Markets and Privacy

Kenneth C. Laudon

WHO OWNS AND CONTROLS PERSONAL INFORMATION IN NATIONAL DATA NETWORKS? WHY NOT LET INDIVIDUALS OWN THE INFORMATION ABOUT THEMSELVES AND DECIDE HOW THE INFORMATION IS USED? A REGULATED NATIONAL INFORMATION MARKET COULD ALLOW PERSONAL INFORMATION TO BE BOUGHT AND SOLD, CONFERRING ON THE SELLER THE RIGHT TO DETERMINE HOW MUCH INFORMATION IS DIVULGED.

PROTECTING individual information privacy is a widely accepted value in democratic societies—without which the concept of democracy based on individual choice makes little sense [1, 7]. Since the 1960s, many nations have developed privacy protection laws and regulations to guard against unfettered government and private use of personal information. While these protections are important first steps in protecting privacy, existing laws and their conceptual foundations have become outdated because of changes in technology. New concepts and methods of privacy protection are needed to address the contemporary and near-future technological environment.

By 2000, technological developments are likely to make existing legal frameworks for protecting privacy even more outdated than today. For instance, the Clinton Administration's proposed National Data Network and the prototype National Research and Education Network, which are important components of the High-Performance Computing Act of 1991, are destined to contain a great deal of personal information, including medical, genetic, insurance, retail purchase, and financial records. This personal information will reside on thousands of file servers—public and private—largely beyond the control of existing privacy laws. While these networks offer society important benefits, like remote diagnosis of disease, lower medical costs, and lower financial transaction costs, such networks will also make it less expensive and much easier to engage in privacy invasion on a scale never before possible. Who should own and control this personal information in future national networks? What accounting should be made to individuals for use of their private information on national networks? Who could be liable for misinformation and the injuries that may result? Current laws and conceptual frameworks do not answer these questions. National data networks also offer opportunities for developing new

concepts and methods of protecting privacy and security in a network-intensive 21st century.

Rethinking Privacy

The premise of this article is that to ensure the protection of individual privacy beyond 2000 we should consider market-based mechanisms based on individual ownership of personal information and a National Information Market (NIM) in which individuals can receive fair compensation for the use of information about themselves. This step is necessary because of the continued erosion of privacy brought about by technological change, institutional forces, and the increasingly outdated legal foundation of privacy protection. Together, these forces have eroded individuals' control over the flow of information about themselves. Today, the cost of invading individual privacy is far lower than the true social cost of invading that privacy. While market-based approaches cannot solve all our privacy problems, they can help strengthen individual control over personal information while strengthening (not replacing) the legal foundations of privacy protection. In the end, privacy should be easily achieved, and there should be as much use of private personal information for commercial purposes as is socially efficient. Today, personal privacy is expensive and in short supply, while the use of personal information is wasteful and inefficient.

Privacy is the moral claim of individuals to be left alone and to control the flow of information about themselves [5, 7, 12, 23, 24]. Privacy is also a social value reflected in founding documents, like the Constitution, and a political statement reflected in the laws. There is also a behavioral reality of privacy—the day-to-day routine practices for handling personal information. The behavioral reality of privacy stands apart from the moral claims, political statements, and laws—and must be considered separately.

When individuals claim that information about them is private, they generally mean they do not want the information shared with others or they personally would like to control the dissemination of this information, sharing it with some but not with others. These claims are sometimes strongly supported by cultural assumptions, making it odious for individuals or organizations to deny the claims.

Nevertheless, translating these general cultural value statements and individual claims to information control into law has been difficult because all societies involve competing claims by government and private organizations demanding access to information about individuals for the sake of national security, public health, law enforcement, commerce, or other valued social ends.

There are three primary sources of privacy protection in U.S. law:

- The common law
- The Constitution
- Federal and state statutes

The common law protects individuals against the intrusions of other private parties. Most jurisdictions recognize one or more common-law actions that allow private parties to seek redress for invasion of privacy. There are four types of privacy torts:

- Intrusion on solitude
- Public disclosure of private facts
- Publicity placing a person in a false light
- Appropriation of a person's name or likeness for commercial purposes [17, 21].

The common-law right to privacy has its origins in a famous article by Warren and Brandeis [23] that sought to extend growing common-law protections of person and property at the end of the 19th century. Warren and Brandeis defined a new "right to be let alone"—a right to privacy based not on property or contract but on a more general, inherent right of the individual that applied to "the personal appearance, sayings, acts, and to personal relations, domestic or otherwise" [22].

Privacy Laws Affecting the Federal Government
- Freedom of Information Act, 1968 as Amended (5 USC 552)
- Privacy Act of 1974 as Amended (5 USC 552a)
- Right to Financial Privacy Act of 1978
- Electronic Communications Privacy Act of 1986
- Computer Security Act of 1987
- Computer Matching and Privacy Protection Act of 1988
- Federal Managers Financial Integrity Act of 1982

Privacy Laws Affecting Private Institutions
- Fair Credit Reporting Act of 1970
- Family Educational Rights and Privacy Act of 1978
- Privacy Protection Act of 1980
- Cable Communications Policy Act of 1984
- Video Privacy Protection Act of 1988

Figure 1. Federal privacy laws in the U.S.

The second major source of privacy law is the federal Constitution, which protects against governmental intrusions into private life. Although "privacy" is not mentioned in the Constitution, jurists and legal scholars have found privacy protections in the First Amendment, which protects freedom of expression; the Fourth Amendment, which protects the privacy of one's personal papers and effects; the Fifth Amendment, which protects against compulsory self-incrimination; the Ninth Amendment, which leaves to the people rights not specifically mentioned in the Constitution; and the 14th Amendment, which protects

against deprivation of life, liberty, or property without due process of law.

Federal and state statutes form a third source of privacy protection. In general, statutes protect individuals against governmental intrusions and uses of information, although increasingly the use of personal information by private organizations is also the subject of legislation. In some instances, state statutes provide stronger protections than federal statutes against government and private-party intrusions [8].

In the U.S., there are 12 major pieces of federal legislation specifically regulating the collection, use, management, and dissemination of personal information by the federal government and private organizations (see Figure 1).

The seven major pieces of privacy legislation involving the federal government set forth the due process rules federal officials must follow when dealing with personal information. The most important contribution of these laws is that they prevent federal officials from rummaging through your bank records without a warrant, listening to your electronic communications without a warrant, or cutting off benefits simply because of a computer match. The federal legislation also sets forth standards of computer security involving personal financial information. The Privacy Act of 1974 applies to all federal records and sets forth the rules the government must follow when managing personal information. The Freedom of Information Act of 1968 is included here because it severely limits federal government claims that information it holds is "private" and cannot be shared with the public.

