control, and (3) security. First, many consumers want to be informed about the collection and use of their personal information by firms (Dommeyer and Gross 2003; Milne and Culnan 2004; Nowak and Phelps 1995), Second, consumers want to feel that they have some control over the collection of their personal information and the sharing of this information among firms (Goodwin 1991; Milne and Boza 1999; Phelps et al. 2000). Third, most consumers want some assurance that the personal information they provide to firms, especially online, and the storage of this information is secure (Hoy and Phelps 2003; Jones 1991; Miyazaki and Fernandez 2000). Although multiple legal, commercial, and technological solutions have been proposed to address these concerns (Foxman and Kilcoyne 1993; Goodwin 1991; Phelps et al. 2000), the protection of consumer privacy remains a constant concern for consumers and a formidable challenge for businesses.

In an attempt to understand these issues, consumer privacy research has sought to define the concept of consumer privacy, outline the privacy expectations and strategies of both consumers and businesses, and examine the degree to which firm's are providing adequate consumer privacy protection. While this body of research has provided us with valuable information concerning these issues, there currently does not exist a review that synthesizes and analyzes the current state of consumer privacy research. Given the complexity of the topic and the diversity of issues that have been explored, we feel that a comprehensive review is necessary to refine our understanding of this important topic and to take consumer privacy to a more advanced theoretical level. As a result, the purpose of this article is to examine the general concept of privacy in order to situate and define the domain of consumer privacy, review the literature on consumer privacy in order to determine what we know, and provide directions for future research in order to address gaps in the literature. We begin by examining the general nature of privacy, privacy rights, and privacy regulation. Next, we review the various conceptualizations of consumer privacy. Third, we examine privacy issues from the perspectives of both consumers and firms. Fourth, we propose directions for future research. Because the conceptualization of privacy in general and consumer privacy in particular differs among cultures and nations, this review will focus primarily on issues of privacy in the United States.

Academy of Marketing Science Review
volume 12, no. 02 Available: http://www.amsreview.org/articles/lanier02-2008.pdf

PRIVACY

The debate on the nature and scope of privacy is vast and includes research in such diverse disciplines as biology, anthropology, and legal philosophy. While it is not our goal to present research on privacy from all the various disciplines in a single article, we feel that a certain amount of background information on privacy is necessary in order to examine and situate of the notion of consumer privacy. This section provides an overview of the general concept of privacy and its relevance to U.S. law and business.

The Nature of Privacy

The relationship between advances in information technology, including the digitizing and dissemination of all forms of information, and the increase in privacy concerns among individuals, organizations, and governments is well documented (e.g., Ashworth and Free 2006; McCrohan 1989; Milne 2000; Peslak 2005; Thomas and Maurer 1997). But while it is tempting to think of privacy as strictly a modern concern brought forth by such things as industrialization, urbanization, and mechanization (Glazer 1998), the desire for privacy can be traced back to primitive (or pre-modern) societies and even to the animal world (Honigmann 1959; Moore 1984; Westin 1967).

Privacy Needs – It has been found that all animals seek different levels of interaction, ranging from seclusion and small group relations to broader social interaction (Allee 1938; Ardrey 1966; Wynne-Edwards 1962). Seclusion is important because it allows animals to regulate resources, propagate the species, and process information about the world around them (Hall 1966). At the same time, social interaction is necessary because it allows animals to learn, grow, and protect themselves (Ardrey 1966; Wynne-Edwards 1962). Because animals need both seclusion and interaction to survive, they constantly seek to establish a balance between seclusion and interaction, or in other words, between privacy and participation (Westin 1967).

This need for both privacy and participation is also evident among humans. Although some anthropologists suggest that privacy did not exist in primitive societies given the structure of these societies (Jones 1914; Lee 1959; Mead 1949), others argue that privacy was maintained in ways that were more psychological rather than physical (Geertz 1973; Murphy 1964). That is, while many individuals in these societies were not able to control access to many physical aspects of their environment, they could restrict and regulate the information about themselves that they shared with others (Jourard 1966; Westin 1967). Through the selective disclosure of information, individuals in primitive societies were able to achieve the seclusion that was needed by all animals, a tactic that holds over even in more developed societies (Simmel 1950).

In addition to the desire for privacy, members of primitive societies also sought to participate with others in the larger group. As Spinoza (1989) argues, humans are social animals that are scarcely able to lead a completely solitary life. While some of the reasons for social interaction are practical, such as satiation of the physical needs for food, shelter, and security (Spinoza 1989), others are less practical, such as curiosity (Berlyne 1960; Siep 1978) and the desire to have fun (Huizinga 1950; Sutton-Smith 1997). In either case, humans often engage in physical contact with others and disclose information about themselves, as well as to seek out information from others, in order to interact socially (Westin 1967).

Because of this need for both seclusion and interaction, privacy is not considered an absolute human condition (Clark 1978; Westin 1967). That is, human nature is such that most individuals do not seek either constant solitude (i.e., total isolation from others) or continuous social interaction (i.e., total immersion with others). Researchers have discovered that psychological abnormalities often develop in those individuals who either completely reject social interaction or who actively seek to avoid solitude (Fromm-Reichmann 1959; Horney 1945). Proper human development requires individuals to constantly seek a balance between privacy and participation (Westin 1967).

At a broader social level, societies also have to address the balance between the need for privacy and participation. All societies require rules and the adherence to them by their members in order to function properly (Moore 1984; Shils 1966). In addition, societies also need to establish mechanisms to detect transgressions of their norms and rules and to punish these behaviors in order to maintain their proper functioning (Westin 1967). These detection mechanisms often take some form of surveillance in which societies monitor their citizens in order to make sure their behavior stays within the bounds of the society's rules (Flaherty 1989; Goffman 1961; Miller 1999). The degree to which societies balance privacy, participation, and surveillance depends on the broader historical culture and traditions from which each society derives (Flaherty 19677; Shils 1966; Westin 1967).

While privacy clearly is not a recent phenomenon, the rise of modern industrial society has had a definite impact on issues of privacy, participation, and surveillance. Both industrialization and urbanization altered peoples' personal and societal relations (Simmel 1950). While these historical factors and the complex societies in which they were embedded provided more opportunities for physical and psychological privacy (e.g., the anonymity of city life), they also required greater individual disclosure and government surveillance in order for these societies to function properly (Honigmann 1959; Merton 1957; Westin 1967). Technological advances, as well as the constant need for information from individuals to participate in modern societies (especially capitalistic and democratic societies), have led to practices in which societal surveillance (by both public and private entities) can overwhelm the delicate balance of privacy and participation necessary for proper individual development (Miller 1999).

Privacy States and Functions – Westin (1967) argues that privacy consists of four basic states: solitude, intimacy, anonymity, and reserve. Solitude is the condition of being physically separated from others and free from observation. Intimacy is the condition of existing as a small unit (e.g., the family) while maintaining seclusion from others outside the unit. Anonymity is the condition of being in public while still being free from identification and surveillance. Reserve is the condition in which a person has created psychological barriers to protect him/herself from unwanted intrusions. In addition, Westin (1967) describes four functions of privacy: personal autonomy, emotional release, self-evaluation, and limited/protected communication. First, privacy helps to secure personal autonomy by allowing individuals to take control of and responsibility for their lives (Shils 1959). Second, privacy provides the individual with a space for emotional release from the pressures of performing daily roles and conforming to social norms (Goffman 1959). Third, privacy gives individuals time to integrate their life experiences and craft their identities through self-evaluation (Jourard 1966). Fourth, privacy allows limited communications in which people can set boundaries in interpersonal situations and protected communication in which the person can share confidences and establish trust (Simmel 1950).

Privacy Rights – Although most Americans believe that they have a right to privacy, the U.S. Constitution does not explicitly grant this right or its protection. In spite of this, the U.S. Supreme Court has argued that the right to privacy is implicit in the First, Fourth, Fifth, Ninth, and Fourteenth Amendments (DeCew 1997; Hosch 1983; McWhirter and Bible 1992). The First Amendment's acknowledgement of the rights of religious practice, free speech, and assembly has been interpreted as providing protection of individual privacy by limiting government intrusion (Glenn 2003). The Fourth Amendment's protection against search and seizures was expanded to include an individual's reasonable expectation of privacy and protection from surveillance without a warrant (Smith 1989). The U.S. Supreme Court has argued that one of the purposes of the Fifth Amendment's protection against self-incrimination is to protect individual disclosure of private information, with the caveat that this protection only applies when there is compulsion, communication, and incrimination (Rich 1987). The Ninth Amendment's claim that there are other rights that citizens retain that are not explicitly stated in the Constitution has been used to argue for the existence of the right to privacy (Glenn 2003; Tuerkheimer 1993). Lastly, the Fourteenth Amendment's requirements that no law or state will abridge an individual's privileges or immunities, deny any person his/her rights without due process, or deny any citizen equal protection under the law have been interpreted as implying the protection of individual privacy (McWhirter and Bible 1992).

It is important to note that although these various Amendments can be interpreted as providing privacy protection (irrespective of whether privacy is considered as a right or a privilege) (Phelps et al. 2000), the U.S. Supreme Court has argued that not every privacy infringement violates a person's constitutional rights (McCrohan 1989).

In fact, it is accepted that explicitly granted constitutional rights supersede any implicit rights, such as the right to privacy (Clark 1978; Found 1961). In addition, the Constitution only protects individuals from the violation of their rights by federal and state governments; violations of rights by private parties must be addressed by federal and state laws (Foxman and Kilcoyne 1993; Nowak and Phelps 1997). This is especially important for assessing any obligations that firms may feel towards protecting consumer privacy.

One of the primary reasons for recognizing the implicit right (or privilege) to privacy is that individual free expression is necessary for the proper functioning of democratic societies (Gavison 1980; Jones 1991; Rachels 1975; Westin 1967). This is evident in the distinction between dictatorships (or totalitarian regimes) and democracies. Dictatorships are based on rule by an individual or select few, extensive surveillance and intrusion, and compelled disclosure (Westin 1967). Individual privacy is sacrificed in the name of protecting and sustaining the particular ideology of the State. Democracies, such as the U.S., are based on popular consent, limited government surveillance and intrusion, and private property (Peslak 2005). In order for a democratic society to reflect the will of the people and not the ideology of the State, citizens must be allowed freedom to participate in organizations (including privacy of membership), freedom of political choice (including secret ballots), and freedom from coercion by the State (including limited surveillance and intrusion) (Westin 1967). All of these requirements, as well as the principles of democracy, are undermined by denying individuals the right to privacy and the ability to control information about themselves and their affiliations.

Definitions of Privacy

Although the U.S. Supreme Court has acknowledged an implicit right to privacy, it has not provided a formal definition of privacy. One of the earliest and most recognized definitions of privacy was crafted by Samuel Warren and Justice Brandeis for an article in the *Harvard Law Review*. As if written today, the legal scholars argue,

> Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right 'to be let alone' . . . [T]he question whether our law will recognize and protect the right to privacy in this and in other respects must soon come before our courts for consideration. Of the desirability – indeed the necessity – of some such protection there can, it is believed, be no doubt (Warren and Brandeis 1890, p.195-96).

Warren and Brandeis (1890) argued that changes in society and business necessitated modifications in the basic tort protection of person and property to include the recognition of new rights – namely the right to privacy. A key aspect of their argument was that existing tort law was unable to protect individuals' intangible rights or property, what they called the protection of private facts, from the increasing use of new technologies. This is apparent in the case of *Olmstead v. U.S. (1928)*, one of the first wiretapping cases heard by the U.S. Supreme Court, which held that wiretapping was legal because it did not involve physical entry or tangible property. This ruling was eventually overturned by the case of *Katz v. U.S. (1967)*, which finally recognized the negative impact of technology on individuals' privacy beyond its physical intrusion. In spite of this recognition of the right to privacy and the acknowledgement by the courts of nonphysical injuries, many critics argued that this early definition of privacy was too vague to adequately protect individual privacy rights (Bloustein 1968; Dickler 1936; Nizer 1941).

In an attempt to better address infringements on individual privacy, Prosser (1960) argued that privacy was not a unitary concept, but encompassed four distinct legal torts: 1) intrusion (i.e., invading a person's solitude or seclusion), 2) appropriation (i.e., using a person's identity or image without permission), 3) disclosure (i.e., making public embarrassing private facts about a person), and 4) false light (i.e., portraying an individual in a way that inaccurately and negatively represents the person). This framework, while extending the earlier conception of privacy, restricts privacy tort violations to individual-level information (versus group-level or aggregated data such as census data, though census data based on residential areas with few homes are not reported in depth because one might infer individual information), to information that is deemed private, and to the public dissemination of this private information (Nowak and Phelps 1997; Zimmerman 1983). This multidimensional definition was meant to clarify the right to privacy and provide for specific causes of action that could be tried in a court of law.

While Prosser's framework has been accepted by most U.S. courts and is the basis of most common law conceptions of privacy (McWhirter and Bible 1992), many critics argue that it does not go far enough in addressing all violations of a personal privacy. In fact, some argue that it favors organizations and businesses and unduly influences their conceptions of privacy (Foxman and Kilcoyne 1993; Nowak and Phelps 1997). For example, the "false light" tort does not apply to the transmission of factual consumer information from one firm to another because the data is not false and has not been made public (Graham 1987) (also see *Shibley v. Time, Inc. 1974*). Likewise, the "intrusion" tort does not apply to situations where the consumer voluntarily provides a firm with personal information and the firm then transfers this information to a third party for purposes unrelated to the intent of the original disclosure (McWhirter and Bible 1992) (also see *Dwyer v. American Express Company 1995*). As a result, the collection and dissemination of consumer information by firms rarely violates these more specific formulations of the right to privacy (Foxman and Kilcoyne 1993; Nowak and Phelps 1997; Phelps et al. 2000).

Due to both the limitations and ubiquity of Prosser's conception of privacy, some legal scholars have argued that privacy should not be considered as a multidimensional concept, but as a unitary concept in order to increase its applicability across a broader range of privacy issues (Benn 1971; Bloustein 1964; Gavison 1980; Graham 1987). These scholars argue that privacy should not be categorized by different interests, but should be based on the more general idea of protecting human dignity (Bloustein 1964; Gavison 1980). This broader conceptualization of privacy is based on peoples' control over their autonomy and accessibility. These scholars argue that this unitary concept of privacy based on control provides a wider base of protection for a broader range of privacy violations.

In line with the unitary conception of the right to privacy, various definitions of privacy have emerged. For instance, privacy has been defined as 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, pp. 6-7). This definition specifically focuses on the ability of individuals to control access to and dissemination of their personal information. This focus on information control is also present in popular definitions of privacy provided by Jourard (1966), Fried (1968), and Parker (1974). Other definitions of privacy focus on the social aspects of control and access (Altman 1975). For instance, Van Deg Haag (1971, p.149) argues that "privacy is the exclusive access of a person to a realm of his own. The right to privacy entitles one to exclude others from (a) watching, (b), utilizing, and (c) invading his private realm" (Introna and Pouloudi 1999). The social component is also echoed in definitions by Gross (1967), who focuses on the right to keep personal relationships private; Posner (1981), who focuses on privacy as freedom from unwanted intrusion by others (similar to Warren and Brandeis); and Johnson (1989), who focuses on privacy as the ability to immune oneself from the judgments of others.

In sum, privacy has been defined in many different ways. For some it is a multidimensional concept; for others, it is a unitary concept. In fact, what constitutes privacy is still a contentious issue that is debated among government officials, policy makers, private organizations, and individual citizens. This is evident in comments made at a 2007 intelligence conference by Donald Kerr, the principal deputy director of national intelligence in the U.S., who argued that the focus of the definition of privacy needs to change from issues of anonymity to issues of security. In another statement that shows the relationship between issues of privacy and surveillance, Kerr argues that it should be the government and businesses that monitor and safeguard people's private information (AP 2007). In spite of the persistent ambiguity of the concept of privacy, the U.S. government has taken some steps to address and regulate privacy protection.

Government Regulation of Privacy

Although Prosser's multidimensional framework still holds sway over most U.S. courts, the more unitary definitions of privacy and the limited ability of the common law to protect individuals' privacy have not gone unnoticed by U.S. law makers. One of the first laws to address individual privacy, the Fair Credit Reporting Act (FCRA)[1], was enacted to protect consumers' right to privacy in the collection of personal information by credit, personnel,

[1] 15 U.S.C. 1681 (1970)

and insurance agencies. Personal information refers to a consumer's financial information, reputation, personal characteristics, and mode of living. According to the FCRA (1970), "consumer reporting agencies [are required to] adopt reasonable procedures for meeting the needs of commerce for consumer credit, personnel, insurance, and other information in a manner which is fair and equitable to the consumer, with regard to the confidentiality, accuracy, relevancy, and proper utilization of such information in accordance with the requirements of this title."[2] Congress realized that in order to function effectively in a capitalist society, consumers are required to provide large amounts of personal information to firms (FCRA 1970). Congress also felt that this almost mandatory disclosure of information required laws that would protect consumers' most vital information, but which would also give firms the flexibility to conduct business in an effective and efficient manner. This was one of the first attempts by the U.S. government to grapple with the issue of privacy rights through the legislative process.

In 1973, an advisory committee to the Secretary of Health, Education, and Welfare presented its findings of a study on the increased use of automated personal data systems for the collection, storage, and use of personal information in both the public and private sectors. The committee was asked to examine the harmful consequences of these new technologies and the safeguards that might be needed to protect individuals and their personal information. Two of the major findings of the committee were that these data systems were having a negative impact on consumers relative to firms and that consumers' control over their personal information was steadily diminishing. The committee linked this lack of control directly to consumers' right to privacy and the need for privacy protection. They found that "under current law, a person's privacy is poorly protected against arbitrary or abusive record-keeping practices."[3] In order to provide a set of minimum standards for data management practices, the committee argued that Congress should enact a Federal Code of Fair Information Practices. These practices include the prohibition against secret data files, notice to the individual, consent for secondary use of personal information, access to personal information, and security of information (Jones 1991). Any violations of the practices were to be subject to both criminal penalties and civil remedies.

