Consumer Online Privacy: Legal and Ethical Issues

Eve M. Caudill and Patrick E. Murphy

Consumer privacy is a public policy issue that has received substantial attention over the last thirty years. The phenomenal growth of the Internet has spawned several new concerns about protecting the privacy of consumers. The authors examine both historical and conceptual analyses of privacy and discuss domestic and international regulatory and self-regulatory approaches to confronting privacy issues on the Internet. The authors also review ethical theories that apply to consumer privacy and offer specific suggestions for corporate ethical policy and public policy as well as a research agenda.

Tracking the movements of consumers as they shop for goods is not a new phenomenon. Marketers have long collected data to assist in making decisions: They have watched while buyers pick out strawberries and noted the process parents go through to choose a box of cereal. Consumers do not appear concerned about this invasion of privacy; after all, they are in a public place and the information being collected—what they have in their cart and ultimately purchase as well as the products they inspect—can be readily observed. Perhaps this lack of concern is based on their assumption of anonymity; their shopping behaviors are collected to study patterns in the aggregate. When information is collected at the cash register, customers can choose to opt in through the use of a personal shopping card, a credit card, or a check. Presumably, customers knowingly give up some of their privacy in this transaction in return for something of value—a product discount, credit, future coupons on heavily used items, and so forth. Anonymity remains, however, if they use cash and resist requests for their phone number, address, or zip code.

This anonymity changes when consumers move onto the Internet. No longer are their shopping behaviors available only in the aggregate. Instead, individuals are tracked, and information is collected from purchasing transactions as they surf through Web sites. The exchange of value between marketer and consumer becomes less defined in this new retail (now e-tail) setting than it is in a brick-and-mortar store environment. The following questions outline the concerns raised by this shift in exchange venues:

- What are the privacy issues pertinent to online marketers collecting and using a consumer's information?
- What are the ethical responsibilities of online marketers?
- What policy initiatives are needed in this new transactional environment?

Privacy as it relates to consumer information is not a new problem in marketing. The growth of databases, such as Lexis-Nexis, has meant that a virtual "mountain" of information is available on most consumers who use credit cards, own cars and homes, and are active spenders (Cespedes and Smith 1993; DeCew 1997). Use of automated dialing systems, caller ID, and e-mail have brought criticism of marketing research, advertising, and the traditional marketing system (Foxman and Kilcoyne 1993). The direct mail industry has also been targeted for ongoing threats to consumer privacy (Milne and Gordon 1993; Phelps, Nowak, and Ferrell 1999). And on the Internet, well-known companies have been criticized: America Online for attempting to sell subscribers' telephone numbers, and Intel for developing the new Pentium chip that identifies users.

As use of the Internet grows, so do concerns regarding online collection and use of consumer information. In several surveys, respondents have told marketers that questions about privacy affect their purchasing decisions. A U.S. Department of Commerce study tracking e-commerce and privacy finds concern about online threats to privacy among 81% of Internet users and 79% of consumers who buy products and services over the Web (Oberndorf 1998). These percentages reflect the seriousness of the problem and a possible impediment to broad-scale adoption of the Internet for purchasing decisions. For example, Microsoft was hammered by privacy buffs because its Windows 98 software, when used on a network, creates identifiers that are collected during registration, which results in a vast database of personal information about its customers. Microsoft insisted that these features were designed to improve services, but fearing a backlash, the company has promised to modify them. It claimed customers can bow out when they register for Windows 98, and it pledged to expunge personal data it collected improperly (Baig, Stepanek, and Gross 1999) (for several extended examples of consumer privacy concerns, see the Appendix).

The purpose of this article, then, is to assess the current landscape and address future challenges regarding online privacy. As we noted previously, many of the existing marketing and privacy paradigms are challenged in the Internet environment. We examine historical perspectives and contemporary initiatives on consumer privacy in both self-regulation and government regulation in marketing, giving attention to both U.S. and international contexts. Our intended contribution is to offer ethical, public policy, and managerial insights into these perplexing issues facing marketing organizations in the new century. We also set an agenda for further research.

EVE M. CAUDILL is Visiting Assistant Professor of Marketing, and PATRICK E. MURPHY is Professor and Chair, Department of Marketing, University of Notre Dame. The authors thank the special issue editor and the three anonymous *JPP&M* reviewers for their helpful suggestions on previous versions of this article.

A Conceptual Analysis of Privacy

Several legal and philosophical scholars have examined the topic of privacy in the home, in the workplace, and in public. A debate in law and philosophy has centered on whether a narrow (Parent 1983) or broad (DeCew 1997; Schoeman 1992) view of privacy should be used for legal and ethical assessments of individual actions. Fried (1968) wrote one of the first and most important philosophical treatments of privacy. He claims that privacy is instrumentally valuable because it is necessary to develop intimacy and trust in relationships. At approximately the same time, Westin (1967) examined privacy and the fundamental right of freedom. Furthermore, Rachels (1975) argues that people need to control information about themselves to maintain a diversity of relationships. Most recently, Nissenbaum (1998) raises the notion of "privacy in public" that deals with retailers; mail order firms; medical care givers; and other organizations that collect, store, analyze, and share information about consumers. She likens these efforts to a type of public surveillance that "constitute[s] a genuine moral violation of privacy" (p. 593).

Privacy and Legal Issues

Even though the right to privacy was not explicitly mentioned in the Bill of Rights, the topic has been debated for more than a century. In "one of the most influential law review articles ever written" (DeCew 1997, p. 14), former Chief Justice Louis Brandeis and a colleague argued for a broad interpretation of a person's right to privacy (Warren and Brandeis 1890). It appears significant that this article defending consumers occurred in the same year as the passage of the Sherman Act (26 Stat. 209), which deals with antitrust and competitive issues. Furthermore, the First, Third, Fourth, Fifth, Ninth, and Fourteenth Amendments provide for protections that fall under the general rubric of privacy (DeCew 1997; Gillmor et al. 1990).[1] In addition, a substantial body of total law serves to protect individuals' privacy (for a brief review, see Schoeman 1992).

Legal protection for individual privacy in the United States is relatively recent, as the first federal law passed less than thirty years ago. This legislation has been limited primarily to the protection of data in the context of specific government functions or the practices of particular industries, including credit reporting, video rental, and banking (for a list of privacy laws, see Table 1). In the 1970s, protection involved consumer notification and the correction of inaccuracies in consumers' records. Later legislation extended protection to cover unauthorized break-ins and illegal access to electronic record systems. The Fair Credit Reporting Act (1970) covers credit reporting agencies' collection, storage, use, and transmission of credit and financial information (Jones 1991). The Privacy Act (1974) extends these restrictions to government agencies, and the Cable Communications Act (1984) covers cable companies' collection and use of subscriber information. The Computer Security Act (1987) outlines minimum acceptable security plans for federal agencies with computer systems. Finally, the Video Protection Privacy Act (1988) requires subscriber consent for the disclosure of video sales and rental information (Bloom, Milne, and Adler 1994). The 1990s has seen only sporadic attempts to protect privacy at the federal level. This brief discussion shows that the majority of U.S. businesses are not regulated in their collection and use of customer data.

Consumer Privacy

Consumer privacy, a subset of privacy, has been described as both a two-dimensional construct, involving physical space and information (Goodwin 1991), and a continuum, contingent on consumers and their individual experience (Foxman and Kilcoyne 1993). A continuum suggests that consumers have varying degrees of concern with privacy and place different values on their personal information; therefore, some consumers may be willing to trade away information for a more valued incentive. An illustration of those trade-offs involves Catalina Marketing Corporation, which offers a variety of incentives to induce consumers to provide personal information. For example, a person's zip code and preferred supermarket is worth $40 of national coupons, and a personal shopping card number garners free products (Quick 1998; Thomas 1998).