Despite the enormous legal armament that has evolved over nearly 100 years in the U.S., most citizens feel their privacy has declined. A survey sponsored by Equifax (of Atlanta), one of the world's largest collectors and purveyors of personal financial information, found in 1994 that 76% of U.S. citizens believe they have lost all control over personal information. The law review literature, as well as public surveys, argues that computer technology is a major threat to privacy. The legal literature itself is highly critical of the existing legal apparatus for protecting privacy, citing the piecemeal, record-system approach to protecting privacy and the absence of meaningful enforcement mechanisms [21]. Scholars from diverse backgrounds in history, sociology, business, and political science have all concluded that the existing set of privacy laws do not protect privacy well and that privacy law is far behind the developmental trajectory of information technology [7, 12, 16, 18]. Private companies' attempts to preserve the privacy of their customers and employees have also met with limited success [19]. Our view is that the conceptual foundations of privacy need rethinking in the U.S., especially for the statutory approach to protecting privacy based on a now outmoded doctrine called "fair information practices."

The existing legal approach to privacy in the U.S.—whether common law, Constitutional, or statutory—has many well-known limitations. Common-law torts have been particularly ineffective for providing privacy to individuals. Common-law claims for protection from being placed in a false light and from the revelation of embarrassing facts interfere with constitutional protections of free speech and expression. The common-law tort of appropriation has been quite effective in protecting celebrities from the appropriation of their likenesses, voices, and styles. Unfortunately, while celebrities have successfully claimed a property-based privacy interest in their personal information—including likenesses and voices—ordinary citizens have not been as successful. Here, we explore options for extending common law property rights to the personal information of ordinary citizens.

Despite the enormous legal armament that has evolved over nearly 100 years in the U.S., most citizens feel their privacy has declined.

Constitutional privacy protections are on weak ground simply because "privacy" per se is not mentioned in the Constitution and therefore must be inferred or derived from other enumerated rights and from judicial interpretation of what the Founding Fathers meant or intended in their original statements. The privacy required to think, believe, and worship is protected by the First Amendment's protections of expression and thought; the privacy of one's home and personal effects is protected by the Fourth Amendment. Somewhat less secure is decisional and behavioral privacy regarding highly personal matters, like sexual behavior, abortion, birth control, and medical treatment. In these areas, the state often claims superiority. There are no constitutional protections for any information you reveal in professional or business transactions—electronic or otherwise—even if such information refers to highly personal matters, like your genetic structure, medical and mental condition, or consumption patterns.

- Medical records
- Genetic records
- Insurance files
- Credit card retail transactions
- Personnel records
- Rental and real estate records
- Financial records
- Most state government records (e.g., motor vehicle, business records)
- Most local government records (e.g., tax receipts, real estate records)
- Criminal records
- Employment records
- Welfare files
- Phone bills
- Workman's Compensation
- Mortgage records

Figure 2. Major record systems not subject to federal privacy protection

Efforts by the Supreme Court to move away from a "home"- or place-based view of privacy toward a more general view based on a "reasonable expectation of privacy" as expressed in Katz vs. U.S. 389 U.S. 347 (1967) have met with mixed success.[1]

Privacy advocates in the U.S. have sought refuge in new laws to protect privacy in the computer age. However, many scholars argue that federal and state statutes protecting individuals against intrusions by government officials are confusing, piecemeal, and riddled with loopholes [12, 18]. Among the significant limitations of this legislation is that it generally limits the behavior only of federal or state officials, and then only mildly. In some states, local officials, private citizens, and organizations may rummage through your bank records or eavesdrop on your cellular phone conversations. And federal agencies have found legal loopholes permitting them to widely share personal information within the government without your personal informed consent and contrary to the original purpose for which the information was gathered. The only absolute federal privacy protection is the prohibition in the Privacy Act of 1974 against federal officials' gathering information on citizens' exercise of their First Amendment rights. In the belief that all record systems are different, U.S. legislation has been piecemeal, moving from one record system to another rather than seeking to define an overall right to privacy. Thus, legislation covers communications privacy, bank record privacy, video rental privacy, and more. Perhaps the most important limitation of this legislation is that enforcement is left entirely to individuals, who must recover damages in court. There are no enforcement agencies.

While states have been somewhat more aggressive in defining a general right to privacy (some in their constitutions) and more aggressive in protecting against government agent snooping[2] and employer snooping into the private lives of employees or job applicants, state legislation suffers from the same limitations as federal legislation. State legislation is piecemeal, takes a record-system approach, and is largely based on an outmoded doctrine. Perhaps the most dangerous aspect of privacy protection in the states is that it varies wildly from state to state. Privacy invaders may simply move to "open-record" states where there are few protections and export data to "closed-record" states [8].

Figure 1 shows that private institutions have for the most part been exempt from privacy legislation. The only exceptions—and they are important exceptions—are the credit data, education, cable, and retail video industries, in which citizens are guaranteed at least due-process access to their records and some protection against dissemination of records. For instance, retail video stores are prohibited from disclosing video rental records to anyone without a court order or the renter's personal consent.

With these exceptions, there are generally no federal laws offering protection for the vast storehouse of personal information gathered by the private and public sectors. Figure 2 lists some of the major record systems—private and public—accessible by private organizations and individuals.

An estimated 200 information superbureaus routinely compile these basic records, collate the information, and then resell it to government agencies, private businesses, and individuals. Among the records offered for a fee are bank balances, rental histories, retail purchases, social security earnings, criminal records, credit card charges, unlisted phone numbers, recent phone calls, and other information. Combined, the information helps develop "data images" of individuals sold to direct marketers, private individuals, investigators, and government organizations.[3] There are no laws regulating superbureaus per se, although some regulations have been issued by the Fair Trade Commission limiting the use of credit data; one state forced a credit agency to pay a small fine for disseminating false credit reports.

Laws are not always good indicators or predictors

[1]Since Katz vs. U.S. (1967), the Supreme Court has sought to ensure that the Fourth Amendment protects people—not just places, like homes, as originally conceived in Boyd vs. U.S. (1886) and in the property-based natural rights view of individual rights.

[2]You have little privacy from government snooping in an open field, in a telephone booth, or from technologically remote surveillance techniques, such as aerial surveillance, pen registers, which monitor incoming and outgoing phone calls, and remote electronic eavesdropping; if you are homeless, your effects may be searched without a warrant (Traver [21], Section 6, 1995).