While the Fair Information Practices (FIPs) were not enacted into law, they have become the benchmark for privacy protection and have influenced subsequent laws and regulation. In 1974, Congress passed the Privacy Act,[4] which regulates the collection, storage, and use of an individual's personally identifiable information by government agencies. This information includes, but is not limited to, education, financial, medical, criminal, and employment information that can be directly linked to an individual. The Privacy Act loosely follows the FIPs by addressing the issues of relevance, reliability, misuse, and security of personal information. The FIPs have also influenced other federal laws including the Right to Financial Privacy Act (1978), the Cable Communications Policy Act (1984), the Computer Security Act (1987), the Video Privacy Protection Act (1988), the Telephone Consumer Protection Act (1991), the Driver's Privacy Protection Act (1994), Health Insurance Portability and Accountability Act (1996), the Children's Online Privacy Protection Act (1998), and the Financial Modernization Services Act (1999), as well as many state and local laws (Smith 2002).

Although the 1973 advisory committee argued that it was not necessary at that time to appoint a government agency to oversee the privacy protection of individuals' personally identifiable information, the Federal Trade Commission (FTC) has since taken on this role. The FTC was established in 1914 primarily to promote consumer protection and competitive markets. Of its three main bureaus, the Bureau of Consumer Protection has as its mission the protection of consumers against unfair, deceptive, or fraudulent business practices. Of primary concern to this bureau is the protection of consumer privacy. It has direct charge over monitoring and enforcing many of the privacy laws and regulations mentioned above, as well as promoting the self-regulation of privacy in those industries in which privacy laws have not been enacted. In the next section of the article, we examine specifically how consumer privacy has been conceptualized in the extant literature and summarize the various consumer privacy issues that have been explored.

---

2 15 U.S.C. 1681, §602b (1970)

3 Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems, July 1973, "Summary and Recommendations," Available: http://aspe.hhs.gov/datacncl/1973privacy/ tocprefacemembers.htm.

4 15 U.S.C. 552 (1974)

A REVIEW OF THE CONSUMER PRIVACY LITERATURE

The following section reviews the current state of consumer privacy research and the dominant themes in the consumer privacy literature. The review is based on articles published from 1989 to 2007 in a variety of academic business journals in marketing, management, business ethics, and information sciences. A summary of the articles' foci, key concepts/issues, and primary findings is provided in Table 1. The review is divided into three main areas: 1) conceptualization of consumer privacy, 2) consumer-related privacy issues, and 3) firm-related privacy issues. The first section examines the definition of consumer privacy, consumer privacy rights, and consumer privacy and ethics. The second section explores issues related to the antecedents of consumer privacy concerns, consumer management of privacy concerns, and the consequences of consumer privacy concerns. The third section explores issues related to firm compliance with the FIPs, legal and business challenges concerning consumer privacy, and managing and communicating privacy protection.

TABLE 1
Summary of Consumer Privacy Literature

Author(s)/Date (Chronological Order)	Focus of Article	Key Concepts/Issues	Key Proposals/Findings
McCrohan (1989)	Examination of the effect of information technology on privacy; specifically, the government use of marketing research data and computer matching.	Types of consumer data: registration, administrative, facilitation, and survey. Uses of consumer data: program design, program evaluation, and program enforcement.	The use of all four types of data for government program design and evaluation is appropriate. Only the use of registration data is appropriate for program enforcement, since the use of the others would severely impact individuals' willingness to provide information.
Goodwin (1991)	Overview and definition of consumer privacy.	Consumer privacy is defined as the consumer's ability to control (a) presence of other people in the environment during a market transaction or consumption behavior and (b) dissemination of information related to or provided during such transactions or behaviors to those who were not present.	Taxonomy of privacy states: 1) total control, 2) environment control, 3) disclosure control, 4) no control. Four sources of privacy conflict: 1) privacy and expected service levels, 2) privacy and other rights, 3) privacy and cost of privacy protection, 4) privacy and societal values.
Jones (1991)	Review of origins of privacy concerns, responses to these concerns, and privacy protection options.	Three ways to promote privacy protection through: 1) competition, 2) industry self-regulation, and 3) government regulation of minimum privacy standards. Provides information on the fair information practices.	Privacy is not an issue on which firms are likely to compete, since it falls into the category of "negative" information about the company. Self-regulation has led to privacy codes that vary in scope and definiteness. Certain minimum standards are necessary to protect consumers' privacy.
Nowak and Phelps (1992)	Examination of how well informed consumers are about marketing information gathering and use practices.	Study focuses on the use of individual-level information – information that pertains or relates to a single identifiable person – by direct marketers. Study attempts to understand why consumers are concerned about their privacy.	Four main results: 1) privacy is an important concern among consumers, 2) many consumers are not very knowledge-able about direct marketing practices, 3) consumer concern is affected by the type of information and information use, and 4) most consumers favor restrictions on the gathering and use of personal information. Consumer ignorance may be a significant contributor to privacy concerns.

Foxman and Kilcoyne (1993)	Examination of the ethical dimensions of marketing information practices and consumer privacy.	Two important dimensions of consumer privacy are consumer control and knowledge. Two major ethical conflicts between marketing practice and consumer privacy include control of information (i.e., information ownership) and conflicting rights.	Firms justify their control of consumer data on utilitarian grounds. This may just be a form of egoism that denies the autonomy of the consumer. Consumers demand conflicting rights: the right to privacy and the right to being informed. These rights also conflict with a firm's right to be left alone. These rights have both deontological and utilitarian justifications.
Milne and Gordon (1993)	Examination of the trade-offs consumers make when considering the attributes of direct mail social contracts.	Direct mail is an implied social contract in which consumers provide information to marketers in return for offers that may be of interest to them. Direct mail social contracts have four attributes: volume, targeting, compensation, and permission	Consumers want improved targeting efficiency and lower mail volume, but they are not willing to pay for these improvements. Consumers perform a cost/benefit analysis of the attributes of direct mail when examining the privacy-efficiency tradeoffs and are willing to provide some private information in exchange for an economic/social benefit.
Bloom, Milne, and Adler (1994)	Examination of the misuse of new information technologies (IT) in marketing.	Four areas of possible IT misuse: 1) price-fixing through information exchanges, 2) monopolizing essential facilities, 3) transmitting inaccurate information, and 4) violating privacy rights	Legal and societal problems associated with each technology should be assessed before adopting them. Four case studies are identified and discussed to address the four problems of misuse, i.e., Airline Tariff Recording System, Microsoft, TRW, and Blockbuster Video.
Culnan (1995)	Study of consumer awareness of name removal procedures from mailing lists.	Study focuses on the use of secondary information – information that is collected for one purpose is reused for another purpose – by firms. Privacy issues concerning secondary information are examined in terms of the fair information practices: notice, choice, access, security, and enforcement.	Consumers who are unaware of name removal procedures tend to be young, poor, less educated, African-American, mail shoppers, and less likely to be concerned about privacy than consumers who are aware of name removal procedures.
Taylor, Vassar, and Vaught (1995)	Study of the beliefs of marketing professionals regarding consumer privacy.	Issues addressed include: 1) differences of beliefs regarding privacy between marketers and consumers, 2) differences between different marketing groups, and 3) beliefs of marketers regarding automatic number identification (ANI).	Marketers and consumers differed significantly in terms of the role government should play in the regulation of privacy. Direct marketers find it more unacceptable to buy and sell consumers' information without consent than members of AMA and purchasing managers. Most marketers believed that the use of ANI without consent is unethical and an invasion of privacy.
Lally (1996)	Study of the conflicting rights of accessibility and privacy.	The article proposes that situationally conditioned belief (SCB), or the role an individual plays in the decision making process, explains the conflict between rights of privacy and accessibility.	Situationally conditioned beliefs (SCB) cause a difference in beliefs about information accessibility and privacy. A technique called information exchange is proposed as a way of closing the SCB gap in business and market transactions.

Campbell (1997)	Comparison of direct marketers and consumer attitudes about information privacy.	Information privacy is defined as the ability of individuals to determine the nature and extent of information about them which is being communicated to others. Three important aspects of information privacy include errors, collection, and unauthorized access/ use.	While both marketers and consumers are concerned about the uses of consumer information, they tend to focus on different aspects of information privacy. Consumers focus on potential abuses of their information by marketers, whereas marketers focus on the potential benefits to consumers from better targeting.
Nowak and Phelps (1997)	Development of a framework for addressing privacy concerns that arise when direct marketers use individual-level consumer information.	Analysis of Prosser's four torts of privacy (intrusion, disclosure, false light, and appropriation) suggests that most direct marketing collection and use of consumer information is not illegal. Consumer privacy concerns correspond with individual-level information as well as consumer knowledge and control.	Increasing consumers' information knowledge and control reduces the significance of privacy related issues. Direct marketers should routinely inform consumers when individual-specific information is collected, how the information will be used, and who will have access to the data. By doing so, consumers' appropriation, disclosure, and false light concerns would be diminished, while the accuracy of marketers' database would be enhanced.
Thomas and Maurer (1997)	Examination of why consumer information in commercial marketing databases is not likely to receive privacy protection.	Sources of consumer data: public, transactional, and long-term commercial relationships. Four primary uses of consumer data: commercial, decision support, lifestyle, and criminal/fraudulent.	Privacy protection requires legislation. There is no competitive incentive for firms to protect consumer privacy. This is due to the fact that the interests of the parties to a sale of database information are asymmetrical. Likewise, database agencies are unlikely to enhance consumer privacy because such actions are costly and produce no increase in value.
Sheehan and Hoy (1999)	Examination of online users' responses to privacy concerns	Seven possible online responses to privacy concerns: 1) not registering with websites, 2) providing incomplete information, 3) providing inaccurate information, 4) notifying Internet providers, 5) requesting name removal, 6) sending a "flame," and 7) not reading unsolicited email.	Correlations were found between online privacy concerns and hypothesized behaviors. As privacy concerns increase, respondents were more likely to provide incomplete information, complain to ISPs, request to be removed from mailing lists, and send a negative message ("flame") to unsolicited online messengers.
Culnan and Armstrong (1999)	Examination of the role of procedural fairness in addressing privacy concerns.	Procedural justice refers to the perception by the individual that a particular activity in which they are a participant is conducted fairly.	Procedural justice is an intermediary to building trust with customers. Customers are willing to disclose personal information when there are fair procedures in place to protect privacy.
Introna and Pouloudi (1999)	Examination of the social dimensions of privacy on stakeholders' interests and values.	Development of a framework that explores the interrelationship of privacy interests and values of various stakeholders. Analysis based on three principles: 1) access principle, 2) representation principle, and 3) power principle.	It is impossible for stakeholders to separate their interests and values when making privacy judgments (i.e., access principle). When claims of privacy/transparency are considered, all stakeholders must be present (i.e., representation principle). All stakeholders ought to be able to have equal power when making claims of privacy/transparency (i.e., power principle).

Milne and Boza (1999)	Study of how improving trust and reducing concern have distinct effects on managing consumer information.	Study focuses on the role of trust and concern in database marketing. Antecedents of trust and control include perceived control, knowledge, and attitude toward relationship marketing.	Building trust is more effective than trying to reduce consumer concern. Consumers who trust their organizations attribute it to experience, reputation, contractual issues, and regulation.
Sheehan (1999)	Examination of gender differences in attitudes and behaviors toward marketing practices involving information gathering and online privacy.	Gender differences are examined in terms of attitudes towards five dimensions of privacy concern (i.e., awareness of data collection, information use, information sensitivity, familiarity with the entity, and compensation) and behaviors including reading unsolicited e-mail, notifying ISP, requesting name removal, sending a flame, and providing incomplete information.	Gender differences were found in attitudes toward privacy. Women are more concerned than men about the impact of information gathering on privacy. When men do become concerned, they are more likely to adopt protective behaviors than women.
Caudill and Murphy (2000)	Examination of legal and ethical issues of consumer online privacy.	Consumer personal information consists of both public and private information. Ethical approaches to online privacy include social contract theory, duty-based theory, and virtue ethics.	What is considered public information is growing and what is considered private information is shrinking with the increase use of the Internet. Ethically, power and responsibility should be in equilibrium. Whichever party has more power has the responsibility to ensure trust and confidence in the other party.
Culnan (2000)	Study of 361 commercial Web sites to determine the extent to which self-regulation is working to protect consumer privacy online.	Self-regulation is based on legislation, enforcement, and adjudication carried out by the private sector rather than the government. Personal information includes information that both can and cannot identify the individual. Privacy disclosures include privacy policy notices and information practice statements.	It was found that 92.8% of the Web sites studied collected some form of personal information. Almost 66% posted some type of privacy disclosure. Of the Web sites that collected personal information, 89.9% include one element of notice, 61.9% contained one element of choice, 40.3% contained one element of access, 45.8% contained one element of security. Only 13.6% contained all five elements.
Milberg, Smith, and Burke (2000)	Development of a multinational approach to understanding information privacy.	Things that affect privacy issues and concerns across countries include cultural values, regulatory approaches, corporate privacy management styles, privacy problems, and regulatory preferences.	A country's regulations concerning consumer privacy are affected by its cultural values. Self-regulation of privacy by firms may not be a sustainable model over time.
Milne (2000)	Explanation of a privacy research framework for academic research on consumer privacy.	The privacy research framework consists of four factors: 1) marketer influences, 2) marketer information strategy, 3) consumer information behavior, and 4) consumer influences.	Privacy is a concern in four marketer-consumer information interactions: 1) information requests and disclosure, 2) information provision, 3) information capturing without consent, and 4) information uses. Giving consumers more knowledge and control over information exchanges provides greater privacy protection.

Milne and Rohm (2000)	Survey of consumer awareness and knowledge of name removal mechanisms across direct marketing channels.	Four factors related to name removal include 1) purchase context, 2) consumer background, 3) customer satisfaction, and 4) situational variables.	Preference for name removal varied by direct channel type, consumer privacy state, channel-specific purchase experience, and consumer demographics. The study also found that despite self-regulation, many consumers are neither aware of data collection efforts nor knowledgeable or name removal mechanisms.
Miyazaki and Fernandez (2000)	Content analysis of online retail privacy and security disclosures of 381 commercial Web sites in 17 product categories.	Online privacy concerns include customer identification, unsolicited contacts, and distribution of customer information. Online security concerns include secure transactions, financial data security, and alternative payment options.	Results indicate that only 23% of the sites offered some type of customer identification policy, 33% offered an unsolicited contact policy, and 29% offered an information sharing policy. In terms of security, 50% offered secure transactions, 6% offered a security guarantee, and 48% offered alternative ordering processes. An additional consumer survey found a positive relationship between online privacy/security statements and consumer purchase behavior.
Petty (2000)	Examination of how the collection of consumer information imposes costs on consumers.	Consumer-borne marketing costs (CBMCs) include contact costs and reliance costs, as well as pecuniary and non-pecuniary costs.	Privacy includes the right to be free from unwanted marketing solicitations because of the costs that they impose. Privacy, as well as economic efficiency, would be enhanced by requiring marketers to internalize the consumer costs of collecting and using consumer information.
Phelps, Nowak, and Ferrell (2000)	Examination of the types of personal information, the benefits of providing this information, factors that affect information sharing, and the tradeoffs consumers make in exchange for their information.	Study identifies five types of information: demographic, lifestyle, shopping behavior, financial, and personal identifiers. Model for understanding consumer privacy concerns includes type of information, amount of control, consequences/benefits, consumer characteristics, beliefs about marketers' information practices, and consumer concern.	On average, consumers are more willing to provide firms demographic and lifestyle information and less willing to provide financial and personal identifiers. 45% of respondents were very concerned about the use of their information by firms and the vast majority desire more control over what firms do with their information. It was also found that there is a positive relationship between information control and purchase intentions.
Sheehan and Hoy (2000)	Survey of online consumers' attitudes toward online privacy.	Fair information practices (FIPs) include notice, choice, access, security, and redress. Other dimensions that are important include how sensitive the person considers the information, how familiar the person is with the collecting entity, and what compensation is offered in exchange for the information.	The fair information practices address many of online consumers' privacy concerns. It was also found that privacy concerns vary by the context, that established relationships between the firm and the customer lessen privacy concerns, and that online customers try to balance the information they give with what is being received.
Phelps, D'Souza, and Nowak (2001)	Examination of the interrelationships between antecedents and consequences of consumer privacy concerns.	The two antecedents of consumer privacy concerns examined are information control and consumers' attitudes toward direct marketers. The two consequences of privacy concerns examined include purchase decision making and purchase behavior.	Consumers' attitudes towards direct marketing are negatively related to privacy concerns and the desire for information control is positively related to privacy concerns. In turn, privacy concerns are negatively related to the purchase decision process and purchase behavior.

