MARKETS AND PRIVACY

Professor Kenneth C. Laudon

Working Paper Series
STERN IS-93-21

Markets and Privacy

Prof. Kenneth C. Laudon
Stern School of Business
Management Education Center
44 West 4th Street, Suite 9-66
New York, New York 10012
(914 271-6321)
Revised Draft Version July 1993

Filename: PRIV3

Abstract

Since the 1960s privacy advocates have relied on regulatory and legislative approaches to privacy protection in the United States, Canada and Europe. While important progress has been made in certain areas, there are large gaps and significant loopholes in existing legislation. I argue that a market-based approach to privacy protection would be far more effective and efficient in protecting individual information than current approaches.

Accepted for publication at:

International Conference on Information Systems (ICIS)
Orlando, Florida
December 1993

DRAFT
NOT FOR QUOTATION OR CITATION

Markets and Privacy

Filename: PRIV3

Introduction

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in the 1960s are important first steps in protecting privacy, existing laws and their conceptual foundation are outdated due to changes in technology.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

By the year 2000 technological developments are likely to make existing legal frameworks for protecting privacy even more outdated than is true today. For instance, the proposed National Data Network of the Clinton Administration, and the prototype National Research and Education Network (NREN) which is an important component of the High-Performance Computing Act (1991), are destined to contain a great deal of personal information including medical, genetic, insurance, retail purchase, and financial records. While these networks offer society important benefits like remote diagnosis of disease, lower medical costs, and lower financial transaction costs, such networks will make it less expensive and much easier to engage in privacy invasion on a scale never before possible. Who will or should own and control this personal information on future national networks? What accounting should be made to individuals for use of their private information stored and available on national networks? Who shall be liable for misinformation and the injuries which may result? Current laws and conceptual frameworks cannot 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.

Re-thinking Privacy

The premise of this paper is that to ensure the protection of privacy beyond 2000 we should consider market-based mechanisms based upon individual ownership of personal information and National Information Markets (NIM) where individuals can receive fair compensation for 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 privacy is far lower than the true social cost. I believe it is possible to strengthen individual control over personal information and to strengthen (not replace) the existing legal foundations of privacy by permitting markets to work. In the end, there should be as much privacy as people are willing to pay for, and as much use of private personal information for commercial purposes as is socially efficient.

Part 1 Privacy: The Current Situation

Privacy is the moral claim of individuals to be left alone and to control the flow of information about themselves. (1) (Warren and Brandeis 1890; Westin 1967; Laudon 1986; Flaherty 1989; Bennett 1992; Gavison 1980). Privacy is also a social value stated in important documents, and a political statement reflected in 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 (or their own behavior)

is private, they generally mean that they do not want this information shared with others, and/or that they would like to control the dissemination of this information, sharing with some (relatives) but not others. These claims of individuals are sometimes strongly supported by cultural assumptions which make it odious for individuals or organizations to deny these claims (2) (Warren and Brandeis 1890; Westin 1967; Laudon 1986; Flaherty 1989; Bennett 1992; Gavison 1980).

