The Revolution in Access Control: Markets for Electronic Privacy[1]

August 1996

Paper for the

"Aspen Summit '96: Cyberspace and the American Dream"

sponsored by the Progress and Freedom Foundation

Prof. Eli M. Noam
Professor of Finance and Economics
Director, Columbia Institute of Tele-Information
tel: (212) 854-4596
fax: (212) 932-7816
e-mail: enoam@research.gsb.columbia.edu
or www.ctr.columbia.edu/citi/

I. INTRODUCTION:

For a long time, the conventional wisdom was that electronic communications constituted a major threat to individual privacy. Wiretapping, eavesdropping, and data banks were part of the Big Brother and Nosy Sister scenario. This fear for personal privacy is justified in the short term. But in the long term, the opposite is more likely to happen, because the electronic tools that permit privacy invasion are even more powerful in controlling an individual's informational autonomy. In the process, still another revolution is upon us, the *revolution of access control.* By gaining such control individuals achieve bargaining strength over those who seek information about them. They can establish a perimeter over the inflow and outflow of information. They can create property rights in personal information. Transactions become possible, and markets in private information can emerge.

No problem is ever new. Jeopardies to privacy have been associated with electronic

[1] Assistance by Thomas Aust, Bruce Olcott and Jérôme Wagner is gratefully acknowledged, as are helpful comments by [ ].

media from the beginning. Gossipy manual operators,[2] party lines with participatory neighbors,[3] and the absence of a warrant requirement for wiretapping[4] all created privacy problems.[5] The first American patent for a voice scrambling device was issued only five years after the invention of the telephone.

The New York Police Department, always on the technology frontier, listened in on telephones since at least 1895. In 1916 this led to a public controversy about eavesdropping on a Catholic priest as well as on a law firm involved with competitors to J.P. Morgan & Co. for World War I munitions contracts.[6]

Today, a new generation of electronic privacy problems has emerged, for several reasons:

- An increasing number of transactions are conducted electronically.[7]
- It has become easier and cheaper to collect, store, access, match, and redistribute information about transactions and individuals.[8]
- Wireless transmission conduits include unsecured portions.
- The number of communications carriers and service providers has grown enormously, leading to an increasingly open network system in which information about use and user is exchanged as part of network interoperability.
- The Internet computer network system is wide open.

In consequence, new electronic privacy problems keep emerging. Recent controversies include:

- Intrusive telemarketing
- Data collection about transactions
- The ability of governments to control encryption.

---

[2] Recall the TV series "Petticoat Junction."

[3] Recall the movie "Pillow talk."

[4] Olmstead v. United States, 277 U.S. 438 (1927)

[5] See Westin (1967).

[6] Seipp (1981).

[7] For example, in 1962, the U.S. federal government had 1030 computer central processing units; in 1972, 6,731; in 1982, 18,747; and in 1985, over 100,000. (Linowes, 1989). Today, their equivalent is probably beyond counting.

[8] In the past twenty years the cost of access to a name on a computer-based mailing list has come down to about one thousandth of its earlier cost.

- The ability to determine an incoming caller's phone number and the use of such information.
- The monitoring of wireless mobile communications,
- employers' monitoring of their employees.
- The ability of using e-cash for illegal transactions.
- The difficulties of law enforcement agencies to keep up with transmission technology.
- The unsecured nature of the Internet, and the ability to track the sites which an individual visits.

And more is coming our way. For example, tiny mobile communication transceivers, together with number portability, will enable telephone subscribers to be continuously connected. Their locational whereabouts, their comings and goings, and the identity of other persons in the same location could, therefore, be continuously ascertained.

Given that privacy is important to so many people, and given that information technology keeps raising new questions, what should the approach to deal with privacy problems?

In the past, if remedies were considered, the primary strategy has been to resort to regulation. The call for the state to control and protect privacy is a natural response especially in the field of electronic communications, given their history around the world as either a state-controlled telephone or broadcast monopoly or tightly regulated sector. This has led to a view of electronic privacy problems largely as an issue of rights versus the state or its regulated monopoly firms-- and to the question how to create such rights in the political, regulatory and legal sphere. But such a view is static: having a right is often believed to be the end of the story. Yet in most parts of society, the allocation of rights is only the beginning of a much more complex interaction.

Privacy is an interaction, in which the rights of different parties collide. A has a certain preference on the information he receives and lets out. B, on the other hand, may want to learn more about A, perhaps in order to protect herself. The controversies about caller-identification, or of AIDS disclosure of medical personnel, illustrate that privacy is an issue of control over information flows, with a much greater inherent complexity than a conventional "consumers versus business", or "citizens versus the state" analyses suggests. In this case, different parties

have different preferences on "information permeability" and need a way to synchronize these preferences or be at tension with each other. This would suggest that interactive negotiation over privacy would have a place in establishing and protecting privacy.

While this article will not suggest that markets can provide a solution to every privacy issue, it will argue that they can be utilized much more than in the past.

II. WHAT IS PRIVACY?

In the information sector, privacy consists of two distinguishable but related aspects:[9]

(a) The protection against intrusion by unwanted information. This is sometimes termed "the right to be left alone,"[10] and it is an analogue to the constitutional protection to be secure in one's home against intrusion.