Carroll (2002)	Analysis of whether bankrupt Internet companies can sell private consumer information to pay off debt.	Study examines consumer privacy in terms of Chapter 7 and Chapter 11 bankruptcy protection law and the commercial interests of creditors versus the privacy interests of consumers.	There are no specific laws prohibiting such sales. Advice for solvent Internet companies: provide explicit details outlining the sale of consumers' personal information, adhere to the privacy policies, and hire privacy officers.
Charters (2002)	Analysis of the ethics of electronic monitoring of consumers and the implications of this practice for consumer privacy.	Electronic monitoring is defined as the use of "cookies," or small data structures placed on a person's computer, to collect and store information about consumers. These cookies allow marketers to develop profiles of consumers and to monitor and track their online behavior.	Although electronic monitoring always constitutes an invasion of privacy, it can be ethically justified using both Utilitarian and Kantian ethical theories. Despite this, it is recommended that the industry move to a user control model in electronic monitoring.
Milne and Culnan (2002)	Longitudinal analysis (1998-2001) of online privacy studies.	Analysis of the data from four U.S. web surveys was used to determine the degree to which the online posting of privacy policies and compliance with the fair information practices (FIPs) has changed over time.	The number of Web sites that posted privacy policies increased from 1998 to 2001, though the posting of information practices decreased in 2001. The number of Web sites that provided the FIPs of notice, choice, and security increased over the four years. Although the data was incomplete, the number of Web sites that provided access appeared to decrease. It was also found that the more popular Web sites were more likely to post privacy disclosures based on the FIPs than the general population of web sites.
Rust, Kannan, and Peng (2002)	Development of an economic model to project the erosion of consumer privacy.	The economic model of privacy is based on six assumptions: 1) technology is advancing, 2) the cost of obtaining and processing information will decline, 3) consumers have an ideal level of privacy, 4) companies may offer to sell privacy protection, 5) each unit of privacy sold is a unit of information not possessed by the firm, and 6) information will only be sold in with its value exceeds its cost.	As the cost of obtaining and processing information decreases, the amount of privacy will decline over time and privacy will be increasingly expensive to maintain. Although a market for privacy will emerge, enabling customers to purchase a certain degree of privacy, the overall amount of privacy and privacy-based customer utility will continue to erode.
Culnan and Bies (2003)	Development of justice theory framework to explain how consumer privacy concerns are shaped by the perceived fairness of a firm's information practices.	A major issue is who should control personal information about the consumer. Information privacy is defined as the ability of individuals to control the terms under which their personal information is acquired and used. Personal information is defined as information identifiable to the individual. A "second exchange," in which consumers make non-monetary exchange of their personal information for some value received, is at the heart of the flow of personal information.	Creating willingness in consumers to disclose personal information requires an exchange based on a fair social contract. Fairness is evaluated by the consumer in terms of distributive, procedural, and interactional justice. One way to provide a fair social contract is to follow the fair information practices (FIPs), which balance consumer privacy concerns and firms' ability to operate efficiently in the marketplace.

Dommeyer and Gross (2003)	Examination of consumer knowledge of privacy-related laws, and consumer awareness and use of privacy protection strategies.	Development of knowledge, awareness, and protection scales. Measurement of effects of gender, age, phone number listing status, and attitude towards direct marketing solicitation on awareness and use of privacy protection strategies.	Consumers were found to have very little knowledge of direct marketing practices and regulations. While consumers were fairly well informed on privacy protection strategies, their use was quite low. Males and younger people are more likely to be aware of privacy protection strategies. Young people, along with those who had a negative attitude towards direct marketing solicitations, were most likely to use privacy protection strategies.
Hoy and Phelps (2003)	Content analysis of 102 nonprofit Christian church Web sites with a focus on privacy and security issues.	Church Web sites were analyzed in terms of the FIPs: notice, choice, access, security, and disclosure.	The vast majority (99%) of church Web sites collected personal identifying information (including that of children and teenagers), but only 3% posted a privacy policy. I was also found that only 36% collected information over a secure server, 13% provided notice, and 2% provided some form of choice. The results show that nonprofit church Web sites provide significantly less privacy protection than do commercial Web sites. In addition, these sites often post more personally identifying information than commercial Web sites.
O'Connor (2003)	Content analysis of the privacy policies of the 30 largest international hotel brands.	Study examines the compliance of international hotel privacy policies with a broad set of global privacy protection principles: notice, choice, onward transfer, access, security, integrity, and enforcement.	Analysis of the privacy policies of the 30 largest international hotels revealed that only 25% fully complied with the global privacy protection principles, 69% partially complied, and only 7% failed to comply with any of the principles. Omissions were found mostly in terms of choice, security, and integrity.
Sarathy and Robertson (2003)	Development of a framework to explain the factors that influence the privacy protection provided by firms.	The framework incorporates four main factors: precursors (e.g., national culture and global trends), external factors (e.g., legislation and type of data), ethical framework (e.g., egoism, relativism, utilitarianism), and firm factors (e.g., age, experience, profit/non-profit).	Privacy strategy should be arrived at by considering a multiplicity of factors. While the firm's ethical framework is important, environmental context and firm factors should also be considered. Likewise, the firm should listen to and incorporate concerns of their customers, the government, and society. The final privacy protection strategy should be both ethical and pragmatic, and tailored to the firm's specific context and situation.
Milne and Culnan (2004)	Examination of why consumers read (or do not read) online privacy notices.	Study examines the role of concern, comprehension, demographics, trust and experience on the reading of online privacy notices.	Reading online privacy notices is related to privacy concern, positive perceptions about notice comprehension, and higher levels of trust in the notice. Reading privacy notices is one way that consumers manage the risk of disclosing personal information online.

Zwick and Dholakia (2004)	Explanation of consumer online identities and how consumers can maintain a sense of control over their identities and privacy in the age of database marketing.	Based on poststructuralist theory, digital representations, or consumers as a set of data points, are argued to constitute total consumer identity. The digital consumer is no longer entirely anonymous or private.	Current consumer strategies (i.e., identifiability, anonymity/pseudonymity, confidentiality, and secrecy) of exerting control over their identities and privacy in the electronic marketplace are ineffective. These strategies are based that the consumer self is ontologically distinct from its digital representation. In the electronic age, the consumer does not exist outside the language governing the electronic marketspace. Consumers can only regain control over their identities if they are given direct access to companies' customer databases.
Pollach (2005)	Examination of privacy policies from a linguistic perspective to determine whether they adequately enable informed consent.	The study explores the interests of key stakeholders in online privacy, examines data handling techniques in terms of various ethical theories, and presents the findings of a critical linguistic analysis of privacy policies.	Corporate privacy policies obfuscate, enhance unethical data handling practices, and use persuasive appeals to influence consumers' trust in the company. Privacy policies need to be written in a more transparent and responsible manner.
Sheehan (2005)	Content analysis of the privacy policies of direct-to-consumer (DTC) branded drug Web sites. The study also examines the "readability" of these privacy policies.	DTC drug online privacy policies were analyzed in terms of the FIPs: notice, choice, access, and security. The FDA encourages these DTC Web sites to follow the FIPs.	The vast majority (94%) of DTC drug sites posted a link to a privacy policy/statement. Although most of the sites provided notice, they had poor compliance with the other three. The average readability score of the privacy policies was far above the suggested eight-grade level. Despite this, many of the visitors tried to read the privacy policies before providing information to DTC drug Web sites.
Ashworth and Free (2006)	Application of theories of justice to understand consumer's online privacy concerns.	A model of online marketing is presented that views the collection and dissemination of consumer information as a form of exchange. Fairness in this information exchange is analyzed in terms of distributive and procedural justice.	Theories of procedural and distributive justice suggest that consumers respond to perceived privacy violations as being similar to an unfair exchange. In terms of distributive justice, consumers are likely to evaluate the fairness of an information exchange in terms of the distribution of outcomes. In terms of procedural justice, consumers are likely to judge the manner in which they are treated in determining how much information to provide in the exchange.
Bowie and Jamal (2006)	Examination of the debate on self-regulation versus state-regulation of privacy rights.	Issues examined include the philosophical justifications for a right to privacy, FIP criteria for good privacy policies, comparison of e-commerce privacy laws between the EU and the US, web seals (such as TRUSTe), and choice consent policies (e.g., opt-in and opt-out).	The use of web seals by firms has been effective in signaling privacy protection to online consumers. In order for privacy seals to be most effective, they should follow certain minimum standards for privacy protection. Formal state mandated privacy regulation is not recommended.

Eastlick, Lotz, and Warrington (2006)	Examination of consumers' privacy concerns and perceived e-tailer's reputation on consumer trust, commitment, and purchase intention.	A research model of information privacy was used to examine the hypotheses that consumers' privacy concerns impact their online purchase intentions directly and indirectly through trust and commitment and that information choice strategies impact privacy concerns and trust.	Results showed that privacy concerns influenced purchase intent with strong negative effects, both directly and indirectly through trust. No effect of choice strategies on privacy concerns were found, nor was it found that choice strategies moderated the effect of reputation on privacy concerns or trust.
Milne, Culnan, and Green (2006)	Longitudinal assessment of the readability of 312 online privacy notices.	Readability was measured primarily with the Flesch-Kincaid grade level and the Flesch reading ease formula.	Results indicate that the readability level of privacy policies had increased between 2001 and 2003. The average length of the notices increased by more than 500 words between 2001 and 2003. In 2003, it was found that the longer notices were also less readable. The findings also showed that privacy notices with privacy seals are more readable than those without privacy seals, and that the average reading level of privacy policies increased over time across industry sectors.
Lwin, Wirtz, and Williams (2007)	Examination of consumer online privacy concerns and responses.	The Power-Responsibility Equilibrium (PRE) framework was used to examine how consumers' actions are influenced by corporate policy and governmental regulations at the macro level.	Results from two experiments indicate that 1) the weaker the perceived company privacy policy, the higher the degree of privacy concern and use of protective strategies, 2) the weaker the perceived government online privacy regulation, the higher the degree of privacy concern and use of protective strategies, 3) a strong company privacy policy is effective in reducing consumer privacy concern when low sensitivity data is collected, but insufficient when high sensitivity data is collected, and 4) consumer privacy concern increased dramatically when the collection of sensitive data was inconsistent with the business context.

Conceptualizations of Consumer Privacy

As with the general notion of privacy, consumer privacy is an abstract concept that encompasses many different aspects and concerns. However, despite the persistent ambiguity and evolution of the notion of consumer privacy in the literature, it still remains an important issue and one that must be understood in order to manage the relationship between consumers and firms effectively.

Definition of Consumer Privacy – Initial attempts to define consumer privacy build upon the early definition of privacy as the right to be left alone and the later conceptualizations of privacy as control over social encounters and personal information. For instance, Goodwin (1991) defines consumer privacy as "the consumer's ability to control (a) presence of other people in the environment during a market transaction or consumption behavior and (b) dissemination of information related to or provided during such transactions or behaviors to those who were not present" (p.152). The first part of the definition focuses on the social aspects of consumer privacy and deals with control over the presence of others in the consumer's environment. Specifically, this part of the definition pertains primarily to intrusions by marketers (via telephone, mail, person, etc.) into the consumer's environment, though it could include the presence of other consumers in the market environment (Milne and Gordon 1993).

The second part of the definition focuses on the information aspects of consumer privacy and deals with consumer control over the information they provide to firms (Jones 1991). Specifically, this part of the definition pertains to marketers' use of consumer information, especially uses that go beyond the intent of the original disclosure.

Privacy based on these two types of control (i.e., social control and information control) give rise to four privacy states: 1) total control, 2) environmental control, 3) disclosure control, and 4) no control (Goodwin 1991). Total control represents situations in which consumers maintain control over both the presence of others in the environment and use of their personal information. This situation represents the highest degree of privacy and requires the least amount of privacy protection (Goodwin 1991). Environmental control represents situations in which consumers control the presence of others in the environment, but do not maintain control over the use of their personal information. Disclosure control represents situations in which consumers maintain control over the use of their personal information, but not the presence of others in the environment. Both of these conditions represent moderate amounts of privacy and require some privacy protection (Goodwin 1991). No control represents situations in which consumers control neither the presence of others in their environment nor the use of their personal information. This represents the lowest degree of privacy and requires the most amount of privacy protection (Goodwin 1991).

This early definition of consumer privacy based primarily on control has been expanded to include consumer knowledge as a second primary dimension (Culnan 1995: Foxman and Kilcoyne 1993; Nowak and Phelps 1997). Consumer knowledge refers to the degree to which consumers are informed about, as well as understand, the information practices of firms in which they interact and their privacy rights in regards to these interactions (Foxman and Kilcoyne 1993). Consumer knowledge, thus, incorporates a number of issues in the realm of consumer privacy. First, do consumers understand what information is collected, how it is collected, and why it is collected? Second, do consumers understand how the information will be used, especially beyond its original use (i.e., the secondary use of information)? Third, do consumers understand their rights (i.e., the actions they can and cannot take) in regards to the collection and use of their information? Consumer privacy is considered high when the answers are affirmative to all of these questions and low when they are negative (Foxman and Kilcoyne 1993; Nowak and Phelps 1997).

Consumer Privacy Rights – As with both the general nature of privacy and perceived privacy rights, consumer privacy is typically not considered an absolute right (Clark 1978; Friedrich 1971; Gavison 1980; Simitis 1987). There are three main arguments as to why consumer privacy is not an absolute right. First, consumers' right to privacy often conflicts with other rights and concerns (Borna and Avila 1999; Milne and Gordon 1993). Second, what constitutes consumer privacy is affected by cultural, situational, and individual factors (Milberg, Smith, and Burke 2000; Smith 2001). Third, consumers and firms maintain competing views over information ownership (Foxman and Kilcoyne 1993; Nowak and Phelps 1992).

In terms of the first argument of competing rights, Goodwin (1991) identifies four sources of conflict with consumer privacy rights: 1) conflicts between consumer privacy and desired service levels, 2) conflicts between consumer privacy and other consumer and marketer rights, 3) conflicts between the consumer privacy and the cost of privacy protection, and 4) conflicts between consumer privacy and other societal values. First, it has been found that consumers are often willing to sacrifice their privacy in order to receive higher levels of service, though they do try to minimize the amount information they provide (Katz and Tassone 1990; Posch 1988; Stone and Stone 1990). Second, it has been found that the desire for consumer privacy often conflicts with consumers' rights to be informed and freedom of choice, as well as with marketers' rights to be left alone and free speech (Clark 1978; Lally 1996; Rasor 1986). Third, it has been found that while consumers demand higher levels of privacy protection, they are unwilling to pay for this protection (Jones 1991; Milne and Gordon 1993). Fourth, societies require a certain amount of surveillance in order to maintain their proper functioning (Flaherty 1989; Westin 1967). As such, consumer privacy will likely be sacrificed if it is perceived to interfere with the greater social good, such as threats to safety, health, and the economy (Etzioni 1999; McWhirter and Bible 1992; Moore 1984). This is evident in the reporting of consumers who make unusually large purchases of fertilizer chemicals that could be used to make explosive devices such as the one use in the Oklahoma City bombing.

The second reason why consumer privacy is not considered an absolute right is that it is often affected by cultural, social, and individual factors (Johnson 1989; Milberg et al. 2000). The culture of a particular country or society broadly influences what individuals consider private (Altman 1977; Schein 1977; Smith 2001). Privacy interests often vary in terms of the degree of autonomy, confidentiality, intimacy, accessibility, and anonymity sought by individuals, organizations, and even governments (Flaherty 1989). What a particular country or society emphasizes as distinctly private will depend on its history, economy, and social structures (Milberg et al. 2000; Smith 1994; Vogel 1992). This is evident in the large differences in the type and degree of consumer privacy protection required by the U.S. Government and the Europian Union (Pincus and Rogers 1997; Sarathy and Robertson 2003; Scheibal and Gladstode 2000).

The third reason why consumer privacy is not considered an absolute right is that there are often competing claims by consumers and marketers concerning information ownership (Foxman and Kilcoyne 1993; Milne and Gordon 1993; Nowak and Phelps 1992). As we saw in the previous section, issues of consumer privacy often focus on control over personal information. At the heart of this issue of control is the notion of information rights. Unfortunately, consumers and marketers often disagree over who maintains the rights to the information provided in an exchange (Foxman and Kilcoyne 1993). Most consumers perceive that the information they provide in a commercial transaction belongs to them, whereas marketers and firms perceive that the information, once given, belongs to the organization (Cespedes and Smith 1993; Nowak and Phelps 1992). These competing claims make it difficult to manage the conflicting rights to privacy claimed by both consumers and firms. For instance, one researcher analyzed whether bankrupt Internet companies can sell private consumer information to pay off their debt and found an absence of specific laws prohibiting such a sale (Carroll 2002). In this case, the commercial interests of creditors clashed with the privacy concerns of consumers, bringing to light the question of information ownership and the difficulty of managing privacy rights.

The Ethics of Consumer Privacy – Because privacy has a strong normative component to it, it is not surprising that researchers have also examined the ethical dimensions of consumer privacy (Ashworth and Free 2006; Caudill and Murphy 2000; Foxman and Kilcoyne 1993). Consumer privacy has been examined in the literature from a number of ethical perspectives including utilitarianism, egoism, relativism, justice, duty, virtue, and social contract theory. In this section, we briefly summarize the findings of the ethical studies of consumer privacy.

Teleological and deontological ethical theories (including utilitarianism, ethical egoism, and ethical formalism) have been used to explain the conflicts that arise between consumers and firms in the collection and use of transactional data (Foxman and Kilcoyne 1993). Firms often justify their use of consumer information on utilitarian grounds by arguing that the collection and analysis of this information will provide greater benefits to consumers as a whole, such as better targeting, higher quality service, and lower prices (Milne and Gordon 1993). From an ethical perspective, there are two problems with this argument. First, firms often benefit more than consumers from the use of this information, as the 1973 supervisory committee found (see above), which may cause firms to ignore or incorrectly estimate the utility of their actions in order to fulfill their egoistic needs. Second, the fact that consumers are often unknowledgeable of a firm's information practices denies them their deontological rights of respect and autonomy (Dommeyer and Gross 2003; Foxman and Kilcoyne 1993; Milne and Rohm 2000).

It has been argued that these problems that arise in the collection and use of consumer information cannot be reconciled simply by a utilitarian justification, but require the application of a deontological ethical theory such as Kant's categorical imperative, which considers an act to be moral if it can be universalized to all people and situations (Kant 1959). Under this approach, both consumers and firms would have to accept the rights and protections that they demand of the other party, with the implication that this can only take place under the condition where there is control and knowledge by both parties (Foxman and Kilcoyne 1993; Nowak and Phelps 1997). Another study, though, has argued that firms' can justify electronic monitoring of consumers' online behavior on both utilitarian and deontological grounds (Charters 2002). As long as the firm focuses on the utilitarian goal of minimizing potential consumer harm and the deontological goal of respecting individual autonomy by providing consumers with enough information to make their own decisions, the firm is behaving ethically in terms of con-

sumers' right to privacy (Charters 2002). For example, while some scholars argue that firms need to offer consumers both a detailed privacy statement and full control over their personal information for the firms' privacy practices to be ethical, others argue that a detailed privacy statement is all that is ethically required by firms for consumers to make an informed choice. Either way, for consumer privacy practices to be considered ethical, there needs to be both knowledge and control on the part of consumers regarding the collection and use of their personal information, though there is clearly still some debate concerning the proper amount of knowledge and control that firms need to provide.