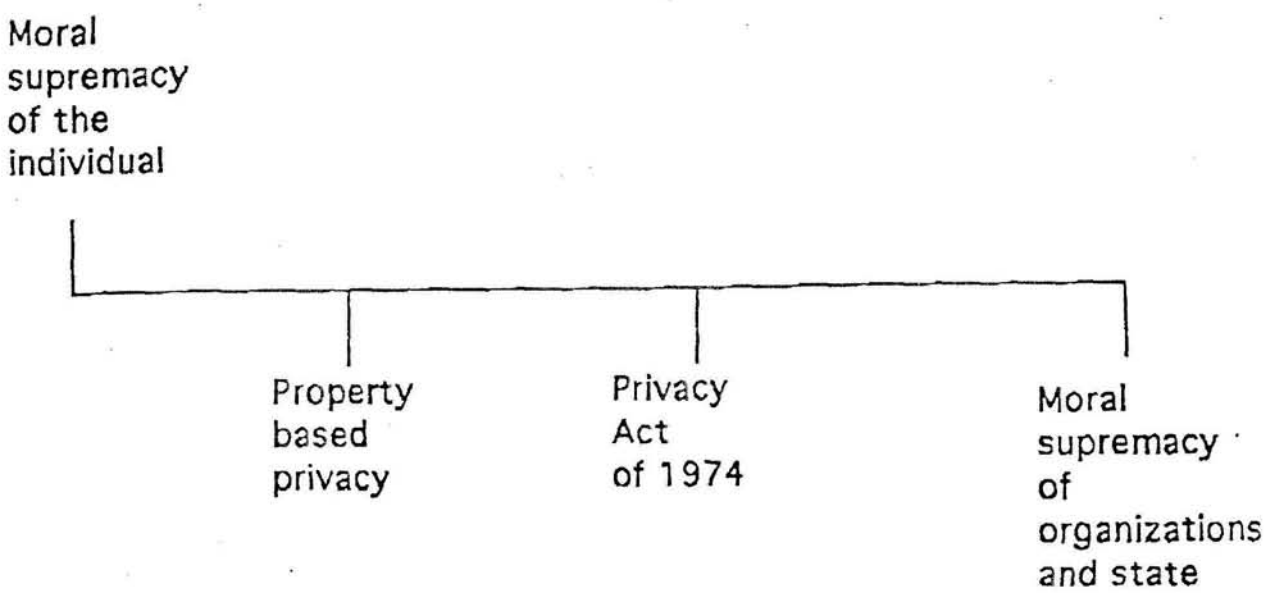
1.1 Privacy as a Moral Continuum

Translating these general cultural value statements and individual claims to information control into political laws has always been difficult because in all societies there are competing claims by government and private organizations demanding access to information about individuals in order to promote national security, public health, law enforcement, commerce, or other valued social ends. In fact privacy is a moral and cultural continuum anchored on one end by absolutist claims for complete individual privacy, and on the other end by totalitarian societies where private and State organizations claim the right to obtain any information which furthers the purpose of the State (Figure 1).

Figure 1 Privacy as a Moral Continuum

In the middle of this continuum one finds due process claims to privacy, a negotiated area which strikes a compromise between organizational claims for efficiency and individual claims to privacy. The tilt of public policy can often be discerned by carefully examining what claim is given primacy. In some cases of

Figure 1



public policy, individual privacy is foremost unless a compelling state interest can be asserted, while in other policies organizational efficiency comes first unless a compelling individual interest can be asserted. This distinction becomes important below when considering privacy as a legal reality.

1.2 Privacy in Law

In the U.S. there are twelve major pieces of Federal legislation specifically regulating the collection, use, management, and dissemination of personal information by the Federal government and private organizations (Figure 2).

Figure 2

Federal Privacy Laws in the U.S.

(1) 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

(2) Privacy Laws Affecting Private Institutions

Fair Credit Reporting Act, 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

The seven major pieces of privacy legislation affecting the federal government set forth the due process rules that federal officials must follow when dealing with personal information. The most important contribution of this legislation is that it prevents 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 legislation also sets forth standards of computer security involving personal financial information. The omnibus Privacy Act of 1974 applies to all federal records and

sets forth the rules which the government must follow when managing personal information. The Freedom of Information Act is included here because it severely limits federal government claims that information it holds is "private" and cannot be shared with the public.

Among the significant limitations of this legislation is that it limits only the behavior of federal officials, and then only mildly. Some state and local officials, private citizens and organizations may rummage through your bank records or eavesdrop on your cellular phone conversations. A second limitation is that federal agencies have found loopholes in the law that permit 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 "absolutist" privacy protection in this legislation is the prohibition in the Privacy Act of 1974 against federal officials gathering information on citizens' exercise of their First Amendment rights. Perhaps the most important limitation of this legislation is that enforcement is left entirely to individuals who must recover damagers in court. There is no enforcement agency.

Figure 2 illustrates that private institutions have for the most part been exempt from privacy legislation. The only exceptions--and they are important large exceptions-- are the credit data, education, cable, and retail video industries where 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 your personal consent.

With these exceptions, for the most part there are no federal laws that offer any protection for the vast storehouse of personal information gathered by the private and public sectors. Figure 3 lists some of the major record systems--both private and public-- which can be and are accessed by private organizations and

individuals.

Figure 3
Major Record Systems Not Subject to Privacy Protections

Medical records
Insurance files
Credit card retail transactions
Personnel records
Rental, 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

An estimated 200 information superbureaus routinely access these basic systems, collate the information, and then resell it to government agencies, private businesses, and individuals (3)(Deveny 1989). Among the records offered for a fee are bank balances, rental history, retail purchases, social security earnings, criminal records, credit card charges, unlisted phone numbers, recent phone calls, and a host of other information services (4)(Rothfeder 1992). Together this information is used to develop a "data image" of individuals that is sold to direct marketers, private individuals, investigators, and government organizations. There are no laws regulating super bureaus per se.