As previously stated, consumer privacy is confined to the context of information and includes Foxman and Kilcoyne's (1993) two factors of control and knowledge. Thus, the violation of privacy depends on (1) consumers' control of their information in a marketing interaction (i.e., Can consumers decide the amount and the depth of information collected?) and (2) the degree of their knowledge of the collection and use of their personal information. In Figure 1, we describe consumers' control and knowledge applied to the Internet; included in this taxonomy are two behaviors consumers engage in on the Internet: purchasing and surfing. We also list issues pertinent to each cell according to whether consumers have control and/or knowledge when accessing the Internet.

Use of the Internet

Internet use has grown exponentially in the 1990s. Although it was negligible in the mid-1990s, use by North American consumers had risen to almost 60 million by 1997. More than 80 million U.S. citizens were using the Internet in 1999. Online use is predicted to expand as technology decreases the barriers for nonadopters and advances capabilities for current users, such as video and voice support. However, only a modest number of people accessing the Internet are actually purchasing goods or services through a Web-based transaction. When asked why they do not, consumers report a fear that companies will misuse personal information.

Along with some shopping, users increasingly access the Internet because of its "decentralized, open and interactive nature" (Center for Democracy and Technology 1999). People can create communities, communicate ideas, engage in commerce, and search for information with unprecedented freedom and ease. These factors bring a downside for

[1]The various amendments deal with several aspects of privacy: First, freedom to teach and give information; Third, protection of one's home; Fourth, protection of the security of one's person, home, papers, and effects; Fifth, protection against self-incrimination; Ninth, rights shall not be construed to deny or disparage others retained by people; and Fourteenth, the due process clause and concept of liberty (DeCew 1997, pp. 22–23).

Table 1. U.S. Federal Regulation on Privacy

Act	Year	Description
Fair Credit Reporting Act	1970	Allows consumers to correct errors in their credit reports.
Privacy Act	1974	Government officials may not maintain secret files or gather information about people irrelevant to a lawful purpose.
Right to Financial Privacy Act	1978	Government officials need a warrant to obtain a bank's copies of checks.
Electronic Transfer Funds Act	1980	Banks must notify customers when disclosing records to third parties.
Privacy Protection Act	1980	Government officials are restricted in their ability to seize records of the print media.
Cable Communications Act	1984	Cable companies may not disclose choices customers make or other personal information without consent.
Family Education and Privacy Right Act	1984	Government officials are restricted in their ability to reveal to third parties information gathered by agencies or educational institutions.
Computer Security Act	1987	All government agencies develop safeguards for protecting sensitive data stored in their computers.
Electronic Communications Privacy Act	1988	Prohibits telephone, telegraph, and other communications services from releasing the contents of messages they transmit (only the recipient of the message can be identified).
Video Privacy Protection Act	1988	Video rental companies may not disclose choices customers make or other personal information without consent.
Computer Matching and Privacy Protection Act	1988	Allows governmental officials to increase the amount of information they gather if the safeguards against information disclosure also increase.
Telephone Consumer Protection Act	1991	Prohibits telemarketers from using automatically dialing telephone calls or facsimile machines to sell a product without obtaining consent first.
Drivers' Privacy Protection Act	1993	Places restrictions on state government agencies and their ability to sell driver's license records.
Children's Online Privacy Protection Act	1998	Sets rules for online collection of information from children.

users. Because their activities are conducted electronically, consumers leave a trail of information that includes not only purchasing information but also data pertaining to their interests and activities, which allow online marketers the opportunity to develop profiles of individual users.

Marketers employ a variety of online collection techniques, including mining e-mail addresses from list servers, chat rooms, and news groups. A particular advantage of the Internet, however, is its ability to collect real-time behavioral data, which are accessed through the use of cookies.[2] This collection method, called "profiling" (see the subsequent discussion), updates a consumer's profile after every Web site visit with information such as the home pages that were visited, the information that was downloaded, the type of browser that was used, and the Internet addresses of the sites that referred consumers to a particular Web site (FTC 1998; Mahurin 1997). Even more powerful software now can follow consumers and collect off-site data. For example, DoubleClick, a developer of Internet software, has devised a tool that extends the reach of these cookies and enables advertisers to follow the behavior of users from their original Web sites to others (Quick 1998).

Overview of Online Privacy Regulation

These increasingly sophisticated data collection methods have raised concerns about consumer privacy, and considerable interest has emerged in developing some type of regulatory structure to ensure privacy on the Internet. Although several groups are involved in this process, the Federal Trade Commission (FTC) has currently taken the lead in developing standards of compliance for companies marketing on the Internet. The commission prepared a major report to Congress in 1998 titled *Privacy Online.* In late 1999, the FTC and the Commerce Department convened a workshop on the topic of online profiling with representatives from Internet advertising and data collection firms, academics, and privacy advocates.[3] The primary reservation expressed

[2]Cookies are text files that are saved in a user's browser's directory or folder and stored in random-access memory while that browser is running. When visiting a Web site, a user is assigned a unique identifier, that is, a cookie (not the actual identity of the consumer), which will identify that user in subsequent visits.

[3]Online profiles of consumers are created through the compilation of their preferences and interests; these profiles are then used to develop advertisements targeted to these consumers on subsequent Web site visits.

Figure 1. Control and Knowledge of Online Surfing and Purchasing Activities

Consumer Knowledge \ Consumer Control	No	Yes
No	**Surfing** •Movements tracked by software. •Consumer no longer owns information. **Purchasing** •Use credit card, no privacy statement. •Consumer no longer owns information.	**Surfing** •Technology solutions, consumer can dismantle tracking software. •General control maintained. **Purchasing** •Use cash (not feasible online), technology. •General control maintained.
Yes	**Surfing** •Able to access privacy statement, no opt-in and opt-out options, no technology solutions. •Consumer no longer owns information. **Purchasing** •Have to use credit card. •Privacy statement, no opt-out. •Consumer no longer owns information.	**Surfing** •Able to access privacy statements, opt-in and opt-out options, technology solutions. •Consumer owns information. **Purchasing** •Able to access privacy statement with opt-out option if using credit card, ability to pay cash with opt-in option. •Consumer owns information.

by the participants was the potential for consumer privacy violations. The FTC chairman suggested that the issue is troubling and warrants further examination (Guidera 1999).

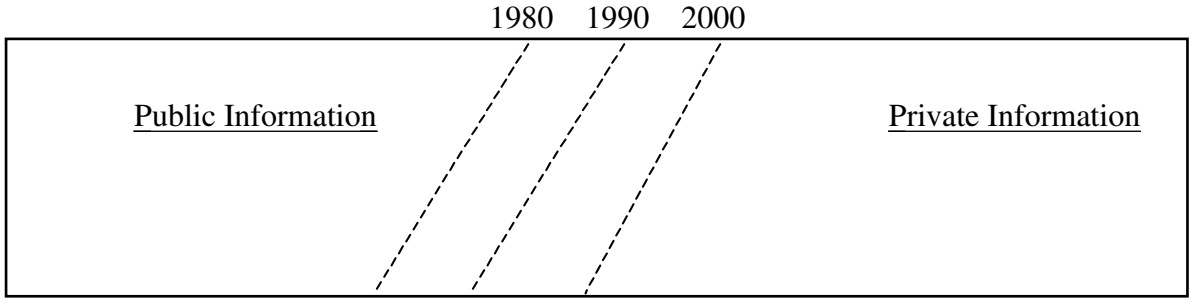
One overriding concern is defining the concept of personal information. A general definition, "data not otherwise available via public sources" (Beatty 1996, p. B1), is thought to be too broad, because it would exempt public records such as home and car ownership and allow for the access, use, and dissemination of that information by third parties. In its report to Congress, the FTC delineated personal information more specifically as (1) personal identifying information, such as a consumer's name, postal address, or e-mail address, and (2) aggregate, nonidentifying information used for purposes such as market analysis or in conjunction with personal identifying information to create detailed personal profiles of consumers, such as demographic and preference information (FTC 1998).