Social contract theory, or the idea that individuals enter into reciprocal relationships based on a form of equitable exchange (Dunfee, Smith, and Ross 1999), has also been applied to consumer privacy in order to explain the perceived trade-offs that are made between consumers and firms in the exchange of consumer information (Culnan 1995; Milne and Gordon 1993). It has been argued that when consumers provide firms with personal information in order to receive some form of benefit, they enter into an implied social contract with the firm (Milne and Gordon 1993). The result of this social contract is that consumers are often willing to sacrifice some of their privacy in exchange for something of value, subject to a "privacy calculus" in which they perform a personal cost/benefit analysis (Cespedes and Smith 1993; Culnan and Armstrong 1999; Laufer and Wolfe 1977). These social contracts, however, are only ethical when consumers understand the terms and conditions underlying these social contracts, as well as the actual costs and benefits that can accrue from the exchange relationship (Culnan 1995; Milne and Gordon 1993). This can only be achieved when there is consumer knowledge and control over the exchange of their personal information.

Justice theory has been applied to consumer privacy in order to explain consumers' perceptions of ethical fairness in the exchange relationship (Ashworth and Free 2006; Culnan and Armstrong 1999; Culnan and Bies 2003; Sarathy and Robertson 2003). Three types of justice that have been examined in the consumer privacy literature include distributive justice (i.e., the evaluation of outcomes or results), procedural justice (i.e., the evaluation of the processes and activities that lead to the outcomes), and interactional justice (i.e., the evaluation of the communication process) (Culnan and Bies 2003; Sarathy and Robertson 2003). In terms of distributive justice, it has been argued that consumers must feel that the value they receive from a firm is commensurate with the personal information they provide in order for the exchange to be considered ethical (Ashworth and Free 2006). This is similar to equity theory in which fairness is based on a comparison of inputs and outputs in the exchange relationship (Adams 1965). It has been suggested that factors such as information sensitivity, data usage, and compensation impact perceptions of distributive justice because they influence consumers' evaluation of both the inputs and outputs of the exchange relationship (Ashworth and Free 2006). For example, if consumers consider the information that they provide to firms as very sensitive, then they must feel that the inputs the firm provides (e.g., data security) and the outputs they receive (e.g., financing) are worth the risk for this to be an ethical exchange.

In terms of procedural justice, it has been argued that consumers are usually willing to disclose personal information and allow this information to be used by a firm when they perceive fair information practices in place to protect their privacy (Culnan and Armstrong 1999). It has also been suggested that awareness is the primary factor that affects perceptions of procedural justice because it directly impacts consumers' evaluations of the information practices of a firm and their ability to exercise control over the exchange relationship (Ashworth and Free 2006). That is, consumers must not only be aware of the information practices of a firm, but they must be provided with enough information to make a reasonable assessment of these practices and an informed choice concerning their personal information for there to be procedural justice. In addition, firms cannot merely enumerate any type of information practices in their privacy policies for there to be procedural justice, but must make sure that the information practices fairly balance the concerns of the firm with the concerns of the consumer (Culnan and Armstrong 1999).

Lastly, in terms of interactional justice, research has found that firms can build trust, and thus mitigate privacy fears, by communicating the fairness of their privacy practices to their customers (Culnan and Armstrong 1999). One way for firms to do this is try to understand the normative expectations of their customers and communicate their duties in regards to these expectations to their customers (Ashworth and Free 2006; Caudill and Murphy

2000). For example, firms should not simply provide a laundry list of information practices in their privacy policies, but should try to address consumers' privacy concerns by explaining the consumers' rights and the firms' obligations. By doing this, firms can move beyond simply establishing a contractual relationship and develop an ethical bond with their consumers that permeates the whole exchange relationship (Caudhill and Murphy 2000). While adherence to any or all of these three forms of justice can mitigate consumers' privacy concerns, it is suggested that violations of any of them will negatively impact consumers' ethical perceptions of the firm (Culnan and Bies 2003).

Consumer-Related Privacy Issues

The increased focus on the consumer and the demand for personal information in almost every business transaction has had a significant impact on consumers' sense of anxiety regarding their personal privacy. To grasp the breadth of consumers' privacy concerns, one needs to examine both the causes and the effects of these concerns, as well as the steps that consumers are taking to manage their privacy. In this section, we review the consumer privacy literature in terms of the antecedents, management, and consequences of consumer privacy concerns.

Consumer Privacy Concerns and their Antecedents – Scholars have identified five major influences on consumers' privacy concerns, viz. consumer awareness, information usage, information sensitivity, familiarity with the firm, and compensation (Phelps et al. 2000; Sheehan and Hoy 2000). In terms of consumer awareness, research suggests that consumers' privacy concerns are triggered when consumers become aware that firms have collected and/or used their personal information without their permission (Cespedes and Smith 1993). One of the most common ways that consumers become aware of these practices is when they receive unsolicited promotions related to recent transactions. Many firms are now offering opt-in or opt-out mechanisms that inform consumers of the firm's information practices and provide them with a choice of whether or not to participate (Milne and Rohm 2000). This is important because it has been found that consumers tend to be less concerned about their privacy when firms seek permission to collect and use their information (Nowak and Phelps 1995).

In terms of information usage, it has been found that consumers become concerned about their privacy when they do not know how their information is being used (Sheehan and Hoy 2000). Of primary concern to consumers is the secondary use of their information (Nowak and Phelps 1995). This is when consumer information obtained in the original transaction is used for purposes unrelated to the transaction or sold to other firms. Consumers often view this secondary use of their information, especially when they are not made aware of these practices, as a violation of their privacy (Cespedes and Smith 1993; Phelps et al. 2000; Wang and Petrison 1993). In addition, the amount of information control desired by consumers also has a bearing on the degree of privacy concern with regards to information usage (Campbell 1997; Culnan and Armstrong 1999). In the direct marketing context, it has been found that the greater the desire on the part of consumers for control over their personal information, the stronger is their concern to maintain their privacy rights (Phelps et al. 2001).

In terms of information sensitivity, it has been found that how sensitive the person considers the information has a impact on their privacy concerns (Sheehan and Hoy 2000). Information sensitivity refers to the degree to which individuals feel that their personal information, if released or shared with others, can harm them (Gandy 1993). The more sensitive the information, the more concerned the person will be about their privacy (Phelps et al. 2000). In general, not all information is regarded as the same. Consumers seem less concerned about the collection and usage of information related to demographic characteristics, purchase behavior, and lifestyle habits and more concerned about the collection and usage of financial data, medical records, and personal identifiers (e.g., social security numbers) (Phelps et al 2000; Sheehan and Hoy 2000; Vidmar and Flaherty 1985). In addition, information sensitivity often differs by individual and situation (Milne 1997; Nowak and Phelps 1992).

In terms of familiarity with the firm, research suggests that consumers' overall attitude towards a firm has a direct impact on their privacy concerns. In one study, it was found that as consumers' positive attitudes towards a firm's direct marketing practices increased, the degree of privacy concerns decreased (Phelps, D'Souza, and Nowak 2001). In another study of online privacy concerns, it was found that the nature of the relationship (i.e., short-term

vs. long-term) between the customer and firm directly influences what types of personal information were provided and the degree of control over the information sought by the consumer (Sheehan and Hoy 2000). A key aspect of familiarity with the firm is trust (Vidmar and Flaherty 1985). It has been found that consumers who trust the firm are less concerned about their privacy and more willing to provide personal information (Schoenbachler and Gordon 2002). Some of the ways for firms to signal trustworthiness include security disclosures, privacy disclosures, seals of approval, and awards from neutral sources (Wang, Beatty, and Foxx 2004).

In terms of compensation, it has been suggested that compensating consumers for sharing their personal information can have an impact on their privacy concerns (Goodwin 1991; Milne and Gordon 1993; Sheehan and Hoy 2000). At the heart of most privacy concerns is the trade-off between the benefits received and the costs incurred from disclosure of one's personal information (Laufer and Wolfe 1977; Westin 1967). Consumers place a value on their personal information and will only disclose this information if they feel that the benefit they receive outweighs costs of disclosure (Ashworth and Free 2006; Dunfee et al. 1999). For instance, research in the direct mail and online contexts suggest that consumers perform a cost/benefit analysis of all the factors related to any particular direct mail situation in order to assess privacy concerns (Caudhill and Murphy 2000; Goodwin 1991; Russell 1989). One way for firms to affect this equation is to provide benefits, in this case some form of compensation, specifically for the disclosure of information. In a conjoint study of the trade-offs among all the attributes associated with direct mail (i.e., volume, targeting, compensation, and permission), it was found that the compensation factor (i.e., consumers getting paid through coupons, rebates, discounts etc.) was the most important determinant of satisfaction (Milne and Gordon 1993).

In addition to the five general factors presented above, research has also examined how various demographic factors affect consumers' privacy concerns (Culnan 1995; Dommeyer and Gross 2003; Sheehan 1999). An examination of gender differences in attitudes and behaviors toward online privacy found that women generally are more concerned than men about the impact of information collection on their privacy (Sheehan 1999). Ironically, in terms of more specific online privacy behaviors, the same study found that women tend to read more unsolicited email than men, that women notify their Internet Service Provider (ISP) about unsolicited email less often than men, and that women register on websites more often than men, though it was found that women provide incomplete information more often than men (Sheehan 1999). Another study found that men, though, are more likely to provide false information online than women (Chen and Rea 2004). In addition, it was found that men tend to react more aggressively to perceived privacy violations than women and adopt a wider range of behaviors (such as complaining) when addressing privacy concerns (Sheehan 1999).

In another study that examined both gender and age on consumers' privacy concern, it was found that men are more likely to be aware of strategies to protect personal information than women, and that younger individuals are more aware of these strategies than older individuals (Dommeyer and Gross 2003). Thus, although women seem to be more concerned about the collection and use of their information than men, men appear to be more aware of strategies to protect their privacy, which may account for the lower concern. In addition to gender, it was found that younger individuals were more likely to employ strategies to protect their privacy than older individuals (Dommeyer and Gross). In a another study of consumer awareness of privacy protection procedures, it was found that those consumers who were most likely to be unaware of these procedures were more likely to be young, poor, less educated, and African-American (Culnan 1995). Lastly, it was found that people who had attended a vocational school or had some college were the most concerned about how companies used their personal information (51%), followed by high school graduates (46%) and then college graduates (36%) (Phelps et al. 2000).

Consumer Management of Privacy Concerns – The lack of comprehensive privacy regulation in the U.S. means that in most situations, consumers who have privacy concerns must take steps to manage their own privacy protection. Some consumer privacy protection strategies include reading privacy notices, providing incomplete or no information to firms (e.g., not filling out product registrations and/or establishing permanent online accounts), engaging in name removal (e.g., choosing opt-out arrangements), and exercising one's legal rights (Milne and Culnan 2004; Milne and Rohm 2000). Unfortunately, even when consumers take precautions to protect their pri-

vacy, once their information has been collected and disseminated, there is often little they can do to protect their personal information.

For consumers, self-management of privacy concerns begins with awareness and knowledge of marketing practices and privacy protection strategies (Culnan 1995; Nowak and Phelps 1992). Studies have noted that overall consumer knowledge of direct marketing practices and regulations, though, is very limited (Dommeyer and Gross 2003). In a national survey of over 1500 consumers who use direct mail to make purchases, Milne and Rohm (2000) found that only 34% of respondents could be classified as existing in a "privacy state" (defined as the condition in which the consumer is aware of a firm's information practices and privacy protection mechanisms). In a study of consumer awareness of name removal procedures, it was found that 52% of the public were not aware of a firm's name removal procedures (Culnan 1995). These results suggest that the limited knowledge of firms' information practices, coupled with the lack of comprehensive government regulation of consumer privacy, leaves consumers in a very vulnerable position with regards to the protection of their privacy by firms. As a result, it is up to the consumer to manage their own privacy protection.

Reading the contents of privacy notices is one way that consumers can increase their knowledge and manage their privacy concerns. Privacy notices can enhance the sense of control consumers feel they have and can help them decide whether or not to share personal information (Wang et al. 2004). One study on online privacy notices found that three factors that positively impact the tendency to read online privacy notices include consumer's concern for privacy, positive perceptions about notice comprehension, and higher levels of trust in the notice (Milne and Culnan 2004). In spite of this, a large majority of individuals do not look for or read privacy policies (Milne, Rohm, and Bahl 2004). Instead, many consumers rely on other heuristics to decipher privacy protection, such as third party privacy seals, brand reputation, or prior experience with the firm (Bowie and Jamal 2006). Interestingly, use of such alternative heuristics is found to be negatively associated with reading of privacy notices (Milne and Culnan 2004).

With the rise of identity theft, numerous strategies have been proposed to help consumers protect their privacy. Offline strategies include understanding information practices, monitoring your credit, protecting your mail, minimizing the amount of information you disclose, and protecting your social security number (FTC 2001). In a study of theft prevention practices by both a college student and non-student sample, it was found that both groups practice many of these offline strategies, but that few individuals in either group order yearly credit reports, ask merchants how they are going to use their personal information before they reveal it, or pick up new checks from the bank (Milne 2003). Other strategies that consumers can employ to protect their privacy online include utilizing secure websites, opting-out of third party information sharing, creating separate email accounts, encrypting email, and using anonymous browsing software (Center for Democracy and Technology 2003). In a study of online identity theft protection behavior, it was found that a majority of respondents utilized secure online forms, opt-out mechanisms, and separate personal email accounts, while less than a third cleared their computer's memory, encrypted their emails, or used anonymous Internet browsing software (Milne et al. 2004). In another study, it was found that there was a strong positive relationship between privacy concerns and online privacy protection behavior (Sheehan and Hoy 1999). As privacy concerns increased, consumers were more likely to provide incomplete information to websites, to complain to their ISP about unsolicited e-mail, request removal from mailing lists, and "flame" (i.e., sending a highly negative message) those entities sending unsolicited e-mail (Sheehan and Hoy 1999).

In addition, studies utilizing poststructuralist theory offer another perspective on how consumers manage their privacy (Zwick and Dholakia 2004). In order to protect their identities and personal information, consumers may or may not choose to represent themselves accurately to firms. Research has identified four approaches that consumers take to manage their online identities: 1) identifiability (i.e., disclosure of all personal information with high accuracy), 2) confidentiality (i.e., disclosure of highly accurate but restricted information), 3) secrecy (i.e., nondisclosure of information), and 4) anonymity/pseudonymity (i.e., disclosure of information that is inaccurate) (Zwick and Dholakia 2004). It is argued that the digital representation of the consumer (i.e., the identity that exists as bits of information about the consumer in firm's databases) constitutes the totality of a consumer's identity

for a firm. In effect, firms market their products and services to these digital representations and not to the physical reality of consumers. Therefore, for consumers the highest state of self-determination and control comes when firms, especially online firms like Amazon.com, provide full access to the content of their databases to consumers so they can craft their digital identity (Zwick and Dholakia 2004).

Consumer Privacy Concerns and their Consequences – If consumers' privacy concerns are not mitigated through self-management strategies or firm initiatives, they can have potentially negative consequences on consumers' attitudes and behaviors (Milne and Boza 1999; Phelps et al. 2001; Sheehan and Hoy 1999). In fact, the relationship between these negative consequences is often complex. For instance, in a study of direct marketing practices, it was found that consumers' negative attitudes towards a firm's information practices directly affected their trust in the firm and their purchase behaviors (Milne and Boza 1999). In another study of 477 U.S. households, researchers found that privacy concerns had a significant impact on online purchase intent, with the greatest negative impact being through its relationship with trust (Eastlick, Lotz, and Warrington 2006). Additionally, a national survey of 556 consumers found a significant negative relationship between privacy concerns and purchase behaviors (Phelps et al. 2001). Consumers who were highly concerned about their privacy demonstrated lower recency, frequency, and monetary value of catalog purchases (Phelps et al. 2001). Firms can mitigate these negative effects by signaling and building trust with the consumer, especially by exhibiting procedural justice through the use of fair information practices and privacy protection (Culnan and Armstrong 1999).

Not only do consumers' privacy concerns have a negative effect on purchase intentions and behaviors, but they can also have a devastating effect on consumers' willingness to provide information (Schoenbachler and Gordon 2002; Sheehan and Hoy 1999; Wang et al. 2004). This is extremely important because it cuts at the very heart of the market orientation approach that underlies most business practices today (Dolnicar and Jordaan 2007). In a national study of online users, it was found that as consumers' privacy concerns increased, the frequency with which they registered on websites decreased, the frequency with which they provided incomplete information increased, and the frequency in which they requested removal of their names from mailing lists increased (Sheehan and Hoy 1999). All of these consequences clearly have a negative impact on the ability of firms to collect information. Another study found that relieving consumers' privacy concerns leads to a higher willingness to disclose personal information (Wang et al. 2004). As mentioned previously, one major way to do this is to facilitate a sense of trust between the consumer and the firm. In a national study of 5,000 direct mail consumers, it was found that consumers' feeling of trust in a firm positively influences their willingness to share information (Schoenbachler and Gordon 2002). In fact, it has been found that establishing trust is more effective than addressing privacy concerns when managing consumer information (Milne and Boza 1999).