1.3 Behavioral Privacy: Existing Information Markets

Laws are not always good indicators or predictors 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 towards defining privacy, many scholars have concluded 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 that in actual practice, with some exceptions, there are only a few meaningful limitations on the flow of personal information in the United States. Surveys of public opinion have documented a growing public concern over the loss of privacy and a growing demand for stronger legislation (5)(Equifax 1990; 1992).

In fact there is already a lively marketplace in the United States for personal information. This market is dominated by large institutional gatherers with little role currently for individuals to participate. Personal information is a valuable asset to private and governmental institutions who 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 the individuals involved have at best "an interest" but not ownership in information about themselves. The 400 million credit records maintained by the three largest credit agencies, 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, not to mention the billions of records maintained and stored by state and local governments, all have a real market value which is demonstrated everyday in the marketplace.

The inability of existing privacy legislation to effectively 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 marketplace in information, and a failure to bring economic perspectives to bear on the problem.

1.4 Re-thinking the Fair Information Practices Regime

Virtually all American and European privacy is based on a regulatory approach or regime called Fair Information Practices (FIP) first set forth in a report

written in 1973 by an advisory committee to the Secretary of the DHEW (6)(U.S. DHEW 1973). The five fair information principles are:

1) There shall be no personal record systems whose very existence is secret,
2) Individuals have rights of access, inspection, review, and amendment to systems that contain information about them,
3) There must be a way for individuals to prevent information about themselves gathered for one purpose being used for another purpose without their consent,
4) Organizations and managers of systems are responsible and can be held accountable for the damage done by systems, for their reliability and security, and
5) Governments have the right to intervene in the information relationships among private parties.

One of the key advances of FIP doctrine is its recognition that individuals have an "interest" in records which contain personal information about them even though those records are created by third parties. This followed, the report argued, from the fact of "mutuality of record generating relationships"--the fact that both parties in a transaction have a need for creating and storing records.

What is the nature of this "interest" and how could individuals and societies protect this interest? The Advisory Committee did not recommend a new enforcement agency, an Ombudsman, or individual ownership of information. Instead the Committee argued that any privacy laws should be enforced by individuals seeking redress in courts of law for damages done by invasion of privacy, and by building statutory incentives for large institutions to comply with the Fair Information Practices principles above.

Europe, Canada and many other nations have followed the lead of the Committee in defining privacy but often they have chosen to enforce their privacy

laws by creating Privacy Commissions or Data Protection Agencies. (7) (Flaherty 1979; 1989). Whether or not these nations have "more privacy" is open to question.

1.5 Technological and Institutional Limitations of the Fair Information Practices Regime

There are many problems with the FIP which seriously undermine its effectiveness in protecting privacy today. The FIP doctrine was based on the technological reality of the 1960s where a small number of very large scale mainframe databases operated by the Federal and State governments, or by large financial institutions, were the primary threats to privacy. In this period it was conceivable that an individual could know all the databases in which he or she appeared. But today large scale database systems can be operated by PC based networks (even individual PCs now rival the size of 1960's mainframe capacities). Large scale databases have become so ubiquitous that individuals have no possibility of knowing about all the database systems in which they appear. Hence the "no secret systems" principle, which originated in an era when only very large scale institutions possessed databases, is technologically out of date.

A cascade of serious problems follows: not knowing about so many systems, it is impossible to gain access, review or correct information in them. It becomes impossible to give "informed consent" for third party use of private information. (8) And it becomes impossible to know if managers of systems are holding personal information secure, reliable, and hence difficult to hold managers of these systems accountable or liable.

The FIP regime does not take into account other forces in modern society which mitigate against individuals having a social space to think, read, write, conspire, and innovate. The FIP does not take into account the systemic nature of the problem of information--how much it costs, who it costs, and who owns it. The

FIP perspective does not account for harm done to the entire society but focuses instead on individual injury. Imagine if we conceptualized and enforced environmental laws in this manner, with no federal standards or enforcement. (9)

Perhaps the most significant weakness of the FIP regime is its failure to specify a stronger form of "interest" that individuals have in their personal information. A strong form of "interest" would be a property interest rather than a mere juridical or administrative interest. We explore this option below.