These definitions do not adequately characterize consumer information.[4] Therefore, instead of defining personal information as the opposite of public space or as the sum of identifying and nonidentifying information, our conception of consumer information encompasses both public and private information (see Figure 2). Thus, personal information includes both public (e.g., a drivers license, mortgage information) and private (e.g., income) data. The dotted line allows for the shifting of personal information from private to public; the public portion of personal information is thought to be growing as the Internet increases the ease with which consumer information can be gathered and disseminated.

Who bears the responsibility of ensuring consumer privacy is a second concern. In debate is whether there should be industry self-regulation, technology-based solutions, consumer and business education, and/or government regulation (FTC 1998). Currently, the FTC endorses industry self-regulation. To ensure success, the FTC has developed five fair information practice principles that would protect consumers in the collection, use, and dissemination of their information:

[4]This section benefited from a faculty seminar at the University of Notre Dame, in which several participants gave helpful comments regarding public versus private information.

Figure 2. Consumers' Personal Information Model



Notes: The dotted lines represent the transition of a greater portion of consumers' personal information from the private to the public realm. This shift is thought to be the result of an increased use of databases (early 1990s) and the Internet (late 1990s) as means to collect and manipulate consumers' information.

1. Notice/awareness: covers the disclosure of information practices, including a comprehensive statement of information use, that is, information storage, manipulation, and dissemination;
2. Choice/consent: includes both opt-out and opt-in options and allows consumers the choice to trade information for benefits, depending on the value consumers place on the benefits;
3. Access/participation: allows for confirmation of the accuracy of information; necessary when information is aggregated from multiple sources;
4. Integrity/security: controls for theft or tampering; and
5. Enforcement/redress: provides a mechanism to ensure compliance by participating companies; this mechanism is an important credibility cue for online companies but is extremely difficult to accomplish effectively (FTC 1998).

Of these principles, the issue of disclosure (under notice/awareness) is central to privacy and covers whether or not consumers are informed of collection methods and information use. The current self-regulatory environment suggests that each company is responsible to develop its own disclosure statement, with varying levels of notice, choice, access, and security. Thus, individual firms decide the degree of information collection and use along with the type and structure of disclosure. This lack of regulatory standardization suggests that the responsibility to assess the privacy practices of Web site operators falls to the consumer and that there is limited enforcement and redress.

Approaches to Internet Regulation

As discussed previously, legal protection for consumer privacy historically has focused on industries thought to be particularly egregious in the collection and use of personal information. Unlike these more static industries, however, in which regulatory actions are reasonably easy to control, the Internet is experiencing rapid growth, which limits government enforcement. Even the FTC questions the scope and extent of the government's powers to pursue regulatory responsibility. The difficulty in regulating online privacy is a central issue debated among self-regulators, government regulators, and privacy advocates.

Industry Self-Regulation

Several arguments have been advanced that government involvement would hurt rather than help consumers and businesses (Miller 1998). First, consumers might get a false sense of privacy if laws were passed that could not be enforced because of the dynamic nature of Web site creation (James 1998). Second, government regulation would interfere with the flow of consumer information that enables companies to provide products and services that cater to the needs and wants of their customers, which would result in decreased consumer choice and diminished competition. Furthermore, mandatory opt-in and restrictions on the sale of customer information could create barriers to entry that would favor older, more established companies that have years of collecting information and developing databases (Brandt 1998). Newer companies would be at a disadvantage if they were not allowed to purchase information. Third, consumers would lose their right to choose their desired level of privacy. Recall that some consumers welcome the collection of their information and willingly sell it if they are provided the right incentives. Finally, government intervention might violate free speech. The information used in the creation of databases is similar to gossip (Singleton 1998), which is protected under the First Amendment, and might be less harmful because the information in databases is likely more accurate, less personal, and so forth.

Self-regulation advocates argue that consumer information is the foundation on which businesses can succeed and allows them to develop markets based on their customers. Furthermore, these advocates contend that the collection and use of this information harms consumers only by being an annoyance, which is not considered reason enough to call for stricter regulatory measures. A breakthrough in the self-regulatory arena occurred with the announcement by IBM in March 1999 that the company would pull its Internet advertising from any Web site in the United States or Canada that did not post clear privacy policies within 60 days (Auerbach 1999). Only 30% of the 800 sites on which IBM advertised at that time made such disclosures.

Seeing the potential for consumer confusion regarding the effectiveness of self-regulation, a new vehicle (third-party intervention) has emerged. Third-party entities have formed to provide legitimacy and trustworthiness to Web sites through seals of approval that are designed to confirm adequate privacy compliance (see Table 2). Three such entities are TRUSTe, the Online Privacy Alliance, and the Council

Table 2. Third-Party Entities

	Goals	Limitations
TRUSTe	Provides guarantee of privacy protection: 1. Gives a seal of trust to Web sites that submit to application process. 2. Acts as a clearinghouse for privacy violation reports. 3. Provides a children's privacy seal program.	1. Limited industry compliance. 2. Critics suggest that guidelines go further in protecting privacy.
BBBOnline	Provides seal of approval to Web sites that adequately perform through a self-assessment and pay a fee.	1. Voluntary nature of member company compliance. 2. Enforcement.
Alliance for Privacy	Publishes guidelines for member companies to follow in the collection and dissemination of information.	1. Voluntary nature of member company compliance. 2. Enforcement.

of Better Business Bureaus, Inc. (BBBOnline). TRUSTe is an industry-launched initiative supported by such companies as AT&T, America Online, Netscape, Oracle, *Wired*, and Tandem Computers (Bayne 1998; Wientzen and Smith 1998). Similarly, the Online Privacy Alliance is a coalition of 85 marketers, technology firms, and associations, including Time Warner, Walt Disney, America Online, and IBM. The BBBOnline offers a distinct seal for sites with advertising for children and will take action against companies that do not comply (Ohlson 1999).

The effectiveness of these organizations has been questioned. Of concern is the scope of their enforcement programs and compliance; that is, do they provide the muscle required to set up an environment that benefits consumers given the enormity of the Internet? Issues include membership numbers, requirements, and compliance, as well as the long-term missions of these organizations (Wigfield 1999b). For example, TRUSTe is revising its licensing agreements, which may change consumers' protection levels. Some critics argue that TRUSTe flunked its first big test when the organization failed to reprimand Microsoft (a $100,000 corporate partner) for putting an identifier on Windows 98 (*New York Times* 1999). Although the effectiveness of these third parties has been questioned, the FTC recently has testified that sufficient progress is being made toward self-regulation, postponing further governmental action at this time (FTC 1999; Heckman 1999).

U.S. Government's Position

The Clinton administration and the FTC advocate self-regulation of commercial collection and use of consumer information on the Internet (FTC 1998; Harmon 1998b; Messmer 1998). The administration believes that the flexibility self-regulation gives to businesses is important to the success of Internet commerce. In a 1999 report to the Subcommittee on Communications, the FTC stated that "self-regulation is the least intrusive and most efficient means to ensure fair information practices online, given the rapidly evolving nature of the Internet and computer technology" (FTC 1999, p. 4). As discussed previously, it will continue to monitor the progress of self-regulation because of challenges still facing the industry (*DIRECT Newsline* 1999; Wigfield 1999a). These challenges include educating those companies that underestimate the need for privacy and creating incentives for greater implementation, as well as educating consumers about privacy protection (FTC 1999).

Although the government's position appears favorable to self-regulation advocates, they continue to lobby for a completely hands-off position. They point out that though the FTC may favor self-regulation, history indicates otherwise. One example cited is former FTC commissioner Christine Varney's position that voluntary systems of standards or ratings, whether for privacy or content, should be backed up with strong government enforcement against misstatement as either deception or fraud (Singleton 1998).