[3]"Data image" was first by defined by the author [12] as a high-resolution digital image of an individual in a society with a powerful, widespread national information system.

of behavior. Speeding is against the law, as is software theft, yet millions of adult citizens knowingly violate these laws. Likewise with privacy legislation. While the privacy legislation of the last 20 years has made an important contribution toward defining privacy, many scholars conclude that the umbrella of privacy protection has failed to keep pace with the growth in computerized records; the laws are more loophole than law; and in practice, with some exceptions, there are few meaningful limitations in the U.S. on the flow of personal information. Surveys of public opinion have documented a growing public concern over the loss of privacy and a growing demand for stronger legislation.

The Market for Personal Information

There is already a lively market in the U.S. for personal information—dominated by large institutional data gatherers, with only a small role for individuals. Personal information is a valuable asset to private and governmental institutions, which use it to reduce their costs of operation.

The existing market for personal information is based on the notion that the gathering institution owns the personal information and that individuals have at best an interest in—not ownership of—information about themselves [22]. The 400 million credit records maintained by the three largest credit agencies, the 700 million annual drug prescription records, the 100 million computerized medical records, the 600 million personal records estimated to be owned by the 200 largest superbureaus, and the 5 billion records maintained (and often sold) by the federal government, as well as the billions of records maintained and stored by state and local governments, all have market value, demonstrated every day in the market.

It is common, especially in the legal literature, to blame information technology for this state of affairs [21]. But the inability of privacy legislation to curtail the flow of personal information or to give individuals a strong sense of control over the flow of their own information reflects a deeper failure to understand the information market or to bring economic perspectives to bear on the problem, and a policy failure lasting more than 20 years.

Virtually all American and European privacy legislation is based on a regulatory regime called Fair Information Practices (FIPs), first set out in a 1973 report by an advisory committee to the Secretary of the Department of Health, Education, and Welfare (now the Department of Health and Human Services) [22]. There are five fair information principles:

- There shall be no personal record systems whose existence is secret;
- Individuals have rights of access, inspection, review, and amendment to systems containing information about them;
- There must be a way for individuals to prevent the use of information about themselves gathered for one purpose for another purpose without their consent;
- Organizations and managers of systems are responsible for the damage done by systems and for their reliability and security; and
- Governments have the right to intervene in the information relationships among private parties.

A key advance of the FIPs doctrine is recognition that individuals have an interest in records containing personal information about themselves, even though those records are created by third parties. The report argued that this idea followed from "mutuality of record-generating relationships"—the fact that both parties in a transaction need to create and store records.

What is the nature of this "interest" and how can individuals and societies protect it? Is it a property interest? The Advisory Committee did not recommend a new enforcement agency, an ombudsman, or individual ownership of information, arguing instead that privacy laws should be enforced by individuals seeking redress in the courts for damages done through invasion of privacy and by building statutory incentives for large institutions to comply with the FIPs.

Many European nations, as well as other nations, including Canada, have followed the Committee's lead in defining privacy, although they often choose to enforce their privacy laws by creating privacy commissions or data protection agencies [3, 6]. Whether or not people in these nations have more personal privacy is open to question.

Unfortunately, the FIPs doctrine is seriously flawed. The FIPs doctrine was based on the technological reality of the 1960s, in which a small number of large-scale mainframe databases operated by the federal and state governments or by large financial institutions were the primary threats to privacy. It was conceivable that an individual could know all the databases in which his or her personal information appeared. But today, large-scale database systems with millions of records are operated by PC-based networks (individual PCs now rival 1960s mainframe capacities). Large-scale databases have become so ubiquitous that individuals have no possibility of knowing all the database systems in which their personal information appears. Hence, the "no secret systems" principle, which originated in an era when only large-scale institutions possessed databases, is technologically out of date.

A cascade of serious problems follows. For example, not knowing about so many systems makes it impossible to gain access to or to review or correct information in them. It is also impossible to give "informed consent" for third-party use of private information. And it has become impossible to know if managers of systems are holding personal information securely and reliably, and hence difficult to hold these people accountable or liable.

The FIPs regime does not take into account other forces in modern society militating against individuals' having social space to think, read, write, conspire, and innovate. For instance, the creators of the FIPs

regime in the late 1960s could not possibly understand the competitive pressures insurance, financial service, medical, and credit-granting businesses face today—and the resulting information intensity of these markets. The FIPs do not take into account the systemic nature of the problem of information—how much it costs, who pays, how much it is worth, and who owns it.

The FIPs perspective does not take into account harm to the entire society, focusing instead on individual injury. Imagine if we conceptualized and enforced environmental laws by relying on the courts to estimate the perceived damages done to individuals by polluters.

Perhaps the most significant weakness of the FIPs regime is its failure to specify a stronger form of the interest individuals have in their personal information. Under FIPs, individuals have only limited rights to control their personal information—rights usually limited to inspection, challenge, and review. There is little or no individual control over the collection and use of personal information. A much stronger form of interest would be a property interest, rather than a mere judicial or administrative interest. Under the legal regime of property, individuals have nearly unlimited control over disposition, use, storage, and sale.

Theories of Social Order

Due process, individual rights, and limitations on the power of the state and private organizations are key ingredients in Age-of-Enlightenment theories of social order. These perspectives have preserved the little privacy we have left. But other theories of social order have different views of information and privacy that is important to keep in mind when formulating new policies. In some of these other theories, progress depends on nearly unfettered exchange of information and the reduction of any barriers to the flow of information—including privacy protections [15]. But in other theories, the unfettered exchange of information can create social costs for which individuals must be compensated in a rational market system in which we can find new grounds for the support of privacy.

In a perfect world characterized by perfect information and perfect information shared by all, capital and labor are combined at their most socially efficient levels to produce the wealth of nations. In this most felicitous world of 19th-century economic thought, symmetry of information among market participants—capitalists, laborers, and consumers—is the lubricant of social and economic progress. Information also plays a critical role in the production process (as opposed to the market process), because it is embodied in labor as knowledge and in capital, which is just a physical instantiation of social knowledge and information. Information technology is like any other capital investment. Presumably cheaper than labor (and more productive), information technology replaces labor in the production function, making labor and overall production more efficient and the society wealthier.

What's wrong with this theory of the firm and markets is that it bears little resemblance to reality and lacks predictive power. As it turns out, information is not symmetrically distributed (hence markets don't function as predicted) and information technology is not freely substitutable for labor (hence productivity in information-based firms does not follow typical patterns). New social theories have been proposed to deal with the asymmetric distribution of information.