Firm-Related Privacy Issues

In addition to the literature on consumer-related privacy issues, researchers have also examined privacy from the perspective of the firm. In general, this firm-level research has addressed three main privacy issues: 1) the extent to which firms are following the fair information practices (FIPs) in their privacy policies/notices, 2) the legal and business challenges that firms face when dealing with consumer privacy protection, and 3) the various alternatives available to firms in order to manage and communicate consumer privacy protection while pursuing strategic and financial success in the marketplace.

Compliance with FIPs – In 1998, the FTC issued a report to the U.S. Congress that investigated the self-regulation of online privacy by commercial businesses (FTC 1998). In the report, the FTC argued that the protection of consumer privacy was necessary for consumers to participate in the online marketplace and for electronic commerce to reach its full potential. The FTC commissioned a study that analyzed the collection of personal information and compliance with the FIPs of over 1,400 online commercial websites. The FIPs were defined as notice/awareness, choice/consent, access/participation, integrity/security, and enforcement/redress (see the Appendix for full details on the FIPs). The results from the study indicated that although more than 85% of commercial websites collected some form of personal information, only 14% provided notice of their information practices, with only 2% doing so through a comprehensive privacy policy (FTC 1998). While a follow-up study in 2000

provided evidence that more firms were providing privacy statements/policies, the FTC concluded that more had to be done to encourage firms to self-regulate their privacy practices and ensure the adoption of the FIPs.

Independent studies have also been conducted that examine the adoption of the FIPs by firms both across and within industries. In a study that examined consumer privacy across industry sectors, Culnan (2000) found that 92.8% of commercial websites collect some form of personal information. Of those websites that posted a privacy disclosure, only 13.6% contained all five FIPs, and only 24.9% contained any four of the five elements. Unlike the 1998 FTC study, Culnan found that 89.8% contained at least one element of notice (Culnan 2000). In a four year (1998-2001) longitudinal study, Milne and Culnan (2002) examined changes in privacy policies, information practices, and FIP compliance for commercial online websites. They found that there were significant increases in all three of these categories. Specifically, they found that more firms were offering privacy policies, that the privacy policies contained more information on the firm's information practices, and that FIP compliance was increasing in the areas of notice, control, and security. Although the data for access were incomplete, the percentage of websites providing consumers with access to their data was significantly less than compliance with the other categories, suggesting that while the majority of firms are addressing the issue of consumer knowledge, they only partially address the issue of control (Foxman and Kilcoyne 1993; Milne and Culnan 2002).

Research has also examined FIP compliance within several different industry sectors. In the retail sector, Miyazaki and Fernandez (2000) found considerable differences in the privacy and security disclosures among online retailers in 17 different shopping categories. A study of Internet health related websites found that although close to 90% of the sites provided some form of notice of their information practices, less than 30% provided information about choice and security, and only 15% provided access (Sheehan 2005). In a study of the privacy policies of 35 Fortune e-50 firms, researchers evaluated the firms' privacy statements in terms of a range of FIP compliance (i.e., full, partial, or noncompliance) and found that the vast majority of firms only partially comply with all of the FIPs (Ryker et al. 2002). Another study that examined the range of compliance in the privacy policies of 30 of the largest international hotel websites revealed similar findings, with the majority of hotels only partially complying with the FIPs (O'Conner 2003). In the non-profit sector, a study of 102 Christian church web sites found that although the vast majority (99%) collected personal information (including information about children), only 36% provided security, only 13% provided notice, and only 2% provided some form of choice (Hoy and Phelps 2003).

The results of these studies suggest that while many firms are increasingly providing privacy policies, there still remains substantial variance in the content of their privacy policies, in their actual information practices, and in their level of FIP compliance. Although firms realize that their position on consumer privacy protection can affect their long-term customer relationships (Nowak and Phelps 1997; Schoenbachler and Gordon 2002), there is still little consistency among firms' privacy policies. Many firms have discovered that explicitly communicating a privacy policy can reduce consumers' fears of providing personal information and build trust in the exchange relationship (Andrade, Kalcheva, and Weitz 2002; Eastlick et al. 2006; Milne and Boza 1999). At the same time, many firms still craft their privacy policies to benefit and protect the firm first and address consumer privacy issues second (Nowak and Phelps 1997; Pollach 2005; Thomas and Maurer 1997).

Legal and Business Challenges – Most market-oriented programs are a two-way street. They can help create personalized communications, customized offerings, and higher levels of customer service only if consumers are willing to provide the firm more personal information (Rust et al. 2002). This poses a unique challenge for market-oriented firms: how to balance greater value delivery through the collection of customer information while addressing both the legal and personal concerns about consumer privacy (Nowak and Phelps 1997). On the legal front, in addition to complying with the FIPs, firms need to be aware of legislation specific to their industries and to their area of operation in the U.S. (Bloom, Milne, and Adler 1994). For instance, legislation exists in the health insurance industry (*Health Insurance Portability and Accountability Act*), credit reporting industry (*Fair Credit Reporting Act*), and telemarketing (*National Do Not Call Registry*). At the state level, a number of different laws exist to protect consumer privacy (Peslak 2005; Smith 2002). For instance, where California forbids using state-agency transaction information (such as auto or property registration), Maryland forbids asking for phone numbers of people when they sign credit card slips (Bloom et al. 1994). Firms also need to be aware of technology-

specific legislation. For instance, technologies such as Caller ID that enable firms to determine the name, address, credit card number, credit rating, past shopping behavior, etc. of the caller before answering the call, are permitted in states like California only if "blocking" (wherein the caller can disable the Caller ID mechanism) is allowed (Bloom et al. 1994). The challenge, therefore, is to *a priori* manage the strategic planning before launching products, services, technology, and customer data collection in a new market, so that lawsuits under privacy protection legislation can be avoided.

In addition to the potential legal pitfalls, privacy protection also poses unique business challenges for firms (e.g., how to best manage self-regulation of consumer privacy so as to deliver an optimal level of privacy protection without unduly restricting the business practices of the firm) (Bowie and Jamal 2006). How consumers perceive the firm's privacy protection efforts is critical to resolving this issue (Culnan and Bies 2003). Research suggests that if consumers do not perceive firms as adequately protecting their privacy, they will distrust self-regulation and prefer state intervention (Milberg et al. 2000). Other scholars argue that if privacy protection is left to the free market forces (assuming no government intervention), the amount of privacy will decline over time due to the fact that firms will find it increasingly expensive to maintain privacy (Jones 1991; Thomas and Maurer 1997; Rust et al. 2002). Therefore the business challenge is to create conditions so that self-regulation of privacy meets or exceeds the expectations of consumers while minimizing the costs of self-regulation for the firm.

Managing Privacy Protection – A growing body of literature addresses ways that firms can address privacy issues to not only abate consumer concerns, but also ensure corporate health. A framework has been proposed that suggests that firm-level factors (e.g., age, experience, profit/non-profit, public/private, and corporate culture) should be taken into consideration (in addition to historical, ethical, and legal factors) before arriving at a privacy protection strategy (Sarathy and Robertson 2002). Research suggests that these firm-level factors have a direct bearing on the degree and type of privacy protection offered by a firm. For instance, it is argued that for-profit businesses that are more information-driven, privately-held, and customer-oriented are more likely to be diligent about protecting privacy and ensuring long-term customer loyalty (Sarathy and Robertson 2002).

Various recommendations have been made to help firms better manage the self-regulation of consumer privacy protection. One recommendation is that firms should conduct a cost-benefit analysis, where the costs include the costs of compliance (i.e., costs of access to data, providing notice, getting consent, giving choice, etc.) against the benefits of additional revenue gains (Sarathy and Robertson 2002). The firm should pick a privacy strategy that aims to reduce the total cost of compliance (e.g., through effective database design) or be willing to compensate the consumer in exchange of more personal information (Milne and Gordon 1993; Sheehan and Hoy 2000). It is also recommended that firms should monitor the gains from the collection of consumer information (e.g., personalization and customization of marketing programs) and communicate these gains to the consumers. Importantly, if consumers do not perceive any gains or an increase in value from the firm's information collection practices, they are more likely to be concerned about providing the firm with personal information (Ashworth and Free 2006; Sarathy and Robertson 2002).

Another recommendation that is often mentioned as a precursor to effective self-regulation is the notion of the firm's trustworthiness (Culnan and Armstrong 1999; Milne and Boza 1999; Sarathy and Robertson 2002; Wang et al. 2004). Winning consumer trust is seen as a strong antecedent to conveying privacy protection to consumers. As mentioned above, research suggests that improving trust helps to reduce consumers' privacy concerns concerning the collection and analysis of personal information (Milne and Boza 1999). Results indicate that consumers who trust businesses attribute it to past experience, reputation, contractual information (i.e., firms clearly disclosing information practices), and regulation (Milne and Boza 1999). It has been suggested that firms can enhance consumer trust, especially in the context of privacy, by building stronger relationships with their customers, maintaining transparent privacy policies, providing fair information practices/procedures, restricting secondary use to consumer information, and signaling actions taken by the firm that serve consumers better (Campbell 1997; Culnan and Armstrong 1999; Milne and Boza 1999; Wang et al. 2004).

Communicating Privacy Protection – Articulating an explicit and transparent privacy policy is also seen as an important precursor to effective privacy protection by firms. Research has examined privacy policies from a linguistic perspective in order to determine if the language of these policies adequately conveys a firm's information practices so the person reading them can provide informed consent (Pollach 2005). Analysis shows that many corporate privacy policies are not very transparent and are often confusing to the reader. It has also been found that most firms use one of four communicative strategies when crafting a privacy policy: 1) mitigation and enhancement (i.e., firms mitigate the negative impact of certain actions and selectively enhance the qualities of other practices), 2) persuasive appeals (i.e., firms use rational and emotional appeals to show consumers that they are trustworthy and reliable), 3) obfuscation of reality (i.e., firms use the hedging technique of using confusing language to side-step privacy issues), and 4) relationship building (i.e., firms use language to emotionally involve readers in the discourse). It has been recommended that firms need to reconsider the unethical practices involved in crafting privacy statements and to revise the wording of their privacy policies in more transparent and responsible ways (Pollach 2005).

Other researchers have analyzed privacy policies in terms of their level of readability (Milne, Culnan, and Greene 2006; Sheehan 2005). Readability has been measured in terms of the grade level at which a privacy policy is written and ease of reading it (Flesch 1949). Because knowledge is a key dimension of consumer privacy and notice, or awareness of a firm's information practices, is one of the five FIPs that firms should follow, consumers should to be able to read and understand a firm's privacy policy in order to exercise their right to privacy. In a longitudinal study of 312 online privacy notices, it was found that the average readability level of privacy policies, as well as their length, had increased between 2001 and 2003 (Milne et al. 2006). Most of the privacy policies analyzed were written at a grade-level much higher than the U.S. national average. This may help to explain why many consumers do not read privacy policies and why their understanding of these policies and their rights remains quite low (Milne, Rohm, and Bahl 2004). In a study of direct-to-consumer drug web site privacy policies, it was found that readability of the policies (almost a twelfth grade-level) was far above the suggested eighth-grade level (Sheehan 2005). Given the sensitivity of medical/health-related information, though, it was found that most consumers still try to read these policies before transmitting personal information.

FUTURE RESEARCH DIRECTIONS

As evidenced by the literature review, research on consumer privacy has grown considerably in the past 20 years and has provided many insights to researchers, practitioners, and policy makers alike. While this research has made significant contributions towards highlighting consumer privacy as a critical business issue, it has addressed this phenomenon primarily from a social point of view and has focused less on developing consumer privacy from a theoretical and practitioner perspective (Margulis 2003). That is, the majority of research reviewed in this article examines consumers' attitudes and behaviors regarding privacy issues and the societal impact of firms' privacy policies and information practices through descriptive studies. Less research attention has been devoted to defining the domain of consumer privacy, operationalizing its various components, and testing the relationships between its antecedents and consequences. In addition, recent changes in information technology, social and cultural mores, and geopolitical policies have affected peoples' view of privacy, participation, and surveillance. In the first section, we propose various extensions to current literature that future consumer privacy research can take in order to develop a more theoretically-driven body of research that may possibly aid in the establishment of a theory of consumer privacy. In the second section, we discuss contemporary issues related to consumer privacy that merit attention in the academic literature.

Future Consumer Privacy Research: Theoretical Issues

In this section, we examine areas of future consumer privacy research that deal specifically with ways to strengthen the theoretical foundations of consumer privacy. These areas include the operationalization of consumer privacy, the examination of competing consumer privacy rights, the understanding of the ethics of consumer privacy,

and the strategy of consumer privacy. Existing research has laid the foundation on these topics, but considerable work still remains to achieving a comprehensive understanding of consumer privacy.

Operationalizing Consumer Privacy – Early work in consumer privacy focused on exploring the foundations of the general concept of privacy and developing and refining the notion of consumer privacy (e.g., Jones 1991). Although many philosophical and legal definitions of privacy have been explored in the literature, consumer privacy has been defined mainly in terms of two dimensions: 1) knowledge and 2) control (Foxman and Kilcoyne 1993; Goodwin 1991; Nowak and Phelps 1995). With much of the literature accepting these dimensions of consumer privacy, a clear operationalization of these components clearly deserves further research attention.

The task of operationalizing the dimensions of consumer privacy, though, is indeed complex. Interestingly, although most researchers define consumer privacy in terms of knowledge and control, they tend to measure consumer privacy protection in terms of the five FIPs (notice, access, control, security, and enforcement), as well as additional factors not covered by the FIPs (Culnan 2000; Hoy and Phelps 2003; Sheehan 2005). Although the FIPs were written in terms of protecting, rather than defining, consumer privacy, they do suggest that there may be more aspects to consumer privacy than those captured in the conventional definitions (Sheehan and Hoy 2000). Likewise, consumers' perceptions of their degree of knowledge and choice, rather than the actual existence of these dimensions, may impact consumers' overall privacy concerns (Eastlick et al. 2006). This suggests that the dimensions of consumer privacy may have to be expanded and operationalized in such a way as to capture both the objective and perceptual aspects of consumer privacy.

If consumer privacy researchers are going to continue to rely on the FIPs as the standard for evaluating consumer privacy protection, then it is also necessary to outline fully what the five FIPs entail. As originally crafted by the FTC (1998), each of the five FIPs encompasses a number of different dimensions (see Appendix). Unfortunately, much of the consumer privacy research has only focused on the broader categories of the FIPs when assessing consumer privacy protection. Is it really appropriate to argue that a firm complies with the FIP of notice if it simply tells consumers that it collects information and nothing else? This would seem to constitute very weak notice on the part of the firm. Likewise, if a firm offers consumers opt-in/opt-out choices concerning the receipt of promotions/solicitations, but does not give them any choice over how their information is managed or whom it is shared with, does this really constitute control? A few researchers have attempted to define each of the FIPs as multi-dimensional constructs in order to evaluate the extent (e.g., low, medium, and high) to which privacy policies encompass all of the dimensions of the five FIPs (O'Conner 2003; Ryker et al. 2002). This clearly makes more sense, but there is currently no consensus in the literature on what constitutes the necessary dimensions of each of the FIPs. As a result, operationalizing not only consumer privacy, but also the dimensions of the FIPs would enhance our understanding of consumer privacy and its protection. For example, we feel that a more adequate test of notice would include whether firms have identified in their privacy statements the entity collecting their data, the nature of the data collected, the means by the which the data will be collected, the uses to which the data will be put, the potential recipients of the data, whether provision of the data requested is voluntary or required, and the steps taken by the data collector to ensure the confidentiality, integrity, and quality of the data (FTC 1998).

Additionally, future research should also address the relationships between the various dimensions of consumer privacy. Although intuitively there seems to be a relationship between knowledge (notice) and control, the literature suggests many different relationships. For example, while there is agreement among researchers that consumers who possess high levels of both knowledge and control require the least amount of privacy protection (Foxman and Kilcoyne 1993; Goodwin 1991), there is also the view that increased knowledge reduces consumers' desire for control (Milne and Gordon 1993). This suggests that there may be an inverse relationship between knowledge and control (i.e., the more knowledge consumers have, the more they are willing to relinquish control). Likewise, there appears to be a relationship between control and access. Does a consumer really have control if they do not have access to their information? At most, it appears that they only have partial control. In addition, while most of the consumer privacy studies ignore the FIP of enforcement, security probably does not mean much unless there is actionable redress for violations of consumer privacy protection. Without clearly operationalizing

these concepts and testing the relationships under various conditions, we are left merely to speculate on how they interact.

Examining Competing Consumer Rights – Two issues related to the definition of consumer privacy that also deserve further theoretical development include consumer privacy rights and information ownership. It has been argued that privacy is not an absolute right and that consumers' right to privacy often conflicts with other rights, such as consumers' right to be informed and marketers' right to free speech (Borna and Avila 1999; Goodwin 1991; Milne and Gordon 1993). In order to clearly understand the relationships between these various rights/privileges, it is necessary to understand theoretically the trade-offs consumers are willing to make between these rights. For instance, research suggests that the role the consumer plays in the decision-making process explains the conflict between the right to privacy and the right to be informed (Lally 1996). The complexity of consumers' perceived rights/privileges suggests that there could be other factors (e.g., involvement, commitment, intentions), beyond the personal, social, and cultural factors outlined in the literature, that impact the trade-offs between privacy and other rights. For example, whether the consumers perceives a transaction with a firm as a single, discrete exchange or the beginning of a long-term commercial relationship may impact their willingness to provide information and the particular right (e.g., right to privacy versus the right to be informed) that takes precedence. Identification and examination of these additional factors and their relationships will not only extend our theoretical understanding, but also potentially inform future business strategy and policy/regulation concerning privacy rights.