The European Union's Privacy Initiatives

Of great interest in the privacy debate are the recent actions taken by the European Union (EU), which has just tightened its privacy laws. It passed a treaty-like directive in 1995, which should have gone into effect October 24, 1998, intending to harmonize privacy protection in all of its 15 member countries (Harbert 1998; Heckman 1999; Messmer 1998). This directive requires adequate privacy protection from the countries of businesses exporting personal information from these 15 countries. The upshot of the directive is that U.S. companies such as hotels, airlines, and banks doing business in Europe cannot transfer information from Europe to the United States (Leibowitz 1999; Swire and Litan 1998). Accordingly, destination countries must have privacy protections the EU deems adequate, which include two components: a national privacy law covering both the public and private sectors and enforcement capabilities through national regulatory agencies.

The EU directive, which takes a more consumer-oriented focus than U.S. companies do, is structured in when and how a company can collect and use consumer information (Harbert 1998). First, a company should have a legitimate and clearly defined purpose to collect information. Second, that purpose must be disclosed to the person from whom the company is collecting information. Third, permission to use information is specific to the original purpose. Fourth, the company can keep the data only to satisfy that reason; if the company wants to use the information for another purpose, it needs to initiate a new information collection and use process. As it stands now, only a few U.S. companies (e.g., Citicorp, American Express; Leibowitz 1999) could meet these criteria, and adoption of these standards may have a chilling effect on Internet marketing.

Enforcement for the EU's directive has been delayed for two reasons (Heckman 1999). First, only about half of EU member countries have passed laws enforcing the directive. Second, the EU currently is negotiating with the U.S. Department of Commerce on Safe Harbor provisions for U.S. companies.[5] These negotiations will eventually result in the formulation of a Safe Harbor program acceptable to European officials. Although both groups agree on the principles (the same as FTC fair information principles), including recognition that U.S. firms will be limited in selling databases, the designated enforcement body to regulate U.S. firms continues to be a major obstacle. When implemented, Safe Harbor programs will guarantee that those companies admitted into the program can be assumed to be in compliance and will be allowed to compete in Europe.

Privacy Advocates' Position

Two primary concerns dominate privacy advocates' argument against self-regulation: the voluntary nature of industry compliance and the degree of consumer knowledge and control of information collection and use (Rotenberg 1998). The voluntary nature of compliance is especially important to privacy advocates, who argue that businesses do not always compete with consumers' best interests in mind; it is more likely that the degree to which a business complies is based more on its own profit objectives. It is argued further that even firms that make a commitment to privacy may at times compromise privacy standards if it is competitively necessary. Privacy advocates point to low compliance rates

[5]Safe Harbor programs will be sets of rules created by industry organizations for their members and designed to comply with various FTC regulations; if a company is admitted to a Safe Harbor program, it is assumed to be in compliance.

among new members of the Direct Marketing Association and question consumers' ability to opt-out, arguing that little prevents members or nonmembers from accessing the information contained in that database (Jones 1991; Rotenberg 1998).

Conflicting data over compliance to FTC regulatory standards exist. The FTC reports low compliance: Of the 1400 sites it has analyzed, 92% of the commercial sites collect personal data, yet only 14% provide notice of information collection practices, the most basic of its privacy principles (FTC 1998). Another survey finds that only half of all Web sites surveyed provide information (and only 10% meet FTC standards) on collection and use practices. However, a third study indicates 94% of the top 100 Web sites in compliance with disclosure standards (Wigfield 1999a, b).

The Georgetown Internet Privacy Policy Survey (1999), a recently conducted progress report to the FTC, finds that the majority of Web sites visited (93.4%) collect either personal identifying or demographic information from consumers. At least one type of privacy disclosure statement (either a privacy policy notice or an information practice statement) is posted on 65.9% of the sample Web sites. The majority of Web sites that collect consumer information and post a privacy disclosure include at least one survey item for notice (89.8%), more than half include a survey item for choice (61.9%), and less than half include a survey item for security (45.8%) and contact information (48.7%).

Even with the disclosure of privacy statements, confusion can arise from the vague and often ambiguous nature of some of them. For example, the Direct Marketing Association's privacy statement on its Web site does not address its policy for collecting tracking information and is unclear about the use of this information. Its policy states, "the information we collect is used to improve the content of our Web page and to contact customers for marketing purposes," though "marketing purposes" is not further explained.

Consumers' lack of knowledge and control of what happens to their personal information is a second concern. The dynamic nature of information collection and manipulation decreases consumers' ability to keep track of their information as it is collected and aggregated from multiple sources to create consumer profiles. Although some of these data are provided by consumers (e.g., demographic information), other information is collected without consumer knowledge, such as tracking information obtained through Web site surfing behavior. Thus, consumers control only a portion of their own profiles.

Privacy advocates warn that consumers' negative perceptions resulting from this lack of control may act as a deterrent to the commercial success of the Internet. A study conducted over the Internet by Georgia Tech finds that privacy is the most important issue facing the Internet (Kantor 1998). A *BusinessWeek* survey finds that people who do not use the Internet cite privacy of their personal information as the primary reason (FTC 1998; Oberndorf 1998; Rotenberg 1998). This lack of confidence parallels consumers' perceptions about the direct marketing industry. A few years ago, the editorial director of *Target Marketing*, citing a "lack of respect on the part of direct marketers" for consumers, pleaded with marketers to consider the effect of their actions in the long run, in terms of both consumer disillusionment and possible government intervention (Jones 1991). A similar disregard is sometimes expressed by online businesses in words and actions. For example, Sun Microsystems chief executive officer Scott McNealy glibly stated, "You already have zero privacy. Get over it" (Baig, Stepanek, and Gross 1999, p. 84).

Unresolved Issues

What is known about privacy on the Internet is that consumers appear concerned about threats to their online privacy, and many companies have been slow to respond. At issue is the perceived ownership of consumer information. Companies' actions suggest that the information, either acquired as part of a transaction or purchased from other sources, belongs to them. As discussed previously, research has shown a lack of voluntary compliance to even the most basic of the FTC's Principles—the right of consumers to be given notice of an entity's privacy practices (FTC 1998). The absence of comprehensive policies is particularly troubling, because consumers do not always understand that complete disclosure has not been included in a privacy statement. This minimalist approach can be seen in the DMA's privacy statement, which outlines its practices for just one subset of information collection and use. A Web site's collection of information through the use of cookies is in obvious violation of the notice/awareness principle, because the majority of consumers do not know the "nature of the data collected and the means by which it is collected" (FTC 1998, p. 8). Furthermore, consumers are not given the option to refuse to participate, because it is their real-time behavior that is being collected.

A consumer's inability to decide whether to proceed suggests an asymmetrical relationship in which the marketer benefits at a cost to the consumer, though some might argue that consumers will benefit through targeted products and services in the long run. Thus, what they do not know will not hurt them in the short run. This asymmetrical relationship is further exacerbated by the lack of a mutually beneficial compensation structure. Traditional information collection methods provide a payment, an incentive to entice respondents to participate, and allow those who do not want to participate to drop out. Similar is the process of engaging in a transaction with a marketer. Consumers participate only with marketers they perceive as providing value. Thus, in both these scenarios, the consumer enters into a transaction in the short run, and possibly the long run, if the arrangement is mutually beneficial. We suggest that it is the consumer's knowledgeable participation in the marketing activity that separates traditional information collection methods from those used online.

Two of these online activities warrant further discussion. The first issue involves the collection and use of consumers' information. Collecting aggregate data on consumer Web site surfing behavior, in isolation, is of negligible harm to those being tracked because of the seemingly innocuous nature of the use of the information—for example, to design Web sites better or provide advertisements targeted more accurately at users. Even the collection of transactional data is thought to be beneficial—for example, when revisiting Amazon.com, a visitor gets a suggested list of books based on previous purchases. Justification of these activities comes largely from the use of a utilitarian argument: The use of this information in the context of marketing provides better goods and services to the community as a whole and

thus justifies the minor inconveniences that some may suffer (Foxman and Kilcoyne 1993).