A number of new theories of social order are concerned with problems arising from asymmetries in the distribution of information and a more realistic view of its distribution. These theories play a large role in education and research in contemporary finance, microeconomics, accounting, and management/organizational behavior. Agency theory focuses on the dilemma of firm owners (principals) who must hire agents (managers) to run their firms [11]. The firm is a nexus of contracts among self-interested individuals in which the agents have most of the information and the principals find it costly or impossible to monitor the real behavior of their agents. Firms—and, by implication, societies—experience agency costs as they attempt to build more complex monitoring mechanisms. Social welfare declines as these investments produce no additional output. Information systems appear in agency theory as a low-cost monitoring tool that permits firms to grow without increasing agency costs. For agency theorists, privacy—or any restriction on information flow by agents—is a costly extravagance raising the costs of management.

Asymmetries in information also drive transaction cost models of social order. Why do firms or organizations exist? Rather than hire people, why don't firms rely on markets to supply their needs—markets in which contractors compete with one another? In transaction cost theory, the answer is that in markets, participants have unequal access to information on the quality of the market's goods and providers [25]. It's costly to participate in markets: contracts have to be written and monitored, goods evaluated, and funds recovered for failure. Firms grow in size as a way of reducing transaction costs. Information technology appears in this theory as a platform for electronic markets in which the costs of obtaining price, supply, and quantity information, and the costs of monitoring compliance with contracts could be reduced. As a result, firms could rely more on markets and less on their own growth. Likewise, firms could shrink in size (number of employees) as they expand business by contracting out vital services. For transaction theorists, privacy raises the costs of gathering information in the market and reduces overall social welfare.

Other contemporary theories—adverse selection and moral hazard—focus on market failures caused by asymmetries in information. Consider adverse selection (market situations in which the bad drive out the good) due to asymmetries in information. Because insurance companies can never be sure

about any individual's health (they lack enough detailed information) and because unhealthy people need insurance most, the insured pool becomes a collection of unhealthy people forcing insurance companies to raise rates. Healthy people drop out—refusing to pay high rates and recognizing they rarely get sick anyway—and soon it becomes uneconomical to insure the insured pool.

Or consider moral hazard (so called because individuals can alter their behavior, potentially creating a hazard, once they have paid a premium insuring against the consequences of their actions). Because insurance companies cannot monitor how many miles people really drive (information asymmetry), drivers know they can drive as many miles as they want once they have paid the insurance premium.

Direct	• Opening unsolicited mail • Responding to telephone, email, and other unsolicited communication
Indirect	• Maintaining excessively large mail and communication facilities to cope with unsolicited mail
Tangible	• Loss of productive and leisure time
Intangible	• Loss of control over information about oneself, feelings of helplessness, feelings of mistrust toward government and large private organizations

Figure 3. Information coping costs

Drivers assume that any additional accident costs they incur will be spread over a large group and that their perceived marginal cost of driving is lower than what it actually is. This situation forces insurance companies to raise rates on all drivers, encouraging wasteful, accident-increasing driving for all.

These theories leave the theoretical status of privacy as a desirable social goal somewhat ambiguous, presenting the dilemma of progress vs. privacy. According to these theories, the restriction of information flows caused by privacy laws leads to a decline in social welfare [15]. Face it: Privacy is indeed about creating and maintaining asymmetries in the distribution of information. At first glance it seems microeconomics is not friendly territory for privacy protection. But there is some salvation in the notion of externalities.

The British economist A. C. Pigou warned in 1932 that when manufacturers did not bear the full costs of making their goods (when they could instead "externalize" some costs by making others pay), the market price of the goods would be less than their real costs, leading to excess production and social inefficiency [14]. Pigou noted that society permitted manufacturers to externalize many costs of production: the health damages done to workers, environmental damages, and loss in aesthetic and other nonmonetary values. If emissions from a chemical factory destroyed the paint on nearby autos, chemicals were being produced at less than their true social cost and were selling at a lower price than they would otherwise. There could be external benefits as well, for instance, when people plant gardens on their front lawns and others enjoy them without paying anything. This problem came to be known among economists as the problem of positive and negative externalities.

For Pigou and many contemporary economists, the remedy to the problem of external costs is to "internalize" the cost, that is, impose a tax on the chemical manufacturer equal to the external costs. When they are charged for the damage they create, so the theory goes, polluters raise prices (forcing consumers to pay the full cost of their production), shift to nonpolluting technologies, or reduce production.

One problem with this approach is determining the size of the externality. Ideally, one would want to charge a tax on polluters equal to the external costs. But calculating the external cost is difficult enough when dealing with such tangible externalities as damages to individuals and structures; it is even more complicated when aesthetic values are involved. How much is a sunny sky worth? What losses in psychological self-worth and well-being occur because of a polluted physical environment?

Political problems also arise. Why should we tax a socially obnoxious behavior, permitting "rich" people and firms who can afford the tax to pollute? If the behavior is obnoxious, why not outlaw the behavior or closely regulate it using standards and enforcement through criminal and civil sanctions?

These questions have no easy answers. It may be much cheaper to permit some small level of obnoxious behavior for those willing to pay rather than ban it entirely and launch a huge bureaucratic effort. Enforcing the Clean Air Act of 1990 is predicted to cost billions of dollars through 2000, force uneconomical production technology into general use, and result in an excessively high cost/benefit ratio. In contrast, an easy-to-administer carbon tax of $100 a ton, coupled with the creation of a market in "pollution rights," may accomplish the same overall level of clean air at greatly reduced cost. Each polluter would be able to choose the best, most economical means of compliance with the law in order to reduce its taxes. This market approach is far superior to bureaucratic dictates that all polluters use the same "approved" technology. In Illinois, for instance, a market-based approach to pollution has resulted in a 75% reduction in the cost of compliance with acid rain regulations compared to a traditional regulatory approach [13].

Given that an efficient information- and knowledge-intensive economy requires the reduction of information asymmetries where possible within socially acceptable limits, can we apply the concept of externalities to achieve a high level of privacy protec-

tion at a minimal enforcement cost? We can if we extend some of the thinking from information economics and externalities outlined earlier.

Market Contexts

Markets don't just happen. They arise in a context of social, moral, and political understandings. Sometimes markets need to be created, encouraged, monitored, and regulated by governments. A legitimate and useful role of government is to create the conditions for markets to function.