In addition, the question of information ownership (i.e., who controls consumer information once it has been collected) is a central issue in the debate over consumer privacy (Borna and Avila 1999; Foxman and Kilcoyne 1993). In order to address this issue, it is necessary for us to understand what exactly constitutes information ownership, how perceptions of ownership vary by information type, and what other factors intensify or mitigate claims to ownership. Because the characteristics of information are different than those of physical possessions (i.e., even when you give or sell information, you still have possession of it), this privacy issue may be better addressed in relation to intellectual property laws. That is, information ownership may be defined in terms of who possesses and maintains the rights to the information and its distribution. We propose that a better understanding of these issues will have a direct impact on the privacy dimensions of knowledge and control, as well as on various other consumer issues such as trust, commitment, and purchase intention. In turn, we also propose that these issues will also impact the long-term business-to-consumer relationship in terms of consumer satisfaction, quality perceptions, and brand loyalty. As a result, businesses, as well as consumers, must be aware of the trade-offs concerning information ownership that are inherent in the consumer privacy debate.

Understanding the Ethical Dimensions of Consumer Privacy – Many of the articles that have examined the ethical dimensions of consumer privacy are conceptual in nature and are based primarily on logical arguments (e.g., Ashworth and Free 2005; Caudill and Murphy 2000; Charters 2002; Culnan and Bies 2003; Foxman and Kilcoyne 1993; Milne and Gordon 1993; Peslak 2005). Although the number of ethical frameworks that have been used is quite extensive (e.g., teleological ethics, deontological ethics, justice theory, and social contract theory), it seems unlikely that all of these theories apply in every situation associated with consumer privacy. In order to extend this area of research, marketers should test under what conditions each of these ethical frameworks has the greatest impact on consumer privacy and the implications of utilizing different ethical frameworks. For example, Culnan and Armstrong (1999) examine the relationship between procedural justice and trust and its effect on the disclosure of personal information. Given the normative component of privacy, it seems likely that there are main effects and interactions between the various ethical dimensions and dimensions of consumer privacy. Therefore, in order to expand our understanding of consumer privacy and its antecedents and consequences, it would be valuable to extend this ethical research by testing the relationship of a firm's ethical practices and consumer perceptions of these practices on consumer privacy.

Exploring the Strategy of Consumer Privacy – In order for firms to be more effective in delivering value in the future, managing consumer privacy protection has to move beyond being a tactical concern towards being a more strategic one. While the notion of privacy protection as a strategic asset has been alluded to by other scholars

(Ashworth and Free 2006), future research should examine the drivers and conditions that help firms' manage privacy protection as a strategically beneficial and proactive alternative. Most firms simply react and adapt to regulatory, industry, or consumer pressures regarding consumer privacy (Sarathy and Robertson 2003). As consumers and policy makers look toward heightened legislation, firms should look beyond being reactive, and instead embrace proactive approaches to managing privacy. Two areas in which this proactive adaptation can play out include organizational structure and strategy (Jennings and Seaman 1994).

In terms of organizational structure, research attention should be given to ways of institutionalizing consumer privacy protection within the firm. For instance, both the short-term and long-term impact of hiring privacy officers ought to be examined. Business practitioners note that privacy officers can not only help assess privacy risks and craft privacy policies, but can also audit company processes and handle consumer complaints and resolution (Shea 2002). In addition, the effectiveness of privacy officers needs to be examined in terms of the contributions they make to the firm's strategic planning and their proactive stance towards putting a good consumer privacy policy in place before it is legislated by the state. By understanding how to utilize privacy offers in a way that benefits both the organization and its customers, firms will be better able to manage the costs associated with consumer privacy protection and to communicate the benefits that accrue to customers.

In terms of strategy, research needs to address a firm's concern for consumer privacy within the broad domain of market orientation (Kohli and Jaworski 1990; Narver and Slater 1990). The full impact of market orientation on the nature and extent of consumer privacy protection needs to be investigated (Dolnicar and Jordaan 2007). From a more strategic perspective, perhaps the very definition of market orientation needs to be re-examined so as to include privacy protection as a critical component of being customer-oriented. The traditional definition of market orientation includes the components of customer orientation, competitor orientation, and interfunctional coordination (Narver and Slater 1990). The domain of the customer orientation component, however, is limited to basic marketing goals such as understanding needs, creating value, and measuring satisfaction. A more progressive redefinition of customer orientation, especially one that includes the goals of creating safety and trust, which have been shown to be directly affected by a firm's information practices and privacy policies, may be in order. Additionally, firms that do go the extra mile on privacy protection need to ensure that their efforts are rightly reflected in measurable marketing outcomes, such as loyalty, brand image, and overall brand equity. Longitudinal empirical work is needed to assess the impact of privacy protection efforts, over multiple years, on customer loyalty and brand equity. It is indeed critical to assess the impact that a firm's consumer privacy protection efforts have on customer acquisition, customer retention, and customer profitability, since these are the primary goals of any market-oriented effort.

Being strategic about consumer privacy could also include using consumer privacy protection as a positioning platform, especially for firms that deal with transfer of highly sensitive information such as financial and medical services. For instance, should firms position themselves on the basis of differentiation in privacy protection vis-à-vis their competitors? Although it has been argued in the literature that firms will find it hard to compete on privacy protection since it falls into the category of negative information (Jones 1991), as incidents of identity theft or other privacy violations increase, consumers may actively seek out firms that provide greater privacy protection. In fact, consumers are now willing to pay banks, credit card companies, and credit agencies just to monitor their credit for fraudulent transactions. Likewise, as customization and personalization gain wider popularity (Pine, Victor, and Boyton 1993; Suprenant and Solomon 1987), firms that are positioned as "safer" or "trustworthy" on the privacy dimension will likely have a competitive advantage (Bowie and Jamal 2006). Future research could throw some light on the efficacy of such an approach.

Finally, more work is needed on effective communication of consumer privacy policies and protection efforts by firms. Clearly, the communication to consumers needs to go beyond a documented privacy policy, which research has found that most consumers do not read. Firms need to communicate the results of their privacy protection efforts, such as successful compliance with regulations, more effective personalization for consumers, reduced or lack of third party solicitations, etc., in order to gain future customer support (Sarathy and Robertson 2003). One way that firms are communicating their privacy protection is through third-party privacy seals (Caudhill and Mur-

phy 2000; Miyazaki and Krishnamurthy 2002; Rifon, LaRose, and Choi 2005). Future research should address the optimal mix, vehicles, and frequency of such communication.

Future Consumer Privacy Research: Contemporary Issues

In addition to extending the existing work on consumer privacy, research also needs to examine current trends and behaviors in consumer privacy. The growing problem of identity theft, the popularity of Internet websites such as MySpace, Facebook, and You Tube, and the events of 9/11 have all had an impact on not only on perceptions of privacy, but also on the related notions of participation and surveillance. This section explores some of the issues related to these three concepts and suggests areas for new consumer privacy research.

Identity Theft – Identity theft, which is defined as "the appropriation of someone else's identity to commit fraud or theft" (Milne 2003, p.388), is one of the most important and widely reported contemporary issues in consumer privacy. In 2002, the FTC reported that victims of identity theft numbered more than 9.9 million and accrued a total loss estimated at $5 billion (Stafford 2004). Identity theft usually occurs when someone uses another person's information (e.g., social security number, birthday, name, and address) to secure rights and privileges s/he does not possess (e.g., an illegal immigrant obtaining a drivers license) and/or to obtain credit in order to purchase items (Milne 2003; Sovern 2004). This information is often obtained through stealing a person's wallet/purse, stealing a person's mail, pilfering through the trash, or engaging in online surveillance (FTC 2001).
Given its widespread nature and the ease by which identity theft can be committed, the issue has received both legislative and academic attention. In 1998, the U.S. Congress criminalized identity theft by passing the Identity Theft and Assumption Deterrence Act. Unfortunately, the act did little to stop the practice of identity theft and it continued to grow (Sovern 2004). In December 2003, President Bush signed the Fair and Accurate Credit Transaction Act (FACTA) into law, which was developed in part to thwart and fight this increase in identity theft. Although some scholars have examined FACTA and other identity theft related legislation (Linnhoff and Langenderfer 2004), more research is needed to study the effects of these acts on identity theft and to determine what else needs to be done at the governmental level to address this important privacy issue.

In addition, there is a small but growing body of academic literature that has begun to address issues of identity theft. In a study of consumer protection practices, Milne (2003) found that although most people follow some types of identity theft preventive measures, more consumer education is needed so that individuals can fully protect themselves. Research is needed to determine the best way to educate consumers about identity theft prevention and victim recovery practices. Also driven by the importance of this problem, the *Journal of Consumer Affairs* recently organized a refereed research colloquium on identity theft. In the resulting papers, scholars have addressed means of curbing identity theft from various angles including using loss allocation rules of common law to force the credit industry to try to prevent identity theft (Sovern 2004), encouraging better organizational preparation and response to identity theft (Lacey and Cuganesan 2004), and developing collective actions of government, businesses, and consumers to jointly protect information from theft (Milne et al. 2004). Lastly, there is work that links consumer demographics to the risk of experiencing identity theft (Anderson 2006). In this study, it was found that women, consumers with high incomes, and younger consumers are found to be at higher risk for identity theft (Anderson 2006).

A number of issues, however, remain unresolved and should direct future research in this area. For instance, the impact of identity theft on the future consumer behavior of victims deserves to be better understood. In addition, research should examine the behaviors of those consumers who do not perceive themselves to be at risk. Research should also examine the role of third parties (e.g., trade associations and information brokers) in dealing with identity theft.

Consumer Online Behavior – In spite of the steady increase in identity theft, the amount and type of information that individuals are voluntarily posting on the Internet has also increased. Two recent PEW Internet and American Life Project studies found that more than 53 million American adults have posted personal information to the Internet (e.g., photographs, newsgroup postings, blogs) and more than half (55%) of American youths ages 12-17

have created detailed profiles on an online social networking site (e.g., MySpace and Facebook) (PEW 2004, 2007). While much of this information may be innocuous, once it has been posted to a publicly accessible website on the Internet, it becomes a matter of public record (McMenamin and Parmar 2007). Anyone from your friends, to the local police, to would-be identity thieves can access this information. And while many people, especially teens, say they do not care about the surveillance of their data and that it has brought them many positive benefits (Nussbaum 2007), it can also have negative consequences. For example, a mother in Oregon and a couple in Maryland were arrested based on information posted on their children's MySpace pages (McMenamin and Parmar 2007). Research should be conducted to determine the degree to which consumers are aware of the possible negative consequences of posting their information on the Internet, beyond the typical security threats, and their attitudes towards these consequences. Researchers should also study perceptions of risk associated with these behaviors and the trade-offs that consumers make when voluntarily posting their information.

In a recent article in the New York magazine, Nussbaum (2007) argues that most American teens accept that privacy no longer exists and that we now live in a surveillance society, and instead of resisting this lack of privacy in our lives, we should embrace it. This sentiment has been echoed by business founders Larry Ellison of Oracle and Scott McNealy of Sun Microsystems who have argued that privacy is largely an illusion and that we just need to get over it (Black 2001; Sprenger 1999). The fact that their companies produce systems that track peoples' information may have something to do with these opinions. Even academics argue that privacy is an overblown concept and that we are concerned about something that we have never had in the first place (Glazer 1998). Whatever the underlying cause of these perspectives, they all point at the inherent relationship between privacy, disclosure, and surveillance. Researchers should examine if there has been a fundamental shift in peoples' privacy expectations. For instance, have we as Americans moved from resisting invasions of privacy to embracing surveillance? More importantly, is this possible shift in attitudes a product of marketing or other business practices? Do we now live in a tabloid world in which we demand, and now accept, close surveillance of all individuals? Does our "right to know" now supersede all other rights? Not surprisingly, federal and state governments, as well as many businesses, have resisted intervening in these activities on legal grounds (McMenamin and Parmar 2007). Whatever the merit of these legal claims, there are clearly political and economic benefits to allowing and enticing individuals to provide detailed information about themselves.

As we have seen in the previous discussion on the ethics of consumer privacy, what benefits government and businesses does not always benefit the consumer. If you believe the argument that the fundamental difference between democracy and dictatorship is the degree of privacy protection and surveillance that these two types of societies entail (Westin 1967), then we may need to be concerned that consumers are giving up more than their right to privacy by willingly revealing so much of their personal information online. Although consumers argue that this unrestrained personal disclosure and transparency equates to the ultimate sense of freedom (Nussbaum 2007), others argue that this unconstrained flow of information actually undermines self-development and personal liberty (Rosen 2004; Solove 2007). As Zwick and Dholakia (2004) argue, a person's digital identity becomes his or her "real" identity, which the person then has little control over. Research is needed to address this online information phenomenon and its effects not only on privacy, but also on the underlying function of democratic and capitalistic societies. Specifically, research should determine what role marketing and business strategy plays in consumer online information practices and their broader societal effects.

Consumer Profiling – The increased collection of information by firms has led to a new a relatively new practice known as consumer profiling. Whereas traditional segmentation uses information to divide a heterogeneous market into smaller groups based on similar characteristics, needs, or behaviors (Dickson and Ginter 1987; Green and Krieger 1991), consumer (or customer) profiling uses information to infer characteristics about consumers and predict their behaviors (Min 2006; Mussi 2006; Spangler, Hartzel, and Gal-Or 2006). Consumer profiling often utilizes large amounts of disparate information such as demographic data, product preferences, shopping behaviors, media habits, and financial information to create dossiers on consumers which are then stored in huge databases (Batislam, Denizel, and Filiztekin 2007; Qian, Jiang, and Tsui 2006). This information can be gathered from various sources, including the data trail that consumers leave behind when using the Internet, choosing programming on their digital television sets through TIVO, using their grocery or supermarket membership cards, or

simply using their credit cards. Market-oriented processes such as customer relationship management (CRM) have institutionalized these practices by utilizing advances in information technology to increase in the collection and analysis of consumer information (Chan 2005).

While researchers have alluded to the privacy dangers of consumer profiling (Gertz 2002; Olivero and Lunt 2004; Spangler, Hartzel, and Gal-Or 2006; Wiedmann, Buxel, and Walsh 2002), it is a growing reality that deserves more research attention. As the depth of data on individual consumers continues to grow, firms will have to balance their market-oriented strategies with their surveillance of consumers very carefully. While research should examine individuals' perceptions of and reactions to consumer profiling, this is an area where future work on the organizational side is sorely needed. For example, what is the best way for firms to manage customer relationships without being (or appearing to be) too invasive of consumer privacy? Clearly business-to-business relationships follow a different paradigm here than consumer marketing, but this is an area that also needs to be explored. The conventional wisdom is that business-to-business clients are glad to share company specific information (e.g., firm demographics, market strategies, credit histories) in return for more customized and personalized services (Chan 2005). This leads to the questions, what constitutes privacy in the organizational realm and how willing are firms to divulge sensitive information to each other? This area needs further exploration.

New Technology Surveillance – Technological advances in various fields have led to the rise of a number of different surveillance-based technologies being tested in the marketplace. For instance, radio frequency identification (RFID) allows any and every product to be uniquely identified through signals transmitted by a device embedded in the product (Peslak 2005). While the technology has tremendous implications for supply chain management, especially inventory control, it raises a number of concerns about consumer privacy (Kumar, Pauly, and Budin 2007). Because RFID tags can be read from a distance (Cochran, Tatikonda, and Magid 2007), consumers wearing clothing with RFIG tags or carrying RFID embedded credit cards can potentially have their location tracked, any time of day or night. Future research needs to look beyond just the ethics of RFID and examine the extent of consumer acceptance of such technology and the effects that it could have on consumer behavior, such as consumer backlash against marketers using RFID. For example, one study has examined how RFID systems affect consumer trust (Lee et al. 2007).

Biometrics, or the identification of human beings through unique physical and behavioral characteristics, is another such technology (Jones et al. 2007). Although finger-prints are the most common form of biometric measurement, other identifiers such as hand prints, facial recognition, iris designs, and genetic profile can also be used to identify individuals. While clearly biometrics can be useful in various business sectors in thwarting fraud, it has ramifications for consumer profiling, consumer anonymity, and identity theft. This is especially the case considering that many biometric systems require other identifiers (e.g., social security numbers) to authenticate a person's identity (Bhargav-Spantzel et al. 2007). Research on organizational and consumer response to biometrics is woefully inadequate and the area of privacy and biometrics is ripe for future work.

Other Contemporary Privacy Issues – Privacy rights clearinghouse (www.privacyrights.org) has identified a host of other privacy-related issues that may have only an indirect bearing on consumer privacy. Nevertheless, these issues deserve a mention and merit further research attention. Monitoring of employee activities at their workplace (e.g., Internet use, video surveillance, email use, and location tracking) is becoming more ubiquitous and may have a bearing on employee's psychological state and workplace performance (Brown 2000; Freedman and Reed 2007). Research could examine if individuals' privacy perceptions at work and their effects influence their privacy expectations in the market. Medical records, although covered by the Health Insurance Portability and Accountability Act (HIPPA), are available to everyone from healthcare providers and insurance companies, to labs and pharmacies. Importantly, patient consent is not required for information sharing between these agencies (Brown 2007). Research could examine if this lack of consumer privacy has any effect on consumers' health care costs? Even more alarming is the issue of financial privacy. The Gramm-Leach-Bliley law (2001) allows financial companies such as banks, mortgage companies, and insurance companies to share information such as loan repayments, investments, account balances in the savings and checking accounts, amongst each other or even with third parties. This often results in unsolicited direct marketing promotions, irrespective of consumer needs and

wants. With the increase in identity theft, research should examine the degree to which these activities (e.g., the constant supply of credit card offers in the mail) contribute to security breaches and negative consequences. Finally, since the events of September 11, 2001, the USA Patriot Act has strengthened the ability of the state to wiretap telephone and Internet communications. Civil liberties groups point to the possibility of the government to abuse of the powers granted by this act and to further eroding of citizens' rights, especially the right to privacy, through its usage. Research should examine just how far consumers are willing to go in giving up their rights under the guise of increased security.