The question is not about what is being collected or even how the data are collected but the knowledge and control of the participants in those activities. America's largest retailer, Wal-Mart, which has a customer database second only to the federal government, continuously collects information on its customers' purchasing behavior (Nelson 1998). The difference is that consumers stay in the aggregate at Wal-Mart, and individual consumers can self-select (i.e., opt in) data collection activities at the checkout counter if the offered incentive is of sufficient value. Thus, consumers maintain control.

A second issue, then, is value to the consumer. Although some online activities require opting in (e.g., consumers knowingly trade away information for convenience and selection when they provide credit card numbers), other trade-offs are not so obvious. Consumers have limited knowledge, for example, when their surfing behavior is collected and limited control when these surfing data are linked to transactional and demographic data. Several questions arise. What is the value derived by consumers in these types of activities? Is the value limited or is there some value gained from consumers' information being collected and used? If there is some value—for example, better Web sites—is the value commensurate with that obtained by the marketer that collects and uses that information? If no value is obtained from the activity—that is, at the minimum, a discount or a coupon—is the marketer taking equity from the relationship, and at what point will the consumer become frustrated enough to decide not to participate? Information obtained by marketers without providing equivalent value to customers and the subsequent feeling of a loss of control by these customers suggest a future point at which consumers may demand retribution, through either government action or boycott.

The Special Case of Children

The Children's Online Privacy Protection Act (COPPA; 112 Stat. 2681) was passed in October 1998 because of concerns regarding online marketing practices aimed at children.[6] FTC research in June 1998 found low industry compliance with its Fair Practice Principles, such as the inclusion of information practice statements (e.g., "Kids, get your parents' permission before you give out information online") and privacy notices as well as parental notification. This report also indicated that information such as age/birth date, sex, hobbies, interests, and hardware/software ownership was collected more from children than from adults. A particular concern with these findings is the limited cognitive abilities of children, which suggests that they may be more motivated by the incentives intended to get their information (e.g., postcards, freebies) than by the information provided in the privacy statement.

Although COPPA prohibits the collection of personally identifiable information for children 13 years of age and younger from Web sites unless the children obtain verifiable permission from their parents (Heckman 1998), questions arise about its ability to protect and about what is to be protected. Unclear is the definition of "information"—Does it include information provided by children, or does it also include the collection and use of all their personal and behavioral data? Also questioned is the difficulty of verifying the child's age and parental consent, as well as the FTC's limited ability to enforce these requirements.

The final rules for COPPA were outlined by the FTC in October 1999, which further strengthened the online privacy of children (Children's Online Privacy Protection Rule 1999). These rules, effective April 21, 2000, require operators of Web sites targeting children under 13 years of age to (1) post prominent links on their sites to notices outlining the collection, use, and/or disclosure practices involving personal information; (2) notify parents about collection practices and obtain their consent before information collection, use, and/or disclosure; (3) cease the practice of linking children's participation in online activities to the collection of additional personal information; (4) allow parents the opportunity to review information on their children, delete this information from databases if desired, and prohibit further collection of information; and (5) formulate procedures to protect the confidentiality, security, and integrity of personal information.

Ethical Theories and Online Privacy

The importance of marketer responsibility in a transaction is not only to complete this particular exchange but also to ensure future exchanges that will build into a relationship. Cespedes and Smith (1993, p. 9) state that companies cannot afford to waste resources on marketing activities that "annoy or alienate potential customers." Consumers continue to visit a particular business because of the perception of trust, that is, that the company has their best interests in mind when providing a product and/or service. We discuss several ethical theories as vehicles to strengthen the bond of trust between marketer and customer.

Social contract theory suggests that a reciprocal relationship exists among those involved in an exchange (Dunfee, Smith, and Ross 1999). At a higher societal level, a social contract might involve the advantages offered by a firm "to society—its customers and employees—in exchange for the right to exist and even prosper" (Dunfee, Smith, and Ross 1999, p. 17). This theory is particularly important to marketing, in which transactions are based on each party believing that value has been obtained. When applied to direct marketing, social contracts are formed when consumers provide information to marketers for the benefit of receiving targeted offers (Milne and Gordon 1993). A social contract is initiated, therefore, when there are expectations of social norms (i.e., generally understood obligations) that govern the behavior of those involved.

Social contract theory applies to the Internet for the same reasons suggested for direct marketing: Consumers opt in to a particular activity from which they perceive future information streams will be of value. The transaction occurs

[6]The COPPA should not be confused with the Child Online Protection Act that makes commercial Web sites criminally liable if minors have access to obscene or indecent material (Raysman and Brown 1998).

when a consumer provides information to an organization and the marketer in turn offers an incentive to the consumer; both of these actions are initiated after an evaluation of the specifics of that particular contract. Implied here is the presence of two parties in the transaction in which information is exchanged for the promise of some benefit, whether present or future. One generally understood obligation accruing from entering into this social contract is that both parties understand the risks involved as well as the returns. Thus, the consumer, in conducting a cost–benefit analysis, enters into an exchange that provides positively perceived benefits, which may not be unduly affected by privacy concerns. Consumers, instead of following an absolute philosophy of "I want to be left alone," as privacy advocates contend, might just want "protection against unwarranted uses of personal information with minimal damage" (Cespedes and Smith 1993, p. 8).

Duty-based theory includes three categories of obligations. First, the duty of fidelity (Laczniak and Murphy 1993) requires companies to tell the truth and redress wrongful acts without delay. It enables companies to build a bond with their customers, who then come to associate these companies with ethical behavior, which most likely results in positive word of mouth and repeat business. Much of the previous discussion regarding online regulatory standards involves the question of how much a company must disclose of its practices. The recent meeting regarding online profiling sponsored by the FTC appears to be an indicator that companies in the industry are now accepting this duty.

Second, the duty of beneficence is the obligation to do good. In the context of online marketing, companies would not track the behavior of their customers because of their duty to do right by these customers. This duty might also include providing a complete disclosure of information collection and use and to provide an opt-in rather than an opt-out system. In this system, marketers would track only those online consumers who were willing to participate.

A third duty involves that of nonmaleficence, the duty not to injure others. This duty covers the FTC's Fair Information Practice Principle of integrity/security. By instituting measures that maintain the security and integrity of consumers' information, marketers ensure that these consumers are safe from harm to their financial state or even to their personal reputations, thus mitigating consumers' reluctance to participate in Internet activities.

Stakeholder theory postulates that those who have an interest in or are affected by an organization have a stake in its decisions (Donaldson and Preston 1995; Goodpaster 1991). The rights of stakeholders regarding organizational privacy have been examined by Stone and Stone-Romero (1998). In the context of online marketing, the stakeholders include the organization itself, as well as consumers, privacy advocates, self-regulation advocates, the government, and, finally, cyber (as opposed to any national) society, whose norms govern expectations of the right to privacy. For the primary stakeholders, customers value some degree of privacy and expect trust in the transaction, whereas some companies place the greatest value on short-term profit generation. The rights of the secondary stakeholders also conflict with the needs of advocacy groups, the government, and societal attitudes in disagreement over the degree of privacy accorded, all of which will affect the behavior of both stakeholders and government. Thus, fairness dealing with the trade-offs among these often conflicting rights will be important to Internet success.

Virtue ethics is another ethical theory relevant to online consumer privacy. Although virtue ethics possess several characteristics (Murphy 1999), the one most relevant for online marketers is the "ethic of the mean," which states that balance is an objective in any relationship—excess is to be avoided. Aristotle, one of the earliest proponents of virtue ethics, indicated that deception is the deficiency of truth, whereas boastfulness represents the excess of truth. A virtuous position is one that strives for middle ground. As prescribed by social contract and stakeholder theories, marketers, public policymakers, and consumers must strive for this delicate balance among marketing goals, consumer privacy, and the public good. Privacy advocates and some companies are taking extreme and adversarial positions without recognizing the importance of balance. Initial positive steps have been made with COPPA, the IBM advertising initiative, and third-party interventions.