In the case of information privacy, markets either have failed to function because of a legal framework that denies individuals a property right to their personal information or have been eliminated by collusion among large market participants benefitting from the externalities created in the current situation. Privacy invasion is partly the result of market failure. Privacy invasion occurs whenever personal information of any kind is obtained and used without the consent of the individual. We should structure personal information markets in such a way that individual consent is required before any personal information is used, just as we structure financial markets so individual consent is required for transference and use of personal property and financial assets. Currently, personal information markets are not structured to ensure individual consent.

If markets were allowed to function more effectively, there would be less privacy invasion. Such failure in personal information markets produces several results:

- The cost of using personal information to invade the privacy of individuals is far lower than the true social cost because part of the cost of invading privacy is borne by the individual whose privacy is invaded. Other costs (regulatory agencies, congressional hearings, federally funded study groups, and a small industry of privacy experts) are created, and the government is forced to pay the costs based on general revenue taxes. In addition, current government communication and postal regulations subsidize the invasion of privacy by maintaining artificially low prices in key communication markets required by privacy invaders.
- Large public and private institutions make far greater use of privacy-invading techniques than they would otherwise.
- Public welfare declines because of the inefficient allocation of tangible resources and a decline in individual self-confidence and public morale. In the end, we are swamped and overwhelmed by activities we do not approve of that are costly and obnoxious. We tend to blame the technology for what is an institutional situation we have created.

In what sense does privacy invasion impose a cost on individuals whose privacy is invaded? There are many kinds of costs: direct, indirect, tangible, and intangible. Many invasions of privacy in a mass society occur through the secondary and tertiary uses of information gathered in the ordinary conduct of business and government. A "secondary use" of information is any use beyond the purpose for which the information was originally gathered. For instance, when a direct marketing organization asks for your credit card number, that is a primary use of information. The information supports a valid transaction. However, the subsequent selling of that information to database marketing organizations interested in knowing your credit card number and what you purchased is a secondary use.

Under current law, individuals largely lose control of information gathered about them in the course of legitimate transactions. While few people object to the primary use of information to support a transaction, the question is, what happens to the information gathered in the transaction? The answer: Once gathered, the information is beyond individual control. Sometimes this loss of control is sanctified by weak "informed consent" clauses often tied to a particular benefit (e.g., to receive public benefits, citizens agree the information they give may be used for other purposes).

Once individuals lose control of information about themselves and ownership of the information, the information is then used freely by other institutions to market and communicate with and about individuals. Individuals must cope with this onslaught of communication and incur "coping costs." Figure 3 highlights some of the coping costs.

The solution to this problem is not stronger privacy laws—often called for by well-meaning privacy advocates—or new regulations or creation of a data protection agency, however helpful these things may be. We should instead strengthen and make more fair the existing information markets.

A National Information Market

One possibility is creation of an National Information Market, or NIM, in which information about individuals is bought and sold at a market clearing price freely arrived at, in which supply equals demand. Institutions gathering information about individuals would be allowed to sell baskets of information to other institutions willing to pay for it. Each basket would contain selected standard information on, say, 1,000 persons (e.g., name and address), basic demographics where available, and specialized information (e.g., health, financial, and occupational). Different markets might specialize in different kinds of information (e.g., financial assets, credit data, health, government, and general marketing). Buying information baskets would confer the right to use the information for commercial purposes other than that for which it was originally collected. Information-using organizations would offer to buy the baskets of information at a price based on the anticipated future revenues each basket represented.

Figure 4 outlines how an NIM might work. The process is similar to the flows of financial assets in

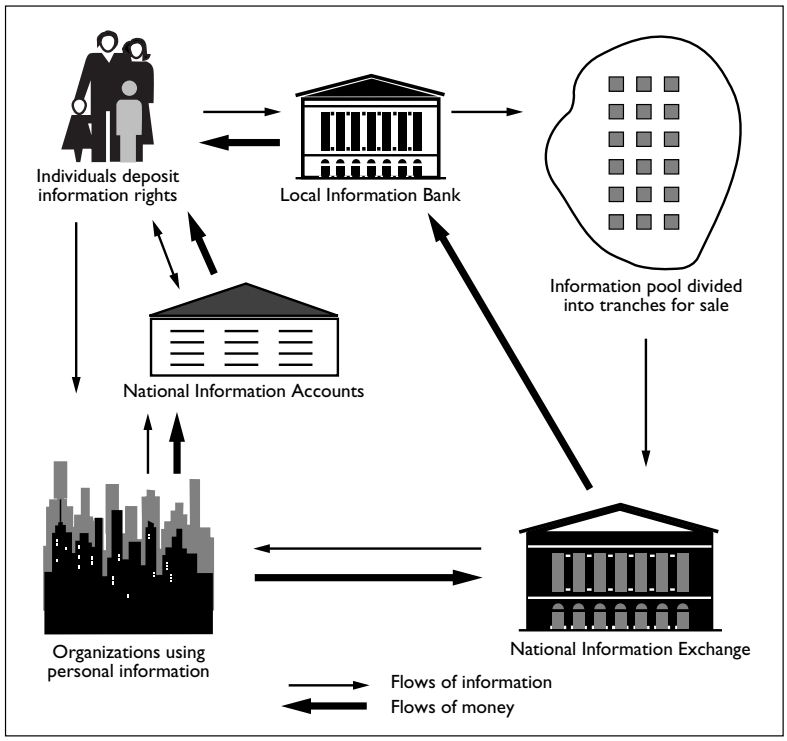

Figure 4. How a National Information Market would work

depository institutions connecting individual consumers, retailers, creditors, and banks; it also borrows some concepts, like bundling of financial instruments into baskets, from the collateralized mortgage market, in which thousands of mortgages are pooled and used to develop financial instruments called collateralized mortgage obligations (referred to as tranches).

Individuals would establish information accounts and deposit their information assets and information rights in a local information bank, which could be any local financial institution interested in moving into the information business. Depositors would grant potential users of personal information the right to use it after buying the rights in the market. The local information bank would pool local depositor assets into an information pool and carve up the pool into marketable information baskets, or tranches. These baskets would contain key personal information (e.g., credit, medical, educational, and income) on groups of individuals. The local bank would sell the baskets on a "National Information Exchange." Buying a basket confers on the buyer the right to use the information for commercial purposes—for a defined period. Like a stock exchange, the Exchange would bring together buyers and sellers of information in a forum (physical or electronic) for the purpose of transacting at a market clearing price. When the transaction was complete, funds would flow back to the local depository institutions, ultimately crediting depositors' accounts, minus, of course, information-handling charges for both the local banks and the Exchange, as well as any brokers involved.