CONCLUSION

This article presents a summary of the general concept of privacy, a review of the consumer privacy literature, and suggestions for future research. Different aspects of privacy and consumer privacy are reviewed and discussed, including the nature of privacy and privacy rights, definitions of both privacy and consumer privacy, ethical dimensions of consumer privacy, and self-regulation of consumer privacy protection by firms. By integrating the extant work on consumer privacy, this article highlights the gaps in the literature and presents future research directions such as 1) defining and mapping out the domain of consumer privacy, 2) understanding the ethical dimensions of consumer privacy rights, and 3) determining the firm-level drivers of customer privacy protection. Substantial progress has been made since the late 1980s in our understanding of the concept of consumer privacy and many of the issues surrounding this concept.

However, there remains an opportunity for more theoretically-driven research in order to develop a working model that specifies and defines the domain of consumer privacy and highlights the relationships between the relevant individual-level and firm-level dimensions, as well as their antecedents and consequences. In addition, contemporary issues in consumer privacy such as identity theft, consumer online behavior, and consumer profiling suggest new areas for research in order to expand our understanding and refine our definitions. Through this review, we summarize the current state of consumer privacy research and suggest ways to extend this very important area of study. The following table succinctly presents our recommendations for future research in consumer privacy.

TABLE 2
Future Consumer Privacy Research Recommendations

Theoretical Issues	Key Tasks
1. Operationalizing Consumer Privacy	• Define the domain of consumer privacy. • Operationalize (a) Knowledge and (b) Control – the two key components of consumer privacy. • Identify and operationalize the elements of the FIPs. • Identify relevant components *outside* the FIPs. • Develop constructs to capture both objective and perceptual constructs of consumer privacy. • Identify the inter-relationships between different dimensions of consumer privacy.
2. Competing Consumer Rights	• Identify and measure the trade-offs consumers are willing to make between different rights. • Identify the personal, corporate, and environmental factors that impact the trade-offs consumers make. • Define information ownership. • Identify the factors that intensify or mitigate claims of information ownership.

3. Ethical Dimensions of Consumer Privacy	• Test the relationships between firms' ethical practices concerning consumer privacy and the consumer perception of these practices. • Empirically examine which ethical frameworks (e.g., teleology, deontology, justice theory, social contract theory) are best applicable to explaining consumer privacy.
4. Strategy of Consumer Privacy	• Examine how firms can embrace privacy protection as a strategic choice. • Examine the process of institutionalizing consumer privacy protection in a company. • Develop metrics for measuring the effectiveness of privacy officers. • Longitudinal assessment of the impact of privacy protection on customer retention and loyalty. • Test the viability of using privacy protection as a positioning platform. • Test and compare different modes of communicating privacy policies.

Contemporary Practice Issues	**Key Tasks**
1. Identity Theft	• Examine the impact of identity theft on the future consumer behavior of victims. • Examine the behaviors of consumers who perceive themselves to be at low-risk of identity theft. • Examine the role of third parties (e.g., trade associations and information brokers) in dealing with identity theft.
2. Online Behavior	• Examine if there has been a fundamental shift in consumers' privacy expectations, especially as a function of the Internet. • Examine the broader societal effects of consumer online information practices.
3. Consumer Profiling	• Examine the optimal ways for firms to manage customer relationships without being too invasive. • Examine the differences in sensitivity to privacy issues between business-to-business and business-to-consumer segments.
4. New Technology Surveillance	• Examine the (possible) effects of RFID on consumer behavior. • Examine the extent of acceptance of biometric systems in marketing.
5. Other Privacy Issues	• Examine if individuals' workplace privacy perceptions influence their privacy expectations in the consumer market.

REFERENCES

Adams, J. Stacey. 1965. "Inequity in Social Exchange." In *Advances in Experimental Social Psychology*. Vol. 2. Ed L. Berkowitz. New York: Academic Press, 267-299.

Allee, W.C. 1938. *The Social Life of Animals*. New York: W.W. Norton & Company.

Altman, Irwin. 1975. *The Environment and Social Behavior*. Belmont, CA: Wadsworth.

Altman, Irwin. 1977. "Privacy Regulation: Culturally Universal or Culturally Specific." *Journal of Social Issues* 33 (3): 66-84.

Andrade, Eduardo B., Veltitka Kalcheva, and Barton Weitz. 2002. "Self-Disclosure on the Web: The Impact of Privacy Policy, Reward, and Company Reputation." *Advances in Consumer Research* 29 (1): 350-353.

Ardrey, Robert. 1966. *The Territorial Imperative: A Personal Inquiry into the Animal Origins of Property and Nations*. New York: Atheneum.

Ashworth, Laurence and Clinton 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.

Associated Press (AP). 2007. "Intelligence Deputy to America: Rethink Privacy," Available: www.cnn.com/ 2007/POLITICS/11/11/terrorist.surveillance.ap/index.html.

Barksdale, Hiram C. and Bill Darden. 1971. "Marketers' Attitudes Toward the Marketing Concept." *Journal of Marketing* 35 (October) 29-36.

Batislam, Emine Persentili, Meltem Denizel, and Alpay Filiztekin. 2007. *International Journal of Research in Marketing*. 24 (3): 201-209.

Benn, Stanley I. 1971. "Privacy, Freedom and Respect for Persons." In Nomos XIII: Privacy. Eds. J. R. Pennock and J. W. Chapman. New York: Atherton Press, 56-70.

Berlyne, D. E. 1960. *Conflict, Arousal, and Curiosity*. New York: McGraw Hill.

Bhargav-Spantzel, Abhilasha, Anna C. Squicciarini, Shimon Modi, Matthew Young, Elisa Bertino, and Stephen J. Elliott. 2007. "Privacy Preserving Multi-Factor Authentication with Biometrics." *Journal of Computer Security* 15 (5): 529-560.

Black, Jane. 2001. "Don't Make Privacy the Next Victim of Terror." *BusinessWeek*. Available: www.businessweek.com/bwdaily/dnflash/cot2001/nf2001104_7412.htm.

Bloom, Paul N., George R. Milne, and Robert Adler. 1994. "Avoiding Misuse of New Information Technologies: Legal and Societal Considerations." *Journal of Marketing* 58 (1): 98-110.

Bloustein, Edward. 1964. "Privacy as an Aspect of Human Dignity." *New York University Law Review* 39 (6): 962-1007.

Bloustein, Edward. 1968. "Tort Law and the Constitution: Is Warren and Brandeis' Tort Petty and Unconstitutional as Well." *Texas Law Review* 46 (5): 611-29.

Borna, Shaheen and Stephen Avila. 1999. "Genetic Information: Consumers' Right to Privacy Versus Insurance Companies' Right to Know a Public Opinion Survey." *Journal of Business Ethics* 19 (4): 355-362.

Bowie, Norman E. and Karim Jamal. 2006. "Privacy Rights on the Internet: Self-Regulation or Government Regulation?" *Business Ethics Quarterly* 16 (3) 323-342.

Brown, Bob. 2007. "Top 10 HIPPA Misconceptions." *Journal of Health Care Compliance* 9 (1): 41-82.

Brown, William S. 2000. "Ontological Security, Existential Anxiety, and Workplace Privacy." *Journal of Business Ethics* 23 (1): 61-65.

Campbell, Alexandra. 1997. "Relationship Marketing in Consumer Markets: A Comparison of Managerial and Consumer Attitudes about Information Privacy." *Journal of Direct Marketing* 11 (3) 44-57.

Carroll, Brian. 2002. "Price of Privacy: Selling Consumer Databases in Bankruptcy." *Journal of Interactive Marketing* 16 (3): 47-58.

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

Center for Democracy and Technology. 2003. *Top Ten Ways to Protect Online Privacy*. Available: http://www.cdt.org/privacy/guide/basic/topten.html.

Cespedes, Frank V. and H. Jeff Smith. 1993. "Database Marketing: New Rules for Policy and Practice." *Sloan Management Review* 34 (Summer): 7-22.

Charters, Darren. 2002. "Electronic Monitoring and Privacy Issues in Business-Marketing: The Ethics of the DoubleClick Experience." *Journal of Business Ethics* 35 (4): 243-254.

Chan, Joseph. 2005. "Toward a Unified View of Customer Relationship Management." *The Journal of American Academy of Business* 6 (1): 32-38.

Chen, Kuanchin and Alan I. Rea, Jr. 2004. "Protecting Personal Information Online: A Survey of User Privacy Concerns and Control Techniques." *Journal of Computer Information Systems* 44 (4): 85-92.

Clark, Lorenne M. G. 1978. "Privacy, Property, Freedom, and the Family." In *Philosophical Law: Authority, Equality, Adjudication, Privacy*. Ed. R. Bronaugh. Westport, CT: Greenwood Press, 167-87.

Cockran, Philip L., Mohan V. Tatikonda, and Julie Manning Magid. 2007. "Radio Frequency Identification and the Ethics of Privacy." *Organizational Dynamics* 36 (2): 217-229.

Culnan, Mary J. 1995. "Consumer Awareness of Name Removal Procedures: Implications for Direct Marketing." *Journal of Direct Marketing* 9 (Spring): 10-19.

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

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

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

DeCew, Judith Wagner. 1997. *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology*. Ithaca: Cornell University Press.

Dickler, Gerald. 1936. "The Right of Privacy: A Proposed Redefinition." *United States Law Review* 70 (8): 435-.

Dickson, Peter R. and James L. Ginter. 1987. "Market Segmentation, Product Differentiation, and Marketing Strategy." *Journal of Marketing* 51 (April) 1-10.

Dommeyer, Curt J. and Barbara L. Gross. 2003. "What Consumers Know and What They Do: An Investigation of Consumer Knowledge, Awareness, and Use of Privacy Protection Strategies." *Journal of Interactive Marketing* 17 (2): 34-51.

Dunfee, Thomas W., N. Craig Smith, and William T. Ross. 1999. "Social Contracts and Marketing Ethics." *Journal of Marketing* 63 (July): 14-32.

Dwyer, F. Robert, Paul H. Schurr, and Sejo Oh. 1987. "Developing Buyer-Seller Relationships." *Journal of Marketing* 51 (April): 11-27.

Eastlick, Mary Ann, Sherry L. Lotz, and Patricia 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.

Etzioni, Amitai. 1999. *The Limits of Privacy*. New York: Basic Books.

Federal Trade Commission (FTC). 1998. *Privacy Online: A Report to Congress*. Available: http://www.ftc.gov/reports/privacy3/priv-23a.pdf.

Federal Trade Commission (FTC). 2000. *Privacy Online: Fair Information Practices in the Electronic Marketplace: A Report to Congress*. Available: http://www.ftc.gov/reports/privacy2000/ privacy2000.pdf.

Federal Trade Commission (FTC). 2001. *ID Theft: When Bad Things Happen to Your Good Name*. Available: http://www.ftc.gov/bcp/conline/pubs/credit/idtheft.pdf.

Flaherty, David H. 1967. *Privacy in Colonial New England*. Charlottesville: University Press of Virginia.

Flaherty, David H. 1989. *Protecting Privacy in Surveillance Societies*. Chapel Hill: University of North Carolina Press.

Flesch, Rudolf. 1949. *The Art of Readable Writing*. New York: Macmillan.

Foxman, Ellen R. and Paula Kilcoyne. 1993. "Information Technology, Marketing Practice, and Consumer Privacy: Ethical Issues." *Journal of Public Policy & Marketing* 12 (1): 106-119.

Fried, Charles. 1968. "Privacy." *Yale Law Journal* 77 (3): 475-493.

Friedman, Barry A. and Lisa J. Reed. 2007. "Workplace Privacy: Employee Relations and Legal Implications of Monitoring Employee E-Mail Use." *Journal of Business Ethics* 19 (2): 75-83.

Friedrich, Carl J. 1971. "Secrecy versus Privacy: The Democratic Dilemma." In *Nomos XIII: Privacy*. Eds. J. R. Pennock and J. W. Chapman. New York: Atherton Press, 105-120.

Fromm-Reichmann, Frieda. 1959. "Loneliness." *Psychiatry* 22 (1): 1-15.

Gandy, Oscar. 1993. *The Panoptic Sort: A Political Economy of Personal Information*. New York: Westview.

Gavison, Ruth. 1980. "Privacy and the Limits of Law." *Yale Law Journal* 89 (3): 421-471.

Geertz, Clifford. 1973. *The Interpretation of Cultures*. New York: Basic Books.

Gertz, Janet Dean. 2002. "The Purloined Personality: Consumer Profiling in Financial Services." *San Diego Law Review* 39 (3): 943-1018.

Glazer, Rashi. (1998). The Illusion of Privacy and Competition for Attention. *Journal of Interactive Marketing* 12 (3): 2-4.

Glenn, Richard A. 2003. *The Right to Privacy: Rights and Liberties under the Law*. Santa Barbara, CA: ABC-CLIO.

Goffman, Erving. 1959. *The Presentation of Self in Everyday Life*. Garden City, NY: Doubleday.

Goffman, Erving. 1961. *Asylums: Essays on the Social Situation of Mental Patients and Other Inmates*. Garden City, NY: Doubleday & Company.

Goodwin, Cathy. 1991. "Privacy: Recognition of a Consumer Right." *Journal of Public Policy & Marketing* 10 (1): 149-166.

Graham, Jonathan P. 1987. "Privacy, Computers, and the Commercial Dimensions of Personal Information." *Texas Law Review* 65 (7): 1395-1439.

Green, Paul E. and Abba M. Krieger. 1991. "Segmenting Markets with Conjoint Analysis." *Journal of Marketing* 55 (October): 20-31.

Gross, Hyman. 1967. "The Concept of Privacy." *New York University Law Review* 42 (1): 34-54.

Hall, Edward T. 1966. *The Hidden Dimension*. Garden City: NY: Doubleday.

Honigmann, John J. 1959. *The World of Man*. New York: Harper.

Horney, Karen. 1945. *Our Inner Conflicts: A Constructive Theory of Neurosis*. New York: W.W. Norton & Company.

Hosch, Heyward C. 1983. "The Interest in Limiting The Disclosure of Personal Information: A Constitutional Analysis." *Vanderbilt Law Review* 36 (1): 139-198.

Houston, Franklin S. 1986. "The Marketing Concept: What It Is and What It Is Not." *Journal of Marketing* 50 (April) 81-87.

Hoy, Mariea Grubbs and Joseph Phelps. 2003. "Consumer Privacy and Security Protection on Church Web Sites: Reasons for Concern." *Journal of Public Policy & Marketing* 22 (1): 58-70.

Huizinga, Johan. 1950. *Homo Ludens: A Study of the Play-Element in Culture*. Boston: The Beacon Press.

Introna, Lucas D. and Athanasia Pouloudi. 1999. "Privacy in the Information Age: Stakeholders, Interests and Values." *Journal of Business Ethics* 22 (1): 27-38.

Jennings, Daniel F. and Samuel L. Seaman. 1994. "High and Low Levels of Organizational Adaptation: An Empirical Analysis of Strategy, Structure and Performance." *Strategic Management Journal* 15 (6): 459-75.

Johnson, Jeffery L. 1989. "Privacy and the Judgment of Others." *The Journal of Value Inquiry* 23 (2): 157-168.

Jones, Livingston F. 1914. *A Study of the Thlingets of Alaska*. New York: H. Revell.

Jones, Mary Gardiner. 1991. "Privacy: A Significant Marketing Issue for the 1990s." *Journal of Public Policy & Marketing* 10 (1): 133-148.

Jones, Peter, Peter Williams, David Hillier, and Daphne Comfort. 2007. "Biometrics in Retailing." *International Journal of Retail & Distribution Management* 35 (3): 217-222.

Jourard, Sidney M. 1966. "Some Psychological Aspects of Privacy." *Law and Contemporary Problems* 31 (2): 307-318.

Kant, Immanuel. 1959. *Foundations of the Metaphysics of Morals*. Indianapolis: Bobbs-Merrill Company.

Katz, James E. and Annette R. Tassone. 1990. "Public Opinion Trends: Privacy and Information Technology." *Public Opinion Quarterly* 54 (1): 125-143.

Kieth, Robert J. 1960. "The Marketing Revolution." *Journal of Marketing* 24 (January): 35-38.

Kohli, Ajay K. and Bernard J. Jaworski. 1990. "Market Orientation: The Construct, Research Propositions, and Managerial Implications." *Journal of Marketing* 54 (April): 1-18.

Kotler, Philip and Gerald Zaltman. 1971. "Social Marketing: An Approach to Planned Social Change." *Journal of Marketing* 35 (July) 3-12.

Kumar, Sameer, Soeren Pauly, and Erin Budin. 2007. "Impact of Radio Frequency Identification Technology on Manufacturing and Logistics: Challenges and Issues." *International Journal of Manufacturing Technology & Management* 10 (1): 57-70.

Lacey, David and Suresh Cuganesan. 2004. "The Role of Organizations in Identity Theft Response: The Organization-Individual Victim Dynamic." *The Journal of Consumer Affairs* 38 (2): 244-261.

Lally, Laura. 1996. "Privacy Versus Accessibility: The Impact of Situationally Conditioned Belief." *Journal of Business Ethics* 15 (11): 1221-1226.

Laufer, Robert S. and Maxine Wolfe. 1977. "Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory," *Journal of Social Issues* 33 (3): 438-58.

Lee, Dorothy. 1959. *Freedom and Culture*. Englewood Cliffs, NJ: Prentice Hall.

Lee, Sang M., Sang-hyun Park, Seong No Yoon, and Seung-jun Yeon. 2007. "RFID Based Ubiquitous Commerce and Consumer Trust." *Industrial Management & Data Systems* 107 (5): 605-617.

Lemon, Katherine N., Tiffany Barnett White and Russell S. Winer. 2002. "Dynamic Customer Relationship Management: Incorporating Future Considerations into the Service Retention Decision." *Journal of Marketing* 66 (January): 1-14.

Levy, Steven and Brad Stone. 2005. "Grand Theft Identity." *Newsweek* 146 (1): 38-47.