In the international arena, applying virtue ethics to online privacy is difficult. The EU has taken a stronger stance than the United States in protecting consumer privacy; one commentator indicated that the United States should "consider importing Europe's more evolved and balanced conception of privacy" (Kuttner 1998, p. 22). Yet a compromise must be reached between the EU and the United States if there are to be viable rules for global commerce.

The power–responsibility equilibrium model (Laczniak and Murphy 1993) might shed some light on these questions for the participants in an online marketing transaction. Power and responsibility should be in equilibrium—whichever partner in a relationship has more power also has the responsibility to ensure an environment of trust and confidence. According to the model, if a company chooses a strategy of greater power and less responsibility, it might benefit in the short run (though the consumer with less power will not benefit); however, that company will lose power in the long run (e.g., increased government regulation). In contrast, a company in balance with its customers should benefit both in the short run and the long run. When large companies require Web sites to post a privacy statement, this action represents a good example of a company with greater power accepting its responsibility.[7]

Future Policy Directions

Although it seems premature at this point to offer definitive directions regarding consumer online privacy, both Web marketers and public policy officials should consider several alternative possibilities. Figure 3 depicts each of the policy proposals examined here on an ethical responsibility continuum. The various ethical theories discussed previ-

[7]Although Microsoft has come under criticism in the past for its lack of emphasis on privacy matters, the company has assumed greater responsibility recently. In June 1999, it put in place a policy similar to IBM's and has included its privacy activities on the company Web page.

Figure 3. Ethical Responsibility Continuum

Business Orientation ⟷ Societal Orientation

Theories	Corporate Business Policy	Corporate Ethical Policy	U.S. Public Policy	EU Public Policy
Managerial egoism[a]	X			
Utilitarianism[b]	X	X		
Stakeholder theory[c]	X	X	X	
Virtue ethics[d]		X	X	
Integrative social contracts theory[e]		X	X	
Duty-based theories[f]			X	X
Power and responsibility[g]	X	X	X	X

[a]Managerial egoism: Executives take steps that most efficiently advance the exclusive self-interest of themselves or their firm. The X is placed under corporate business policy because the sole motivation is to further the firm; trade-off incentives are offered for the purpose of obtaining consumer information that is viewed as the property of that company.

[b]Utilitarianism: Corporate conduct is proper if a decision results in the greatest good for the greatest number of people. Self-regulatory advocates maintain that consumers are not hurt by corporations' collection and use of personal information but are annoyed (the costs are low); furthermore, the information allows for a wide assortment of product choice (benefits are great).

[c]Stakeholder theory: Organizations affect and are affected by several stakeholder groups. On the continuum, this theory ranges from corporate business policy, because of the effect of corporate actions on consumers (e.g., incentive trade-offs), to corporate ethical policy, because of the positive influence of privacy statements and privacy audits on many stakeholders, to public policy, because government and society are seen as important stakeholders.

[d]Virtue ethics: Balance in the relationship between the online marketer and the consumer should be achieved for the market system to work effectively. Thus, corporations and public policymakers need to move toward the ethic of the mean in the privacy debate.

[e]Integrative social contracts theory: This theory presupposes that the Internet community precedes the development of rules of conduct, public policy, or "microsocial contracts." Corporate ethical policies assume that the corporation's participation in the development of social rules would necessitate transparent ethical practices.

[f]Duty-based theories: The normative nature of these theories means that they are used by policymakers in determining the company's absolute duties to consumers. If the duties of fidelity, beneficence, and nonmaleficence are violated in the course of Internet marketing, greater participation by regulatory agencies in the United States and Europe can be expected.

[g]Power and responsibility equilibrium: Corporate power and responsibility must be approximately equal for Internet marketers to be effective; in the long run, those who do not use power in a way that society considers responsible will lose it. This covers the entire continuum, because it incorporates organizational stakeholders and includes the multiple public policy perspectives.

ously are arrayed and explained as to their relevance to online privacy questions.

Corporate Business Policy

Before examining broader ethical and public policy implications, we briefly outline the progress companies have made toward increased online privacy. It appears that more business firms are putting in place mechanisms that protect consumer online privacy or offer benefits to consumers who are willing to trade off some of their privacy rights. For example, several major auto manufacturers are experimenting with online market research, which asks in-depth questions of potential consumers about both their lifestyles and their demographics as well as past purchasing patterns. In return, respondents are offered vouchers for several hundred dollars to be used on any of the firms' products. This open exchange of information for substantial monetary compensation begins to mitigate some of the ethical and policy concerns examined in this article. Amazon.com's attempt to alleviate fears about sharing credit card and personal information over the Internet by adding a "guarantee" button to its home page (which lists the firm's security assurances and an option to telephone in the last five digits of the consumer's credit card) is an example of concern with the integrity/security of consumer information (Zeller et al. 1999).

Corporate Ethical Policy

In the spirit of the ethic of the mean and the substantial self-regulatory initiatives already in place, some specific corporate actions seem necessary to protect consumer privacy in an online environment. Although the following proposals have not been applied specifically to this context, the approach follows the position advocated by Phelps, Nowak, and Ferrell (1999, p. 43), who state that marketers should adopt a proactive stance in alleviating consumer concerns about privacy. Possible corporate policies are

- Privacy statement: Every Web marketer should have an explicit policy statement on privacy. Ideally, it should not be a legalistic document but one that could be easily understood by a layperson. Similar to other ethics statements, the privacy statement should be widely communicated, regularly revised, and even promoted (Murphy 1998).
- Privacy audit: Companies should go to greater lengths in studying the methods they use to collect, store, and disseminate consumer information. In some cases, such an audit will probably lead to the conclusion that consumers should be informed if the firm plans to sell their information to third parties.
- Privacy technology: New technologies that enhance privacy rather than weaken it should be adopted if possible. The leading marketers and advertisers on the Web could set a higher standard than currently exists. Some of these new technologies include software that ensures anonymity on the Internet, encryption of messages and transactions, and audit trails that determine who accessed a file and thus deter unauthorized queries (Etzioni 1999).

Public Policy

The policy arena for online privacy is a global one; international regulation, rather than just U.S.-based public policy, is likely the long-term answer. Therefore, future initiatives should strive for input across nations. The fundamental disagreement between Americans (who generally distrust government) and Europeans (who usually place little faith in self-regulation) means that the needed compromise between the EU Privacy Policy and the United States continues to be assessed. However, the realities of a new century are that at least some information will be collected about consumers and electronically stored. The long-standing goals for a fair marketplace and a level playing field suggest that policy-

makers should strive for more universal policies. To accomplish these goals, the following policy proposals are offered:

- Individual privacy consent: One of the major stipulations in the EU directive is the opportunity for consumers to provide their consent for the use of personal information. This appears to be unworkable in our computerized age. However, the details on how to move beyond the case-by-case method to a more generalized consent without giving up privacy represents a major policy question. Both U.S. and EU policymakers need to strive for an ethic-of-the-mean resolution to this difficult issue.
- Innovative self-regulation: The FTC is seeking the input of all major privacy groups in developing a workable privacy policy for the Internet. The opt-out and opt-in issue continues to be a policy concern. Web sites could be required to seek the consumer's agreement instead of assuming that silence means consent. At the very least, the FTC must ensure that any opt-out awareness campaign is heavily publicized (Green 1999).
- Limited new regulation: One area that apparently needs further protection is medical privacy. No federal regulation prohibits disclosure of such sensitive information as abortion, cancer treatment, or mental illness (Etzioni 1999). This area seems to strike at the core of individual privacy and has become a consumer (not just a medical) privacy concern.