Part 2 Finding Conceptual Support For Privacy in Microeconomic Perspectives

Due process, individual rights, and limitations on the power of the State and private organizations are all key ingredients in Enlightenment theories of social order. These perspectives have preserved what little privacy we have left. But other theories of social order have very different conceptions of information and privacy which are important to keep in mind when formulating new policies. In these other theories, progress depends upon the near unfettered exchange of information, and the reduction of any barriers to the flow of information. Insofar as these theories are reflections of real world forces, none of this bodes well for privacy (10)(Posner 1979).

2.1 When Things Go Right: Production Function Models of Order

In a perfect world characterized by perfect information and perfect information systems widely 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 market process) because it is embodied in labor

as knowledge and in capital which after all 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 of course 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). This has created an industry and market for new theories based on opposite assumptions: the asymmetric distribution of information.

2.2 When Things Go Wrong: Asymmetries in Information

A number of contemporary theories of social order are concerned with problems arising from asymmetries in the distribution of information, a more realistic view of the real distribution of information. 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)(Jensen and Meckling 1976; Fama 1980). 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 very 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 and more complex monitoring mechanisms. Public welfare declines as these investments produce no additional output. Information systems appear in agency theory as a convenient low cost monitoring

tool which permit firms to grow without increasing agency costs.

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 where contractors would compete with one another? In **transaction cost theory** the answer is that in markets participants have unequal access to information on the quality of goods and providers in the marketplace (12)(Williamson, 1985; 1975). It's costly to participate in markets: contracts have to be written, 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 where information on suppliers and prices, and costs of monitoring compliance with contracts, could be reduced. This means that firms could rely more on markets, less on firm growth in size. Likewise, firms could shrink in size (number of employees) as they expand business by contracting out vital services.

Other contemporary theories--adverse selection and moral hazard-- focus on market failures caused by asymmetries in information. Market failures are often attributed to asymmetries in information. Consider **adverse selection** (market situations where 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 these high rates and recognizing they rarely get sick anyway--and soon the insured pool becomes uneconomic to insure.

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. Drivers assume any additional accident costs they incur will be spread over a large group and their perceived marginal cost of driving is lower than what in fact it actually is. This forces insurance companies to raise rates on all drivers and encourages 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. At first glance it seems microeconomics is not friendly territory for privacy protection. But there is some salvation in the notion of externalities.

2.3 Paying the Price by Finding the Cost: Externalities

Pigou warned in the 1920s that when manufacturers did not bear the full costs of making their goods, when they could "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 resulting social inefficiency. 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 non-monetary values. If emissions from a chemical factory destroyed the paint on nearby autos, then chemicals were being produced at less than their true social cost, and they were selling at a lower price than they would otherwise.

The remedy to this problem of external cost is to "internalize" the cost: impose a tax on the chemical manufacturer equal to the size of the externality. When they are charged for the damage they create, so the theory goes, polluters will raise prices (forcing consumers to pay the full cost of their production), shift to non-polluting technologies, or reduce production.

One problem with this approach is finding the size of the externality. Ideally,

one would want to charge a tax on polluters just equal to the external costs. This is difficult enough when dealing with tangible externalities, e.g., damages to individuals and structures, but is very 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 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?

There are no easy answers to these questions. It may be much cheaper to permit some small level of obnoxious behavior for those willing to pay rather than ban it entirely which would require a huge bureaucratic effort. Enforcing the Clean Air Act of 1990 is estimated to cost billions of dollars through the year 2000, force uneconomic 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 may accomplish the same overall level of clean air at greatly reduced cost. Moreover, each polluter would be able to choose the best, most economic means of compliance with the law in order to reduce their taxes. This is far superior to bureaucratic dictates that all polluters use the same "approved" technology.

2.4 Externalities in an Information Economy

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 protection at a minimal enforcement cost? I think we can if we extend some of the thinking from information economics and externalities outlined above.

Part 3 Building Information Markets: The Cheapest and Best Protection of Privacy May Lie in Markets and Taxes-- Not Regulation

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

In the case of informational privacy, markets have either failed to function because of the lack of a legal framework, (i.e. who owns information about a transaction), or have been eliminated by collusion among very large market participants who benefit from externalities created in the current situation. The results of this failure of markets are several. First, the cost of using personal information to invade the privacy of individuals is far lower than the true social cost. This is because a part of the cost of invading privacy is borne by the individual whose privacy is invaded. Other costs (regulatory agencies) are created and then 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.