Linnhoff, Stefan and Jeff Langenderfer. 2004. "Identity Theft Legislation: The Fair and Accurate Credit Transactions Act of 2003 and the Road Not Taken." *The Journal of Consumer Affairs* 38 (2): 204-216.

Lwin, May, Jochen Wirtz, and Jerome D. Williams. 2007. "Consumer Online Privacy Concerns and Responses: A Power-Responsbility Equilibrium Perspective." *Journal of the Academy of Marketing Science* 35 (4): 572-585.

Margulis, Stephen T. 2003. "Privacy as a Social Issue and Behavioral Concept." *Journal of Social Issues* 59 (2): 243-261.

McCrohan, Kevin F. 1989. "Information Technology, Privacy, and the Public Good." *Journal of Public Policy & Marketing* 8 (1): 265-278.

McKitterick, J.B. 1957. "What is the Marketing Management Concept?" In *The Frontiers of Marketing Thought and Science.* Ed. F. M. Bass. Chicago: American Marketing Association, 71-82.

McMenamin, Brigid and Neil Parmar. 2007. "Family Secrets." *SmartMoney* 16 (9): 76-82.

McWhirter, Darien A and Jon D. Bible. 1992. *Privacy as a Constitutional Right: Sex, Drugs, and the Right to Life*. New York: Quorum Books.

Mead, Margaret. 1949. *Coming of Age in Samoa: A Psychological Study of Primitive Youth for Western Civilisation*. New York: New American Library.

Merton, Robert K. 1957. *Social Theory and Social Structure*. New York: Free Press.

Milberg, Sandra J., H. Jeff Smith, and Sandra J. Burke. 2000. "Information Privacy: Corporate Management and National Regulation." *Organization Science* 11 (January-February): 35-57.

Miller, Stephen P. 1999. *The Seventies Now: Culture as Surveillance*. Durham, NC: Duke University Press.

Milne, George R. 2000. "Privacy and Ethical Issues in Database/Interactive Marketing and Public Policy: A Research Framework and Overview of Special Issue." *Journal of Public Policy & Marketing* 19 (1) 1-6.

Milne, George R. 2003. "How Well Do Consumers Protect Themselves from Identity Theft?" *The Journal of Consumer Affairs* 37 (2) 388-402.

Milne, George R. and María-Eugenia Boza. 1999. "Trust and Concern in Consumers' Perceptions of Marketing Information Management Practices." *Journal of Interactive Marketing* 13 (1): 5-24.

Milne, George R. and Mary 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.

Milne, George R. and Mary 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.

Milne, George R., Mary J. Culnan, and Henry Greene. 2006. "A Longitudinal Assessment of Online Privacy Notice Readability." *Journal of Public Policy & Marketing* 25 (2): 238-249.

Milne, George R. and Mary Ellen Gordon. 1993. "Direct Mail Privacy-Efficiency Trade-offs Within an Implied Social Contract Framework." *Journal of Public Policy & Marketing* 12 (2): 206-215.

Milne, George R. and Andrew 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.

Milne, George R., Andrew J. Rohm, and Shalini Bahl. 2004. "Consumer Protection of Online Privacy and Identity." *The Journal of Consumer Affairs* 38 (2): 217-232.

Min, Hokey. 2006. "Developing the Profiles of Supermarket Customers through Data Mining." *The Service Industries Journal* 26 (7): 747-763.

Miyazaki, Anthony D. and Ana Fernandez. 2000. "Internet Privacy and Security: An Examination of Online Retailer Disclosures." *Journal of Public Policy & Marketing* 19 (1): 54-61.

Moore, Barrington. 1984. *Privacy: Studies in Social and Cultural History*. Armonk, NY: M.E. Sharpe.

Mussi, Silvano. 2006. "User Profiling on the Web Based on Deep Knowledge and Sequential Questioning." *Expert Systems* 23 (1): 21-38.

Murphy, Robert F. 1964. "Social Distance and the Veil." *American Anthropologist* 66 (6): 1257-1274.

Narver, John C. and Stanley F. Slater. 1990. "The Effect of a Market Orientation on Business Profitability." *Journal of Marketing* 54 (4): 20-35.

Nussbaum, Emily. 2007. "Say Everything." *New York Magazine*. 40 (5): 24-30.

Nizer, Louis. 1941. "The Right of Privacy: A Half Century's Developments." *Michigan Law Review* 39 (4): 526-596.

Nowak, Glen J. and Joseph Phelps. 1992. "Understanding Privacy Concerns." *Journal of Direct Marketing* 6 (4): 28-39.

Nowak, Glen J. and Joseph Phelps. 1997. "Direct Marketing and the Use of Individual-Level Consumer Information: Determining How and When 'Privacy' Matters." *Journal of Direct Marketing* 11 (4): 94-108.

O'Conner, Peter. 2003. "What Happens to My Information if I Make a Hotel Booking Online: An Analysis of Online Privacy Use, Content and Compliance by International Hotel Companies." *Journal of Services Research* 3 (2): 4-28.

Olivero, Nadia and Peter Lunt. 2004. "Privacy versus Willingness to Disclose in E-commerce Exchanges: The Effect of Risk Awareness on the Relative Role of Trust and Control." *Journal of Economic Psychology* 25 (2): 243-262.

Parker, Richard B. 1974. "A Definition of Privacy." *Rutgers Law Review* 27 (2): 275-296.

Peslak, Alan R. 2005. "An Ethical Exploration of Privacy and Radio Frequency Identification." *Journal of Business Ethics* 59 (4): 327-345.

Petty, Ross D. 2000. "Marketing Without Consent: Consumer Choice and Costs, Privacy, and Public Policy." *Journal of Public Policy & Marketing* 19 (1): 42-53.

PEW Internet & American Life Project (PEW). 2004. *Content Creation Online*. Available: http://www.pewinternet.org/pdfs/PIP_Content_Creation_Report.pdf.

PEW Internet & American Life Project (PEW). 2007. *Teens, Privacy & Online Social Networks*. Available: http://www.pewinternet.org/pdfs/PIP_Teens_Privacy_SNS_Report_Final.pdf.

Phelps, Joseph E., Giles D'Souza, and Glen J. Nowak. 2001. "Antecedents and consequences of consumer privacy concerns: An empirical investigation." *Journal of Interactive Marketing* 15 (4): 2-17.

Phelps, Joseph, Glen Nowak, and Elizabeth Ferrell. 2000. "Privacy Concerns and Consumer Willingness to Provide Personal Information." *Journal of Public Policy & Marketing* 19 (1): 27-41.

Pincus, Laura B. and Roger J. Johns. 1997. "Private Parts: A Global Analysis of Privacy Protection Schemes and a Proposed Innovation for their Comparative Evaluation." *Journal of Business Ethics* 16 (12-13): 1237-1260.

Pine, B. Joseph II, Bart Victor, and Andrew C. Boynton. 1993. "Making Mass Customization Work." *Harvard Business Review* 71 (5): 108-11.

Pollach, Irene. 2005. "A Typology of Communicative Strategies in Online Privacy Policies: Ethics, Power and Informed Consent." *Journal of Business Ethics* 62 (3): 221-235.

Posch, Robert J. 1988. *The Complete Guide to Marketing and the Law*. Englewood Cliffs, NJ: Prentice Hall.

Posner, Richard. 1981. *The Economics of Justice*. Cambridge, MA: Harvard University Press.

Pound. 1961. "The Fourteenth Amendment and the Right to Privacy." *Case Western Reserve Law Review* 13 (1): 34-55.

Prosser, William. 1960. "The Torts of Privacy." *California Law Review* 48 (3): 383-423.

Qian, Zhiguang, Wei Jiang, and Kwok-Leung Tsui. 2006. "Churn Detection via Customer Profile Modeling." *International Journal of Production Research* 44 (14): 2913-2933.

Rachels, James. 1975. "Why Privacy is Important." *Philosophy and Public Affairs* 4 (Summer): 323-333.

Rasor, Paul B. 1986. "Privacy Implications of Consumer Credit Protection Laws." *The John Marshall Law Review* 19 (Summer): 941-957.

Rich, Amy Schlesinger. 1987. "Pleading the Fifth." *Cardozo Law Review* 8 (3): 633-55.

Roman, Ernan. 1988. *Integrated Direct Marketing: Techniques and Strategies for Success*. New York: McGraw-Hill.

Rosen, Jeffrey. 2004. *The Naked Crowd: Reclaiming Security and Freedom in an Anxious Age*. New York: Random House.

Rust, Roland T., P.K. Kannan, and Na Peng. 2002. "The Customer Economics of Internet Privacy." *Journal of the Academy of Marketing Science* 30 (4): 455-464.

Ryals, Lynette. 2005. "Making Customer Relationship Management Work: The Measurement and Profitable Management of Customer Relationships." *Journal of Marketing* 69 (October): 252-261.

Ryker, Randy, Elizabeth LaFleur, Bruce McManis, and K. Chris Cox. 2002. "Online Privacy Policies: An Assessment of the Fortune E-50." *Journal of Computer Information Systems* 42 (4): 15-20.

Sarathy, Ravi and Christopher J. Robertson. 2003. "Strategic and Ethical Considerations in Managing Digital Privacy." *Journal of Business Ethics* 46 (2): 111-126.

Schein, Virginia E. 1977. "Individual Privacy and Personal Psychology: The Need for a Broader Perspective." *Journal of Social Issues* 33 (3): 154-168.

Scheibal, William J. and Julia A. Gladstode. 2000. "Privacy on the Net: Europe Changes the Rules." *Business Horizons* 43 (May-June): 13-18.

Schoenbachler, Denise D. and Geoffrey L. Gordon. 2002. "Trust and Customer Willingness to Provide Information in Database-Driven Relationship Marketing." *Journal of Interactive Marketing* 16 (3): 2-16.

Sheehan, Kim Bartel. 1999. "An investigation of gender differences in on-line privacy concerns and resultant behaviors." *Journal of Interactive Marketing* 13 (4): 24-38.

Sheehan, Kim Bartel. 2005. "In Poor Health: An Assessment of Privacy Policies at Direct-to-Consumer Web Sites." *Journal of Public Policy & Marketing* 24 (2): 273-283.

Sheehan, Kim Bartel and Mariea Grubbs Hoy. 2000. "Flaming, Complaining, Abstaining: How Online Users Respond to Privacy Concerns." *Journal of Advertising* 18 (3): 37-51.

Sheehan, Kim Bartel and Mariea Grubbs Hoy. 2000. "Dimensions of Privacy Concern Among Online Consumers." *Journal of Public Policy & Marketing* 19 (1): 62-73.

Shils, Edward. 1959. "Social Inquiry and the Autonomy of the Individual." In *The Human Meaning of the Social Sciences*. Ed. D. Lerner. New York: Meridian Books.

Shils, Edward. 1966. "Privacy: Its Constitution and Vicissitudes." *Law and Contemporary Problems* 31 (2): 281-306.

Siep, David J. 1978. *The Right to Privacy*. Boston: Harvard University.

Simitis, Spiro. 1987. "Reviewing Privacy in an Information Society." *University of Pennsylvania Law Review* 135 (3): 707-746.

Simmel, Georg. 1950. *The Sociology of Georg Simmel*. Glencoe, IL: Free Press.

Simonson, Itamar, Ziv Carmon, Ravi Dhar, Aimee Drolet, and Stephen M. Nowlis. 2001. "Consumer Research: In Search of Identity." *Annual Review of Psychology* 52, 249-275.

Smith, Glenn D. 1989. "We've Got Your Number! (Is it Constitutional to Give it Out?): Caller Identification Technology and the Right to Information Privacy." *UCLA Law Review* 37 (1): 145-223.

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

Smith, H. Jeff. 2001. “Information Privacy and Marketing: What the U.S. Should (and Shouldn’t) Learn From Europe.” *California Management Review* 43 (2): 8-33.

Smith, Robert Ellis. 2002. *Compilation of State and Federal Privacy Laws*. Washington D.C.: Privacy Journal.

Solove, Daniel J. 2007. *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet*. New Haven, Connecticut: Yale University Press.

Sovern, Jeff. 2004. “Stopping Identity Theft.” *The Journal of Consumer Affairs* 38 (2): 233-243.

Spangler, William E, Kathleen S. Hartzel, and Mordechai Gal-Or. 2006. “Exploring the Privacy Implications of Addressable Advertising and Viewer Profiling.” *Communication of the ACM* 49 (5): 119-123.

Spinoza, Benedictus de. 1989. *Ethics*. London: J.M. Dent.

Sprenger, Polly. 1999. “Sun on Privacy: ‘Get Over It.’” *Wired*. Available: www. Wired.com/politics/law/news/1999/01/17538.

Stafford, Marla Royne. 2004. “Identity Theft: Laws, Crimes, and Victims.” *The Journal of Consumer Affairs* 38 (2): 201-203.

Stone, Eugene F. and Dianna L. Stone. 1990. "Privacy in Organizations: Theoretical Issues, Research Findings, and Protection Mechanisms." In *Research in Personnel and Human Resources Management*, Vol. 8. Eds. K. M. Rowland and G. R. Ferris. Greenwich, CT: JAI Press, 349-411.

Suprenanat, Carol F. and Michael R. Solomon. 1987. “Predictability and Personalization in the Service Encounter.” *Journal of Marketing* 51 (April): 86-96.

Sutton-Smith, Brian. 1997. *The Ambiguity of Play*. Cambridge, MA: Harvard University Press.

Taylor, Raymond E., John A. Vassar, and Bobby C. Vaught. 1995. “The Beliefs of Marketing Professionals Regarding Consumer Privacy.” *Journal of Direct Marketing* 9 (4): 38-46.

Thomas, Robert E. and Virginia G. Maurer. 2000. “Database Marketing Practice: Protecting Consumer Privacy.” *Journal of Public Policy & Marketing* 16 (1): 147-155.

Tuerkheimer, Frank M. 1993. "The Underpinnings of Privacy Protection." *Communications of the ACM* 36 (August): 69-73.

Van Den Haag, Ernest. 1971. "On Privacy." In *Nomos 13*. Eds. J. R. Pennock and J. W. Chapman. New York: Atherton Press, 147-153.

Vogel, David. 1992. "The Globalization of Business Ethics: Why America Remains Distinctive." *California Management Review* 35 (1): 30-49.

Wang, Paul and Lisa A. Petrison. 1993. “Direct Marketing Activities and Personal Privacy: A Consumer Survey,” *Journal of Direct Marketing* 7 (1): 7-19.

Wang, Sijun, Sharon E. Beatty, and William Foxx. 2004. "Signaling the Trustworthiness of Small Online Retailers." *Journal of Interactive Marketing* 18 (1): 53-69.

Warren, Samuel D. and Louis D. Brandeis. 1890. "The Right to Privacy." *Harvard Law Review* 4 (5): 193-220.

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

Winer, Russell S. 2001. "A Framework for Customer Relationship Management." *California Management Review* 43 (Summer): 89-105.

Wynne-Edwards, Vero C. 1962. *Animal Dispersion in Relation to Social Behavior*. Edinburgh: Oliver and Boyd.

Zimmerman, Diane L. 1983. "Requiem for a Heavyweight: A Farewell to Warren and Brandeis's Privacy Tort." *Cornell Law Review* 68 (3): 291-367.

Zwick, Detlev and Nikhilesh Dholakia. 2004. "Whose Identity Is It Anyway? Consumer Representation in the Age of Database Marketing." *Journal of Macromarketing* 24 (1): 31-43.

APPENDIX

Fair Information Practices and their Dimensions (FTC 1998)

1. Notice/Awareness – consumers should be given notice of a firm's information practices. The following dimensions of notice have been identified as necessary to ensuring that consumers are properly informed:
    a. Identifying the entity collecting the data
    b. Identifying the nature of the data collected
    c. Identifying the uses to which the data will be put
    d. Identifying any potential recipients of the data
    e. Identifying the means by which the data is collected (if not obvious)
    f. Identifying whether the provision of the requested data is voluntary or required (and the consequences of refusal to provide the requested information)
    g. Identifying the steps taken by the data collector to ensure the confidentiality, integrity, and quality of the data
2. Choice/Consent – consumers should be provided with options as to how they would like their personal information to be used. The following dimensions of choice have been identified as necessary to ensuring that consumers can assert some control over the firm's information practices:
    a. Providing choice regimes (e.g., opt-in or opt-out)
    b. Providing a means for consumers to tailor the kinds of information they revealed
    c. Providing a means for consumers to decide how their personal information will be used
    d. Providing a means for consumers to remove information that has been collected
3. Access/Participation – consumers should be provided with a means to access data about him or herself. The following dimensions have been identified as necessary to providing consumers access:
    a. Providing a simple, timely, and inexpensive way for consumers to view their personal data
    b. Providing a simple means for consumers to contest inaccurate or incomplete data
    c. Providing a mechanism by which the data collector can verify the consumer's information
    d. Providing a means by which corrections and/or consumer objections can be added to the data file and sent to all recipients
4. Integrity/Security – firms must take steps to make sure that consumers' data is accurate and secure
    a. Integrity – the following dimensions have been identified as necessary to data integrity:
        i. Using only reputable sources of data
        ii. Cross-referencing data against multiple sources
        iii. Destroying untimely data or converting it to anonymous form
    b. Security – the following dimensions have been identified as necessary to data security:
        i. Establishing internal organizational measures that limit access to data
        ii. Ensuring that those individual with access do not utilize data for unauthorized purposes
        iii. Using encryption in the transmission and storage of data
        iv. Establishing limits on access to data
        v. Storing data in a secure location (e.g., secure servers and computers)
5. Enforcement/Redress – firms must have mechanisms in place to enforce and punish any violations of the fair information practices. The following dimensions have been identified as alternative ways to provide for enforcement and redress:
    a. Participating in industry self-regulation
    b. Obtaining privacy certification by outside agencies
    c. Agreeing to legislation that would create remedies for consumers
    d. Developing regulations that would enforce privacy protection through civil and criminal sanctions