Organizational users of personal information (e.g., credit-granting agencies, medical institutions, insurance agencies, government agencies, and retailers) would buy baskets of information on the Exchange, either directly or through brokers acting as intermediaries. Private placements and nonmarket transactions would also be possible. Individuals and organizations might transact information off the market, with individuals granting organizations rights to use information about them in return for a fee. For instance, organizations that collect credit histories could—with the consent of individuals, probably involving payment—sell baskets of this information on the Exchange.

Payments for private placement sales of personal information could be cleared through a National Information Accounts Clearinghouse (NIAC), established by Congress for the purpose of permitting individuals to collect fees for the use of their private information (a system similar to that established in the music industry, whereby individual artists can collect fees based on use of their music). The NIAC would also act as an audit mechanism, tracking the use of all secondary, commercial use of personal information and maintaining a record for individuals about who purchased information about them, where the purchase took place, and where the information was used.

The NIM would be the only legal avenue for the transfer of information about individuals being used for secondary purposes, that is, for purposes and institutions other than those for which the information was originally gathered. Thus, MasterCard could use information on your credit history for the purpose of authorization of future MasterCard purchases (a primary use), but it could not sell your history of credit card purchases to other institutions, like TRW Credit Data, without your permission—and most likely some payment. The NIM would be self-supporting with a transfer tax charged and the revenue used to support the market's infrastructure, enforcement of rules, and monitoring activities.

A key aspect of an NIM would be development of National Information Accounts (NIAs) for suppliers (individuals and institutions) and buyers (information brokers, institutions, and individuals). Every participating citizen would be assigned an NIA with a unique identifier number and barcode symbol. The NIA would help individuals keep track of who is using their information by informing the account whenever the individual's name is sold as part of a basket of information. Every secondary use of personal information must be authorized by the individual at some point and an NIA informed (and credited if

Social and Legal Issues
- People should not be allowed to sell a basic right.
- Property is regressive; only the rich and powerful would benefit (equity).
- A revolution in American property law would be required.
- Government privacy regulation is required, as in auto safety, because markets do not respond to social and individual needs for privacy.

Economic Issues
- An NIM would raise business transaction costs and inhibit trade.
- An NIM would experience high administrative costs.
- Individual privacy leads to market fraud; there is too much privacy already.

Figure 5. Issues in and objections to market-based privacy

required). The greatest threat to individual privacy—use of personal information by organizations without the knowledge or consent of the individual—would be minimized through NIAs, because to use personal information without consent would be a crime, just as the appropriation of another's tangible property is a crime.

The NIA has several purposes:

- Personal accounts—like bank accounts—ensure that some percentage of the purchase price of information sold on the market is returned to individuals as revenue to compensate them for their cost of dealing with privacy invasion.
- No commercial unsolicited mail could flow through the system without a unique NIA identifier barcode, permitting automatic crediting of NIA accounts.
- A complete computer-based audit trail for personal information would be available for commerce—a long-sought objective of privacy reformers [4].

Citizens calling a toll-free number could find their account balances and perhaps trace the flow of information about themselves (e.g., how did Brown Harriman Investment Banking, which just contacted me through an unsolicited phone call, get my bank balance information from the Bank of New York?). An NIAC could empower individuals to trace the flow of information about themselves.

From a societal point of view, it is only through national accounts that external costs of an information-driven economy are properly internalized. From an individual point of view, an NIA restores some measure of real control—and the subjective perception of control and order—to the flow of information.

Because most people would not have the time or interest to participate directly in information markets, a role would emerge for information fiduciaries, or agents acting on their behalf who assume certain legal responsibilities. Like banks, they would accept deposits of information from depositors and seek to maximize the return on sales of that information in national markets or elsewhere in return for a fee, possibly a percentage of the total returns. Such information fiduciaries could be recruited from the ranks of information superagencies and local credit and information bureaus.

Would governments have to pay for information they need to administer programs? Generally, no. The concept of an NIM applies only to secondary and tertiary uses of information. The information collected by the government in the course of conducting business with citizens could be used to administer programs without cost. However, if a government sells the information to third parties or seeks information from sources outside government programs, it would be treated as simply another market participant, pay for information received, and be compensated for information sold. In either event, individual citizens would receive a fair percentage of these transactions. For law enforcement and national security purposes, these restrictions could be waived.

Objections

I have presented the same ideas that are in this article to market research and advertising executives, privacy policy advocates, privacy scholars, and social science scholars from the fields of economics, sociology, and political science. While there is much support for these ideas, surprisingly, market research, advertising executives, and others have raised objections to the notions that individuals should own their personal information and that NIMs based on trading personal information would advance the cause of privacy (see Figure 5).

Lets look at each of these issues:

• **Selling a basic right.** In the existing unfair information markets, individuals give up or lose control of their personal information as a matter of course every day, sometimes under threat of not receiving a benefit. Surely these same individuals could charge for this information, which they currently give away or have stripped away without violation of any Constitutional privilege. It is by no means clear that "privacy" is an unqualified Constitutional right. The Constitution only explicitly protects the privacy of one's papers and personal effects; this protection is generally interpreted by the Supreme Court as the privacy of one's home. The Constitution makes no mention of personal information in one's data image, although many legal scholars believe such privacy can be inferred from the Constitution and its history. In any event, people can and do choose to give up their Constitutional rights under selected circumstances all the time. For instance, people may choose to give up some freedom of speech to achieve greater social harmony.

• **An inequitable property regime.** The property regime is regressive and inequitable. In an NIM, some people will sell their privacy, the poor more

than the rich. Rich people may receive much more for the right to invade their privacy, but because they are rich, most will not care to sell their privacy and most will charge excessively high prices, ensuring a nonsale, or simply withdraw from the market to preserve their privacy. Information from middle-income groups will be in high demand, and these individuals will seek out the best prices.

The ability of large information-using institutions to dominate the proposed new NIM is also dubious. As it now stands, individuals have no institutions to represent their interests in the existing information market. Professionally operated local information depository institutions would be a powerful economic and legal representative for individuals. It is likely that existing consumer banking corporations would be capable of and interested in becoming local information depositories. In this manner, individuals could be as well represented in the information market as they are in financial markets by such giants as Merrill Lynch and Citibank. Currently, individuals have no such protection at all in the existing information markets.

Finally, to those who argue that property is an elitist institution incapable of protecting the rights of people who own no property, I agree that property is not equally distributed. Nevertheless, everyone possesses information about themselves that would be valuable under some circumstances to others for commercial purposes. Everyone possesses his or her own reputation and data image. In this sense, basing privacy on the value of one's name is egalitarian. Even the poor possess their identity. In the current regime of privacy protection, not even the wealthy can protect their personal information.