Second, as a result, large public and private institutions make far greater use of privacy-invading techniques than they otherwise would. Third, this results in a decline in public welfare 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, are costly and obnoxious. We tend to blame the technology for what in fact is an institutional situation we have ourselves 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 costs. Many invasions of privacy in a mass society occur through the secondary and tertiary uses of information gathered in the conduct of business and government. Under current law, individuals largely lose control over information gathered about them in the course of legitimate transactions. Once gathered it is beyond individual control, and sometimes this is sanctified by very weak "informed consent" clauses which themselves are often tied to a particular benefit, e.g., in order to receive a public benefit, citizens must agree that the information they give may be used for other purposes.(13)

Once individuals lose control of information about themselves, and lose any ownership in that 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 4 highlights some of the different kinds of coping costs.

Figure 4
Information Coping Costs (14)

Direct	Opening unsolicited mail Responding to telephone, e-mail, 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 towards government and large private organizations.

The solution to this problem is not regulation, or simply the creation of a "Data Protection Agency," however helpful this may be, but the creation and strengthening of information markets which are more symmetrical in terms of power and information.

3.1 National Information Markets (NIMs)

One possibility is the creation of National Information Markets (NIMs) in which information about individuals is bought and sold at a market clearing price. Institutions who gather 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, 1000 persons (name, address, etc.), basic demographics where available, and specialized information, e.g., health, financial, occupational, or market information. Different markets might exist for different kinds of information, e.g. financial assets, credit data, health, government, and general marketing.

National Information Markets would be the only legal avenue for the transfer of information about individuals being used for secondary purposes, i.e. for purposes and institutions other than those for which the information was originally gathered. Hence MasterCard could use information on your credit history for the purpose of authorization of future MasterCard purchases, but it could not sell your history of credit card purchases directly to other institutions. It could however sell this information on a National Information Market where it could be purchased by a credit bureau like TRW Credit Data who could then use the information for credit histories.

The National Information Market is self-supporting: a transfer tax is charged and this revenue is used to support the marketplace infrastructure, enforcement of rules, and monitoring activities.

3.2 National Information Accounts

A key aspect of a National Information Market is the development of National Information Accounts for both suppliers (individuals and institutions) as well as purchasers (information brokers, institutions, and individuals). Every citizen who chooses to participate in the marketplace would be assigned a National Information Account with a unique identifier number and unique bar code symbol.

The purpose of the NIA is several fold. Personal accounts are required to assure 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. Unique bar codes are required to control the flow of unsolicited mail in the U.S. Postal and private mail systems: no commercial unsolicited mail can flow through private and public post systems without a unique NIA identifier bar code which permits automatic crediting of NIA accounts.

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, National Accounts restore some measure of real control, and the subjective perception of control, and order to the flow of information. 15

The revenue percentage returned to individual's accounts would have a fixed floor and a variable ceiling depending on market conditions. A fixed floor is necessary because the invasion of privacy has some minimal cost. A variable ceiling is necessary because individuals should be able to set their own prices for participation in the market, including the right not to be included and not to be the object of privacy invasion. An "account blocking" capability is built into the markets' computers to prevent illegal buyers of information from participating or using personal information.

3.3 Information Fiduciaries

Because most people would not have the time or interest to participate directly in information markets, information fiduciaries would naturally arise. Information fiduciaries are agents acting on your behalf who have assumed certain responsibilities under law. 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, some percentage of the total returns. Such information fiduciaries could easily be recruited from the ranks of existing information superagencies and local credit/information bureaus.

3.4 National Information Clearinghouse

Participants calling an 800 number could find their account balance, and perhaps trace the flow of information about themselves, e.g., how did Brown Harriman Investment Banking who just contacted me with an unsolicited phone call obtain my bank balance information from the Bank of New York? A National Information Clearinghouse could empower individuals to trace the flow of information about themselves.

3.5 Government Exemptions

Would governments have to pay for information that it needs to administer programs? In general, no. The concept of National Information Markets applies only to secondary and tertiary uses of information for purposes other than those for which it was gathered. 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 this information to third parties, or seeks information from sources outside government programs, then it would be treated as simply another market participant and it would pay for information received, and be

compensated for information sold. In either event, individual citizens would receive some fair percentage of these transactions. Of course, for law enforcement and national security purposes, these restrictions may be waived.