Research Agenda

Academic researchers can inform the ethical and policy debate by systematic study of consumer privacy questions facing business and government. These include the following:

- Are the privacy statements currently adopted by industry effective in dealing with consumer knowledge and control questions? A content analysis of these statements by independent judges could assess the ethical principles companies espouse and whether the statements increase the likelihood of use by consumer.
- Which of the fair information principles proposed by the FTC are most central to consumers? A depth interview approach may lead to insights into which principles are the most central concerns and which ones consumers may be willing to trade off under certain circumstances.
- What trade-offs are online consumers willing to make for their personal information, and do they perceive the compensation to be fair? A large-scale survey could assess the perceived value of one-on-one marketing in the context of a cost–benefit analysis.
- How do organizations' activities in collecting and using information affect long-term relationships? Will customers forgive marketers' short-term activities (e.g., loss of control, loss of privacy) in return for future rewards? A longitudinal study of consumers participating in Internet loyalty programs might uncover whether marketers' increasing demands for personal information are detrimental to long-term customer satisfaction.
- Can international privacy standards be developed for this medium given vast cultural differences? A comparison study starting with U.S. and European consumers and then expanded to other countries might ascertain whether a set of universal core privacy rights do exist. Such a project should assist policymakers in determining the levels of future regulatory action.

Conclusion

Marketers and public policymakers both have a vested interest in solving the online privacy dilemma. Increasing consumers' confidence and trust in the privacy and security of their information will fuel growth of e-commerce on the Internet. Only through massive growth in purchasing from companies on the Internet, and not just surfing, will the revenue be produced to compensate for the high costs companies need to bear to be competitive and to build brand equity. The arguments in support of self-regulation suggest a short-term approach: Companies are looking for the means to market to customers in the present and may fail to see how their actions affect their long-term success in this medium. Public policymakers in the United States and Europe need to agree on common privacy standards, even if it is only at a minimal level.

This article proposes that ethical standards, not just policy statements, should be adopted in confronting online privacy concerns. Several positive recent developments, including increasing industry and government dialogue and the growing use and enforcement of privacy standards, signal an enlightened emphasis on privacy. The proactive business actions and policy initiatives outlined in the previous section should be helpful in answering this fundamental question: What is the right thing to do for the customer? Our aspirations for consumer privacy suggest an integration of business, ethical, and public policy standards to mitigate what some believe to be an inevitable erosion of privacy.

Appendix
Illustrations of Online Privacy Issues

True story: recently, I followed a lead from *MacUser* magazine to a web page for dealing with spam e-mailers. That page suggested that one of the first steps to take was to contact services that track people's e-mail addresses. With growing horror, I connected page after page on the list and located myself in their databases. Some services listed far more than just names and e-mail address. My home address and phone number were accessible from the same record. Two services even had a facility to show a map of my neighborhood and the location of my house in it. The widespread dispersal of information of this sort, without prior consent, is a serious invasion of privacy (Handler 1996).

With a 98% compliance rate, our registered users provide us with specific information about themselves, such as their age, income, gender and zip code. And because each and every one of our users have verifiable e-mail addresses, we know their data [are] accurate—far more accurate than any cookie-based counting. Plus, all of our user information is warehoused in a sophisticated database, so the information is stable, accessible and flexible. Depending on your needs, we customize user groups and adjust messages to specific segments, using third-party data or additional user-supplied information. So you can expand your targeting possibilities. What's more, because they're *New York Times on the Web* subscribers, our users are affluent, influential and highly engaged in our site (*New York Times* advertisement).

America Online Inc. (AOL) recently announced it would drop its plan to sell subscriber phone numbers to its business partners for telemarketing purposes. This action came after tremendous criticism from customers, privacy groups and consumer leaders. According to a statement to its subscribers, AOL never planned to make its customers' telephone numbers available for rental to telemarketers. "The only calls we intended for you to receive would have

been from AOL and a limited number of quality controlled AOL partners," according to the statement. "However, upon further reflection, we today decided to change our plans. We will not provide lists of our members' telephone numbers even to our partners. The only calls you might receive will be from us." Responding to the initial announcement of the plan, consumers swamped AOL's toll-free number to complain and New York Attorney General Dennis Vacco criticized the plan during an interview on CNBC. In addition, Wall Street responded with a four percent drop in AOL's stock price (*Direct Marketing* 1997, p. 6).

Intel Corp. last week decided to make changes in a security feature of its upcoming Pentium III chip after privacy groups started a boycott of the chip giant's products. Identification numbers that application vendors could use to identify a processor and its users would make the Internet and electronic commerce more secure, the Santa Clara-based company said. But privacy advocates argued that the identification numbers would erode Internet privacy and make it easier for companies to track users for marketing purposes (Savage 1999, p. 83).

Rima Berzin recently inherited a laptop computer from her husband and began an intense two-day honeymoon with the Internet. She went all the way; buying jeans at GAP, browsing for books at Barnesandnoble.com and registering for Martha Stewart's online journal. While Berzin was shopping, something very un-Martha happened: her spree left muddy digital footprints all over the Net. Berzin, a Manhattan mother of two, is like a lot of other Americans just stepping onto the Web. When a friend told her how much personal information she had swapped for the convenience of home shopping, she was angry at first, then confused. On Berzin's first visit to Gap, hidden files called "cookies" were deposited on her computer. Other software programs whirred into action to track and analyze her online behavior. Marketers didn't know her name at first, but the anonymity evaporated when Berzin made her first purchase (Baig, Stepanek, and Gross 1999, p. 84).

Comet Systems acknowledged that its popular software tracks customers as they travel across the Internet, recording which Web sites are being visited. The software, which changes a Web browser's computer cursor into cartoon characters and other images, is installed on more than 16 million computers. Customers' unique serial numbers are collected upon their visit to any of 60,000 Web sites, including dozens of sites aimed at young children. Critics contend this information is being collected without full disclosure to its customers and today's technology makes it possible for the company to correlate the serial numbers with consumers' identities (*Wall Street Journal* 1999, p. B6).

References

Auerbach, Jon G. (1999), "To Get IBM Ad, Sites Must Post Privacy Policies," *The Wall Street Journal*, (March 31), B1, B4.

Baig, Edward C., Marcia Stepanek, and Neil Gross (1999), "Privacy on the Net," *BusinessWeek*, (April 5), 84–90.

Bayne, Kim M. (1998), "Privacy Still Burning Web Issue," *Advertising Age*, (June 29), 37.

Beatty, Sally Goll (1996), "Consumer Privacy on Internet Goes Public," *The Wall Street Journal*, (February 12), B1.

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

Brandt, John R. (1998), "What Price Privacy?" *Industry Week*, 9 (May 4), 4.

Center for Democracy and Technology (1999), *Testimony of Deidre Mulligan, Senate Committee on Commerce, Science, and Transportation, Subcommittee on Communications*, (July 27). Washington, DC: Center for Democracy and Technology.

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

Children's Online Privacy Protection Rule: Issuance of Final Rule (1999), 64 *Fed. Reg.*

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

Direct Marketing (1997), "AOL Bows to Criticism over Selling Members' Phone Numbers," 60 (August), 6.

Direct Marketing Association (1998), *DMA Web Site Privacy Policy*, (May 16), [available at http://www.the-dma.org].

——— (1998), *DMA Web Site Privacy Policy*, (October 27).

DIRECT Newsline (1999), "FTC Commissioner Blasts Agency Over Privacy Stance," (July 29), [available at http://www.directmag.com/content/newsline/1999/1999072902.htm].

Donaldson, Thomas and Lee E. Preston (1995), "The Stakeholder Theory of the Corporation," *Academy of Management Review*, 20, 65–91.

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

Etzioni, Amitai (1999), "Protecting Privacy," *Financial Times*, (April 9), 18.

Federal Trade Commission (1998), *Privacy Online: A Report to Congress*, (June).

——— (1999), *Self-Regulation and Privacy Online: A Report to Congress*, (July 27). Washington, DC: Federal Trade Commission.