The point is that overall privacy invasion will decline and there will be a net increase in privacy because the cost of invading privacy will go up. People will have a greater understanding of the flow of information in the society (the NIM would make it visible), the flow will be more institutionalized and less secret, and they will experience more control over the fate of their own information. The concept of a market includes the potential to withdraw to totally protect one's privacy.

• **A revolution in property law.** No revolution in American property law is required to support an NIM or the ownership of one's personal information. On the contrary, the connection between privacy and property has strong historical precedents [2]. Property law is quite flexible in recognizing value in a variety of tangible and intangible assets, including one's personal image. Personal information—from genetic codes to credit history to medical information—has many of the key characteristics of property as defined in American law and in the Hohfeldian theory of property [1, 10]. For instance, since the 19th century, the courts have recognized the claims of celebrities to a property interest in their photographic images and the right of celebrities to seek compensation whenever such an image is used for a commercial purpose. What is needed is the extension of a property interest to the digital data images of ordinary individuals. Today's "data images" of individuals have as much resolution as many photographic images. How can a property interest be granted to protect photographic images but not extend to data images?

• **More regulation.** Government regulation is required to achieve satisfactory levels of privacy. One theory of government is that government is required by the failure of markets (e.g., to regulate natural monopolies or to correct asymmetries in information by forcing disclosure of information, as in financial markets). Yet another theory holds that markets fail when governments regulate [20]. Many privacy advocates argue for more regulation, more laws, more enforcement agencies, and more standards being imposed on everyone [4, 6, 12]. With some notable exceptions, described earlier, the regulatory approach to privacy has not worked well [19].

Would markets work any better to protect privacy? Social policy analysts may well question whether markets can solve the problem of privacy invasion any better than markets solved the problem of automobile safety. For instance, auto makers did not respond well to market demands for such automobile safety features as air bags. Rather, the solution was regulated by government. Also, in a "free market," wouldn't large institutions dominate the terms of transactions?

Our approach is empirical, not dogmatic. While automobile safety is a visible threat to people, and no doubt important, protecting one's property and ensuring a fair return on one's assets is a proven motivator in free economies. Told that personal information is an asset worth real money in an NIM, individuals might easily be convinced to demand a proper institutional foundation for ensuring a fair return on their assets. And there is some reason to believe individuals pursuing their own self-interest can protect their assets over the long term better than governments can. Moreover, auto safety features—as manufacturers pointed out—generally meant money out of pocket for consumers. An NIM—properly structured—should mean money *into* the pocket for millions of people, or at least a sense of justice. There is indeed a proper role for government, namely ensuring that the NIM operates fairly.

• **Increased transaction costs**. Those who argue that transaction costs would rise and inhibit trade are ignorant of the enormous cost of the existing set of arrangements, under which individuals have lost virtually all control over their personal information and are therefore included in marketing databases in which they do not want to be and from which they do not want to receive information. Nevertheless, owners of marketing databases send (or call) millions of individuals substantial information, most of which is promptly tossed out or ignored, causing a waste of billions of dollars. For instance, according to the Direct Marketing Association in New York, about 14.5 billion catalogs were distributed to homes in 1994.

Researchers have found that 75% of these catalogs are tossed out within five seconds of receipt. Millions of telephone solicitations are also ignored. The precise cost of the wasteful system of nonconsensual databases is unknown, but it may approach $50 billion annually, adding significantly to market transaction costs. Much of this waste could be avoided in a market-based system of privacy because only consensual databases would exist. Consensual databases could be based on individual ownership of personal information, and they could be operated for pennies per transaction. For this reason, many marketing and advertising executives support consensual databases.

• **Costly NIM operations.** The costs of operating an NIM should be much less than the costs of operating credit card or debit card systems. Owners of personal information would voluntarily submit, correct, and update information; users of personal information would make inquiries to national repositories to identify individuals and costs, then submit payments to individuals for using their information via the same route. The record complexity would be quite low compared to that of, say, credit or debit record systems. The costs of operating a system of NIMs may well be less than the waste generated by the existing system.

An NIM will be self-supporting, based on fees charged to market participants. As it turns out, information technologies are marvelously efficient and powerful at keeping accounts and useful in creating electronic markets involving huge transaction volumes for pennies per transaction.

• **Too much privacy already.** Some economists analyzing privacy have reached opposite conclusions from ours [9, 20]. Some legal scholars, writing from an economic perspective, argue that too much privacy has been accorded individuals and that the property right to personal information should be assigned "away from the individual where secrecy would reduce the social product by misleading the people with whom he deals" [15]. In this view, privacy is an intermediate—not ultimate—value; privacy is not a necessary utilitarian condition for contemporary society and indeed may interfere with transactions insofar as the claim to privacy is tantamount to claiming the right to deceive others in the market [15]. For Posner, more privacy—not less—should be accorded businesses that, in this view, require secrecy to perform entrepreneurial functions. These views, while interesting, fail to account for the negative information externalities inherent in the new information age. These views also fail to recognize the noneconomic functions of privacy (e.g., political freedom and liberty) that contribute to social welfare.

Some economists have attacked the remedy for external costs we and other economists propose for controlling pollution—namely to tax the polluters in proportion to the damage they cause rather than regulate them. R. H. Coase [5] argues that if a manufacturer damages a neighbor's property, creating an external cost not accounted for by the manufacturer in its pricing schedule, it may make more economic sense to move the neighbor rather than tax the manufacturer. To tax the manufacturer in an amount equal to the damage to neighboring property could result in reducing the overall welfare when compared to the simple expedient of removing the damaged neighbor or striking a bargain with local home owners (e.g., fixing their homes or cars injured by pollution). Moreover, Coase argues that taxing the polluter does not alter the overall distribution of resources but instead reduces the efficiency of society as a whole. This argument makes little sense when applied to either privacy invasion or to environmental pollution on a massive scale. How do you move away from privacy invasion and avoid experiencing the costs? The argument makes even less sense if the risks are life-threatening, catastrophic, or injurious to liberty in some general sense.

Under a regime in which individuals own their personal information, transaction costs may rise but only as far as necessary to pay for the cost of invading privacy. An NIM raises the cost of using personal information for reasons other than those for which it was gathered. This added cost discourages the obnoxious use of information that could undermine the foundations of a free society if left unchecked. There should be no free lunch when it comes to invading privacy. An NIM will result in less use of unsolicited communications—a key source of privacy concerns. Many other obnoxious uses of personal information will also decline. But an NIM will also lead to cost savings as firms use the latest technology to target their communications to smaller groups, devise new ways to market products and get market information, and compete with one another on their privacy-related corporate practices. Overall social welfare will increase.