3.6 Objections and Issues

There will be many objections to market-based approaches to privacy. Privacy advocates will worry that people will be encouraged to "sell" their privacy rights; the market may be regressive as wealthy people may charge more for their information than less well off people; and wealthy institutions willing to pay will be able to invade privacy whereas small businesses will not be able to afford privacy invasion on such a large scale. Privacy invasion will proceed, albeit at a lower level.

The credit data, financial service, health, and government agencies who benefit from and encourage the failure of information markets would object that National Information Markets are in reality an "information tax." Compensating individuals for use of information about them would raise the cost of doing public and private business transactions, result in less unsolicited market information coming to the consumer, potentially creating other market inefficiencies. Administering the marketplace, some will argue, would be a costly nightmare. Defenders of the FIP doctrine will object that a revolution in American property law would be required and that it would be impossible from a public policy view to create national information markets.

Let's take the objections of privacy advocates first. Privacy advocates typically argue for more regulation, more laws, more enforcement agencies, and more standards being imposed on everyone. With some notable exceptions, described earlier, this approach has not worked. In a market some people will indeed sell their privacy in a marketplace, the poor more than the rich, but the price offered will likely be so low as to not attract many sellers. Rich people may receive

much more in the marketplace 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 assuring a non-sale, or simply withdraw from the market entirely to preserve their privacy completely.

The point is that overall privacy invasion will decline, 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 markets will 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 protect ones privacy entirely.

As advocates of the status quo argue, transaction costs will indeed rise but only insofar as to pay for the cost of invading privacy, the externalities of the Information Age. National Information Markets will indeed impose a "tax" on the uses of some kinds of information for some kinds of purposes. The purpose of this tax is to discourage the obnoxious use of information which could undermine the foundations of a free society if left unchecked. There should not be any "free lunch" when it comes to invading privacy and currently that's just what the information industry wants.

National Information Markets will result in a decline in the use of unsolicited communications--a key source of privacy concerns. But it will also lead to cost savings as firms use the latest technology to target their communications to a smaller group, devise new ways to market products and obtain market information, and compete with one another on their privacy-regarding corporate practices.

The cost of administering National Information Markets will be trivial once the infrastructure is built. It will be self-supporting based on fees charged to market participants. As it turns out, information systems are marvelously efficient and powerful at keeping accounts and very useful in the creation of electronic markets

involving huge transaction volumes at only pennies per transaction. National Information Markets also open the possibility of detecting quickly large scale privacy invasions. (16)

No revolution in American property law is required to support national information markets. First, property law is quite flexible in recognizing value in a wide variety of tangible and intangible assets, including one's personal image. For instance, since the turn of the century courts have recognized the claims of celebrities to a property interest in their photographic image and the right of celebrities to seek compensation whenever their image is used for a commercial purpose. What is needed is the extension of a property interest to the digital data image of ordinary individuals.

3.7 National Oversight: A Federal Information Commission (FIC)

We have argued that the principal privacy enforcement mechanism be a marketplace rather than a regulatory agency. Nevertheless, even marketplaces need an oversight agency to assure 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 lines, and more in common with the U.S. Securities and Exchange Commission (SEC). Functions of the FIC would include:

*Creating and monitoring National Information Markets
*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 on information matters

3.8 The Responsibility of IS Professionals

IS professionals in a democracy are obligated to help individuals and society achieve that level of privacy required for the preservation of democracy. IS professionals also have obligations to the organizations for whom they work to achieve efficiencies in administration which may require the extensive use of personal information. These obligations are not necessarily opposed and there are several opportunities for professionals to have a positive impact on their resolution. First, we should ensure that our professional associations (the ACM, DPMA) develop public policies on privacy and clarify the obligations of professionals. Second, we should encourage organizations that claim to represent and speak for IS professionals in Washington (like CPSR--Computer Professionals for Social Responsibility) to seriously consider new ways to achieve privacy aside from the traditional methods of more regulation and more bureaucracy in the form of Data Protection Commissions and the like. Third, we should encourage our employers to devise policies which do not

Part 4 Conclusion: Towards Second Generation Privacy Policies

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

If privacy is to be taken seriously as a public value, then the solution is to rely on more powerful and less wasteful mechanisms like markets to reduce the level of

privacy invasion. As things currently stand, there is much more unsolicited invasion of privacy than is tolerable, socially efficient, or politically wise. The current situation is costing corporations billions of dollars in sheer waste as they pour money into privacy-invading marketing and authorization techniques. Millions of dollars worth of junk mail is tossed out without even being opened, millions of telephone solicitations result in hang-ups, 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 suggesting a polluted, even toxic information environment. A powerful way to clean our information environment is through a mixture of market and regulatory mechanisms.