Foxman, Ellen R. and Paula Kilcoyne (1993), "Information Technology, Marketing Practice, and Consumer Privacy: Ethical Issues," *Journal of Public Policy & Marketing*, 12 (Spring), 106–19.

Fried, Charles (1968), "Privacy," *Yale Law Journal*, 77, 203–22.

Georgetown Internet Privacy Policy Study (1999), [available at msb.edu/faculty/culnanm/gippshome.html].

Gillmor, Donald M., Jerome A. Barron, Todd F. Simon, and Herbert A. Terry (1990), *Mass Communication Law*. St. Paul, MN: West Publishing.

Goodpaster, Kenneth E. (1991), "Business Ethics and Stakeholder Analysis," *Business Ethics Quarterly*, 1 (January), 53–73.

Goodwin, Cathy (1991), "Privacy: Recognition of a Consumer Right," *Journal of Public Policy & Marketing*, 10 (Spring), 149–66.

Green, Heather (1999), "Privacy Online: The FTC Must Act Now," *BusinessWeek*, (November 29), 48.

Guidera, Jerry (1999), "Regulators, Internet Firms Discuss Privacy in Profiling," *Dow Jones Newservice*, (November 8), [available at http://nrstg2p.djns.com].

Handler, Jon (1996), "Action Alert: Stop the Spread of Personal Information on the Net," *Risk Forum Digest*, (December 23), [available at http://catless.ncl.ac.uk/risks/18.71.html].

Harbert, Tam (1998), "None of Your Business," *Electronic Business*, (September), [available at http://www.eb-mag.com/eb-mag/issues/1998/9809priv.asp].

Harmon, Amy (1998a), "FTC to Call for Laws to Protect Children on Line," *New York Times*, (June 4), 1.

——— (1998b), "U.S. in Shift, Drops Its Effort to Manage Internet Addresses," *New York Times*, (June 6), 1.

Heckman, James (1998), "Legislation," *Marketing News*, (December 7), 1, 16.

——— (1999), "Debates Should Wind Down by Year's End," *Marketing News*, (August 30), 4.

James, Frank (1998), "FTC Urges Internet Privacy," *Chicago Tribune*, (June 5), 14.

Jones, Mary Gardiner (1991), "Privacy: A Significant Marketing Issue for the 1990s," *Journal of Public Policy & Marketing*, 10 (Spring), 133–48.

Kantor, Andrew (1998), "Privacy Replaces Censorship as #1 Concern of User," *Internet News*, (March 26), [available at http://www.internetnews.com/bus-news/article10,1087,3_19821,00.html].

Kuttner, Robert (1998), "The U.S. Could Use a Dose of Europe's Privacy Medicine," *BusinessWeek*, (November 16), 22.

Laczniak, Gene R. and Patrick E. Murphy (1993), *Ethical Marketing Decisions: The Higher Road*. Upper Saddle River, NJ: Prentice Hall.

Leibowitz, Wendy R. (1999), "E.U. Extends Its Privacy Protection," *The National Law Journal*, (January 18), B1.

Mahurin, Matt (1997), "Invasion of Privacy," *Time*, (August 25), 29–35.

Messmer, Ellen (1998), "U.S., Europe at Impasse Over Privacy," *Network World*, (December 7), 49.

Miller, Leslie (1998), "Net Can Give False Sense of Privacy," *USA Today*, (January 19), 4D.

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 (Fall), 206–15.

Murphy, Patrick E. (1998), *Eighty Exemplary Ethics Statements*. Notre Dame, IN: University of Notre Dame Press.

——— (1999), "Character and Virtue Ethics in International Marketing: An Agenda for Managers, Researchers and Educators," *Journal of Business Ethics*, 18 (January), 107–24.

Nelson, Emily (1998), "Why Wal-Mart Sings, 'Yes We Have Bananas!'" *The Wall Street Journal*, (October 6), B1.

New York Times (1999), "Microsoft Offers to Fix for Privacy Problems," (March 19), [available at http://nytimes.com].

Nissenbaum, Helen (1998), "Protecting Privacy in an Information Age," *Law and Philosophy*, 17, 559–96.

Oberndorf, Shannon (1998), "User Remain Wary," *Catalog Age*, (August 1), [available at http://www.catalogagemag.com/content/monthly/1998/1998080103.html].

Ohlson, Kathleen (1999), "Better Business Bureau Joins Online Privacy Fray," *CNN*, (March 19), [available at http://wwww.cnn.com/TECH/computing/9903/19/bbb.idg].

Parent, William (1983), "Recent Work in the Concept of Privacy," *American Philosophical Quarterly*, 20, 341–56.

Phelps, Joseph, Glen Nowak, and Elizabeth Ferrell (1999), "Marketers' Information Practices and Privacy Concerns: How Willing Are Consumers to Provide Personal Information for Shopping Benefits?" *Marketing Science Institute Working Paper No. 99-112*. Cambridge, MA: Marketing Science Institute.

Poynder, Richard (1996), "Infringement of Privacy or a Big Fuss About Nothing?" *Information World Review*, (November), 16.

Quick, Rebecca (1998), "On-Line Groups Are Offering Up Privacy Plans," *The Wall Street Journal*, (June 22), B1.

Rachels, James (1975), "Why Privacy Is Important," *Philosophy and Public Affairs*, 4 (Summer), 323–33.

Raysman, Richard and Peter Brown (1998), "Regulating Internet Content, Privacy; Taxes," *New York Law Journal*, (November), Computer Law section, 3.

Rotenberg, Marc (1998), "Self Regulation Won't Work," *USA Today*, (July 7), 12B.

Savage, Marsha (1999), "Intel Modifies Security Feature After Outcry," *Computer Reseller News*, (February 1), 83–84.

Schoeman, Ferdinand (1992), "Privacy," in *Encyclopedia of Ethics*, L. Becker and C. Becker, eds. New York: Garland Publishing, 1015–1018.

Singleton, Solveig (1998), "Privacy as Censorship: A Skeptical View of Proposals to Regulate Privacy in the Private Sector," *Cato Policy Analysis*, 295 (January 22), [available at http://www.cato.org/pubs/pas/pa-295.html].

Smith, Robert Ellis (1997), "Show-and-Tell Time in Washington," *Privacy Journal*, 23 (8), 1.

Stone, Dianna L. and Eugene F. Stone-Romero (1998), "A Multiple Stakeholder Model of Privacy in Organizations," in *Managerial Ethics*, Marshall Schminke, ed. Mahwah, NJ: Lawrence Erlbaum Associates, 35–59.

Swire, Peter B. and Robert E. Litan (1998), *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive*. Washington, DC: Brookings Institute.

Thomas, Paulette (1998), "'Clicking' Coupons On-Line Has a Cost: Privacy," *The Wall Street Journal*, (June 18), B1, B8.

Wall Street Journal (1999),"Popular Software for Computer Cursors Logs Web Visits, Raising Privacy Issues," (November 30), B6.

Warren, Samuel and Louis Brandeis (1984), "The Right to Privacy," in *Philosophical Dimensions of Privacy*, F. Schoeman, ed. Cambridge: Cambridge University Press, 75–103. Originally published in *Harvard Law Review*, 4 (193).

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

Wientzen, H. Robert and Robert Ellis Smith (1998), "Privacy Sound Off: Regulation vs. Self Regulation," *Internet Week*, (September 21).

Wigfield, Mark (1999a), "Study: Web Sites Fail to Protect Privacy," *Dow Jones Newswires*, (July 27), [available at http://nrstg2p.djns.com].

——— (1999b), "Internet Group Charges Few Sites Adhere to FTC Privacy Standards," *The Wall Street Journal Interactive Edition*, (July 28), [available at http://interactive.wsj.com/ushome.html].

Zeller, Wendy, Stephanie A. Forest, Kathleen Morris, and Louis Lee (1999), "The Big Guys Go Online," *BusinessWeek*, (September 6), 30–32.