Although the principal privacy enforcement mechanism would be market forces rather than a regulatory agency, even markets need oversight to ensure efficiency and standards. The functions of a Federal Information Commission (FIC) would be similar to, but go beyond, the traditional Data Protection Agency structured along the European and Canadian models; it would have more in common with the U.S. Securities and Exchange Commission. FIC functions would include:

- Creating and monitoring the NIM
- Conducting system and participant audits
- Developing data quality standards and expectations
- Developing privacy metrics
- Gathering and publishing statistical reports
- Conducting educational programs in schools
- Advising Congress and the executive branch on information matters

IS professionals in a democracy are obligated to help individuals and society achieve the level of pri-

vacy required for the preservation of democracy. IS professionals are also obliged to their employers to achieve efficiencies in administration, possibly requiring extensive use of personal information. Such obligations do not necessarily conflict, and there are several opportunities for professionals to positively influence their resolution. We can do the following:

- Ensure that our professional associations (the ACM and the Data Processing Managers Association (DPMA) develop public policies on privacy and clarify the obligations of professionals;
- Encourage organizations that claim to represent and speak for IS professionals in Washington (like Computer Professionals for Social Responsibility) to consider new ways to achieve privacy, aside from the traditional methods of more regulation and more bureaucracy, in the form of a Data Protection Commission and the like;
- Encourage our employers to devise policies that do not demean the individual's control over personal private information and that may compensate individuals for use of such information;
- Encourage our employers to compete on privacy much as Citibank and L.L. Bean do in their advertising, which promises individuals a measure of control over the information they give to these organizations. In the long run, establishing relationships of trust with customers about their personal information will have strategic business value and restore some measure of control to individuals.

Conclusion

The deals cut in the first regulatory generation of privacy legislation—segregating files by function; prohibiting secondary uses of information without "informed consent"; establishing individual rights vis-à-vis record systems, management accountability, and due process rules—were steps along the road to civilized management of information in a digital age. Nevertheless, technology, economics, and organizational behavior have vitiated the strength of the regulatory approach. There is too much money, political gain, and bureaucratic advantage to allow the regulatory approach to work by itself.

If privacy is to be taken seriously as a public value, the solution is to rely on more powerful and less wasteful mechanisms, like markets, to reduce privacy invasion. As things stand, there is much more unsolicited invasion of privacy than is tolerable, socially efficient, or politically wise. The current situation costs corporations billions of dollars in waste as they pour money into privacy-invading marketing and authorization techniques. Millions of dollars' worth of junk mail is tossed without being opened; millions of telephone solicitations are cut off in mid-sentence; market researchers are refused vital information by disgusted and fearful consumers; millions of faulty credit authorizations are issued based on poor data quality; and public cynicism about the information trade is growing. All this suggests a polluted, even toxic, information environment. A powerful way to clean our information environment is through a mixture of market and regulatory mechanisms. ◻

References

1. American Law Institute. Restatement of Property. 1936.
2. Barrad, C., and Valerio, M. Genetic information and property theory. *Northwestern Univ. Law Rev. 87* (Spring 1992), 52–70.
3. Bennett, C.J. *Regulating Privacy: Data Protection and Public Policy in Europe and the U.S.* Cornell University Press, Ithaca, New York, 1992.
4. Berman, J., and Goldman, J. *The Federal Right of Information Privacy: The Need for Reform.* The Benton Foundation, Washington D.C., 1989.
5. Coase, R.H. The problem of social cost. *J. Law Econ. 3* (Oct. 1960), 1–44.
6. Flaherty, D.H. *Protecting Privacy in Surveillance Societies.* University of North Carolina Press, Chapel Hill, 1989.
7. Gavison, R. Privacy and the limits of law. *Yale Law J. 89*, 3 (Jan. 1980), 421–471.
8. Gormley, K., and Hartman, R.G. Privacy and the states. *Temple Law Rev. 65* (1992), 23–40.
9. Hirshleifer, J. Privacy: Its origins, function and future. *J. Leg. Stud. 9* (1980), 649–664
10. Hohfeld, W.N. Fundamental legal conceptions as applied in judicial reasoning. *Yale Law J. 26* (1917), 1–26.
11. Jensen, R., and Meckling, W. Theory of the firm: Managerial behavior, agency costs, and ownership structure. *J. Financ. Econ. 11* (1976), 305–360.
12. Laudon, K.C. *Dossier Society.* Columbia University Press, New York, 1986.
13. Passell, P. Illinois is looking to market forces to help reduce its smog. *The New York Times* (March 30, 1995).
14. Pigou, A.C. *The Economics of Welfare.* 4th ed. Blackwell Books, London, 1932.
15. Posner, R. Privacy, secrecy, and reputation. *Buffalo Law Rev. 28* (Dec. 1979), 1–55.
16. Privacy Protection Study Commission. Personal privacy in an information society. *Report of the Privacy Protection Study.* Government Printing Office, Washington, D.C., 1977.
17. Prosser, W. Privacy. *California Law Rev. 48* (1960), 383–423.
18. Rule, J.B., MacAdam, D., Stearns, L., and Uglow, D. *The Politics of Privacy.* Elsevier Press, New York, 1980.
19. Smith, J.H. *Managing Privacy: Information Technology and Corporate America.* University of North Carolina Press, Chapel Hill, N.C., 1994.
20. Stigler, G.J. An introduction to privacy in economics and politics. *J. Leg. Stud. 9* (1980), 623–644.
21. Traver, C. *Privacy, Law, and the Human Genome Project: A Review of the Literature 1968–1993.* Center for Social and Legal Research, Hackensack, N.J., 1995.
22. U.S. Department of Health, Education and Welfare. *Records, Computers and the Rights of Citizens.* MIT Press, Cambridge, Mass., 1973.
23. Warren, S.D., and Brandeis, L.D. The right to privacy. *Harvard Law Rev., 193* (1890), 193–220. (This phrase also appeared in a Brandeis dissent in Olmstead vs. U.S. 277 U.S. 438, 473, 1928.)
24. Westin, A.F. *Privacy and Freedom.* Atheneum, New York, 1967.
25. Williamson, O.E. *The Economic Institutions of Capitalism.* The Free Press, New York, 1985.

KENNETH C. LAUDON is a professor of information systems at New York University's Stern School of Business. He can be reached at klaudon@stern.nyu.edu