Notes

1. The development of the right to privacy (and its definition as the right to be left alone) in American law is given in the classic article by Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy," 4 Harvard Law Review, 193 (1890); and later this phrase appeared in a Brandeis dissent in Olmstead v. United States 277 U.S. 438, 473 (1928) in a case concerning the admissibility of wiretap evidence. Other contemporary works are Alan F. Westin, Privacy and Freedom, New York: Athenum, 1967; Kenneth C. Laudon, Dossier Society, New York: Columbia University Press, 1986; and David Flaherty, Protecting Privacy in Surveillance Societies, University of North Carolina Press, Chapel Hill, N.C., 1989; and Colin J. Bennett, Regulating Privacy: Data Protection and Public Policy in Europe and the United States, Ithaca, New York, 1992). See also Ruth Gavison, "Privacy and the Limits of Law," The Yale Law Journal 89, No. 3, January 1980.

2. Claims to privacy are so widespread and powerful that the cultural assumptions are reflected in important documents like the Declaration of Independence in the U.S., and the U.S. Constitution. While not mentioning 'privacy' per se, these documents declare that individuals shall be free to "life, liberty, and the pursuit of happiness" (Declaration of Independence), and they guarantee against government abridgement of "freedom of speech," (First Amendment), and the "right to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.." (Fourth Amendment). In other cultures like Germany or Sweden similar claims to privacy are expressed. The development of the right to privacy (and its definition as the right to be left alone) in American law is given in the classic article by Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy," 4 Harvard Law Review, 193 (1890); and later this phrase appeared in a Brandeis dissent in Olmstead v. United States 277 U.S. 438, 473 (1928) in a case concerning the admissability of wiretap evidence. Other contemporary works are Alan F. Westin,

Privacy and Freedom, New York: Athenum, 1967; Kenneth C. Laudon, Dossier Society, New York: Columbia University Press, 1986; and David Flaherty, Protecting Privacy in Surveillance Societies, University of North Carolina Press, Chapel Hill, N.C., 1989; and Colin J. Bennett, Regulating Privacy: Data Protection and Public Policy in Europe and the United States, Ithaca, New York, 1992). See also Ruth Gavison, "Privacy and the Limits of Law," The Yale Law Journal 89, No. 3, January 1980.

3. See for instance Kathleen Deveny, "Is Nothing Private," Business Week, September 4, 1989.
4. Jeffrey Rothfeder, Privacy for Sale, New York: Simon and Shuster, 1992. See also

5. See the Equifax Report on Consumers in the Information Age, A National Survey. Equifax Inc., 1990.
Public opinion recognizes the absence of privacy and the weakness of existing law. Public opinion polls show that when it comes to information privacy most Americans are bewildered, fearful, confused, and increasingly distrustful about public policy in this area. According to a recent Harris poll, 79% of the public is "concerned or very concerned" about their privacy, 76% of Americans believe they have lost all control over personal information, and 67% believe that computers must be restricted in the future to preserve privacy. Most Americans feel powerless to do anything about what happens to their personal information held by third parties.

6. U.S. DHEW, Records, Computers and the Rights of Citizens. Cambridge: MIT Press, 1973

7. Few would deny that European EEC countries and Canada have stronger data protection and privacy mechanisms in place than the United States. The differences among countries have many origins in politics, culture, and history. There are three primary differences among nations: (1) the presence of explicit Constitutional protections versus mere statutory protections, (2) the existence of a formal bureaucratic enforcement agency versus reliance upon individuals, and (3) formal recognition of international privacy conventions and declarations. [See Figure 3]

While some argue that the stronger European laws and regulatory structures create "stronger protections of privacy," there is little objective or subjective evidence that "more privacy" exists in these countries than in the U.S. Conceptually, the European and Canadian approaches to privacy are heavily dependent upon and influenced by the Code of Fair Information Practices developed by DHEW in 1973. See David H. Flaherty, Privacy and Government Databanks: An International Perspective (Mansell, London, U.K., 1979); and Flaherty, Protecting Privacy in Surveillance Societies, University of North Carolina Press, Chapel Hill, 1989). See also Priscilla Reagan, "The Globalization of Privacy: Implications of Recent Changes in Europe." Paper delivered at the Annual Meeting of the American Sociological Association, August 20-24, 1992.

For an excellent review of the differences between American and German law, and an appreciation of the German Constitutional Court's doctrine of "right of informational self-determination" see Paul Schwartz, "The Computer in German and American Constitutional Law: towards an American Right of Self-Determination," The American Journal of Comparative Law, Volume XXXVII, Fall 1989 Number 4.

8. In the U.S. and many other countries, "informed consent" is tacitly obtained by a "Privacy Notification" on documents listing routine uses of the information, sometimes with an option to "opt out" (and sometimes lose a benefit). "Informed consent" under these circumstances is not consent at all and poses little threat to governments who wish to use whatever data they want.

9. An analogy to toxic pollution is appropriate here. Imagine that we protected our physical environment with principles like FIP (Fair Information Practices). Take away the EPA, all environmental laws, and replace it with a single law based on the following principles:

1) You have a right to know what toxic substances, if any, your employer or local industry may be exposing you to,

2) There can be no secret pollution and all pollution will be done in pursuit of commerce or a statutory purpose, in an orderly fashion,

3) Managers and organizations are accountable for the pollution they create and can be held liable for any proven damages they do to individuals,

4) Government has the right to regulate pollution.

Now imagine the bewilderment of the American public if they were told, "If you think you've been harmed by some industrial polluter, you should sue that polluter in a Court of law."

Obviously, placing the burden of proof upon individuals who would have to demonstrate actual harm in court, harm which might be irreversible, would destroy any possibility for systematically addressing environmental pollution before harm was done. The only environmental policy would be correction of past catastrophes. Likewise with privacy: we need a far broader foundation and understanding to protect privacy in the 21st Century.

10. For an interesting application of economic thought to privacy and secrecy, see Richard Posner, "Privacy, Secrecy, and Reputation," Buffalo Law Review, Vol. 28, 1979.

11. See Richard Jensen and William Meckling, "Theory of the Firm: Managerial Behavior, Agency Costs, and Ownership Structure," Journal of Financial Economics

11 (1976): 305-360; and Eugene Fama, "Agency Problems and the Theory of the Firm," Journal of Political Economy 88 (1980).

12. See Oliver E. Williamson, The Economic Institutions of Capitalism, New York: Free Press, 1985; and O. E. Williamson, Markets and Hierarchies, New York: Free Press, 1975.

13. We have avoided the knotty question of who owns information about a transaction. For instance, does an individual credit card holder retain some ownership or tangible interest in records about his (her) credit card transactions? Focusing on "costs" allows us to sidestep this issue temporarily. Ownership interests returns as an issue when we discuss "cost compensation" or who receives the revenue from privacy invasion.

14. Direct costs are those that can be attributed to a specific activity, division, or product. Indirect costs are those which cannot be so attributed and are usually allocated arbitrarily. Tangible costs (benefits) are those which are palpable and can be easily quantified. Intangible costs (benefits) are those which cannot be easily quantified.

15. The revenue percentage returned to individual's accounts would have a fixed floor and a variable ceiling depending on market conditions. A fixed floor because the invasion of privacy has some minimal cost. A variable ceiling because individuals would be able to set their own prices for participation in the market, including the right not to be included and not to be the object of privacy invasion. An "account blocking" capability is built into the markets' computers.

16. Some possibilities here are to encourage private industry to manufacture devices to protect personal privacy--technological data security. Congress should discourage efforts by public agencies like the FBI to deny individuals the right to technological data security. For instance, the argument of the FBI and other security agencies that new digital services be built in such a way as to make "wiretapping" feasible, and that firms should be prohibited from marketing products that encode digital communications, is simply ludicrous. Privacy is a precious commodity, the more so when criminal conspiracy is afoot. The technological means for scrambling digital transmissions is sufficiently wide-spread and powerful as to make its prohibition through a "Digital Volstead Act" meaningless. Worse, a new market could be called forth to distribute precisely those products the FBI fears most.

In addition, privacy invaders can be quickly detected and punished. Inevitably there will be attempts to circumvent National Information Markets by using information gathered from a black market. Firms that attempt this and get caught can be locked out of the marketplace for a period of time, and they can be prohibited from using postal and telecommunication systems all of which would require a code to initiate communications. The postal system and telecommunications systems then become crucial enforcement mechanisms.