(b) The ability to control information about oneself and one's activities; this is related in some ways to proprietary protection accorded to other forms of information through copyright laws,[11] and security of information about oneself from tampering by others.

The common aspect of both these elements is that they establish a barrier to informational flows between the individual and society at large. In the first case, it is a barrier against informational inflows; in the second instance, against informational outflows.

The concept of privacy is not without its detractors. Among the major criticisms are:

(a) "Privacy protects anti-social behavior"

In this view, privacy is a smoke-screen used to hide activities that should be discouraged. This may be true at times; yet it is also the price of personal freedom. Authoritarian or backward societies do not value a private sphere since they do not tend to respect individuality and subordinate it to the demands of rulers or societal groups.[12] The recognition of a private

---

[9] See, e.g., Richard Posner, (1981).

[10] Warren and Brandeis, (1890).

[11] The common-law copyright protection provided primarily that if one had not published information in one's possession, no one else could take and publish it. This was similar to a trespass and conversion action.

[12] On the history of privacy, see Posner (1981); Simmel (1906); Westin (1965); Seipp (1978). In the United States, privacy is a non-partisan issue. The Privacy Act of 1974 was co-sponsored by Senators Edward Kennedy and Barry Goldwater.

sphere is hence one of the touch-stones of a civilized and free society.[13]

(b) "Privacy is costly to the economy"

Privacy protection raise the cost of information search. For example, potential employers and buyers have to spend more effort (and money) to find out who they are dealing with if access to personal information is restricted. Deception becomes easier and transaction costs rise.

But there are also economic arguments on the other side. Privacy affects the ability of companies and organizations to hold on to their trade secrets and details of their operations, and to protect themselves from leaks of insider information and against governmental intrusion. Information has value, and where it has no protection through property rights it must be protected through confidentiality or secrecy.[14] To permit its easy breach[15] would lead to a lesser production of such information.

The loss of privacy leads to inefficiency in information flows, just as excessive privacy protection may. One of the predictable results of third party monitoring of telephone calls is to force speakers to disguise or modify their communications in order to keep them secret. A staple of spy novels are enormously complex transfers of information, and equally elaborate restrictions of access to it. This adds cost, wastes time and increases errors.

Partly in response to economic and social needs, many transactions have been specifically accorded special common-law informational protection known as "privileges," e.g. between attorney-client, patient-doctor, citizen-census taker, penitent-clergy, etc. The idea in each case is that the protection of information leads to an economically and socially superior result even if it is inconvenient in an individual instance to others.

(c) "There is no demand for Privacy"

This objection views privacy as an issue of concern only to a small elite group. But to the contrary, attention to privacy is widely shared. For example, according to information from the New York Telephone Co., of a few years ago, 34% of all residential households in Manhattan and 24% of all its residential households in the State had unpublished telephone numbers at

---

[13] Justice Louis Brandeis, in a famous dissent, wrote of "the right to be left alone -- the most comprehensive of rights and the right most valued by civilized men." Olmstead at 478.

[14] In the extreme, private information is so valuable to an individual as to make him a target for blackmail. See also Brown and Gordon (1980) for an economic perspective from the FCC.

[15] See Richard A. Posner, *The Economics of Justice*, Harvard University Press, Cambridge, Massachusetts (1981, pp. 231-347).

subscribers' request. Most policemen, doctors, or judges, to name but a few professions, have unlisted numbers. On the West Coast, the spread of unlisting is still further advanced, reaching 55% in California! It should be noted that it costs extra to be unlisted. In other words, a large number of customers is willing to pay in order to increase its privacy. With more than half of the population willing to do so, it becomes impossible to keep denying that privacy is an important issue.

III. POLICY APPROACHES

As the new technological options emerge they create new opportunities but also new privacy problems. How can such problems be dealt with?

As was mentioned, the primary policy response has been regulatory. Within that position there were two major directions -- centralized general protection and decentralized ad-hoc protection. West European countries, in particular, have pursued the former, and passed comprehensive (omnibus) data protection laws and established institutionalized boards with fairly rigorous rules, and coordinated internationally on information collection and data flows.[16] The United States, in contrast, has dealt with specific problems, one at a time, and with different approaches across the country.

In Europe, advances in data processing led in the 1970s to fears about the abuse of information storage and the potential for a "1984"-like surveillance state would become possible. Many of these fears were based on the technological notion of computers as vast centralized mainframes, a notion which corresponded to the state of computer technology of the 1960s. But since then, this technology has moved steadily toward a decentralized system, with millions of small computers in people's offices and homes.

Though the origin of concern over privacy was the potential violence abuse of data by government agencies, the focus of remedial action shifted quickly to data collection activities by private business. Rules against the government's collection of data were also set, but with less severity. At the same time that Germany promulgated the first data protection laws against private data abuse, its federal and state governments took a quantum leap in the use of data—processing technology for the surveillance of its citizenry. During the 1970s, a handful of

---

[16] See Noam, Eli M., *Telecommunications in Europe*, Oxford University Press, 1993.

terrorists prompted the German police to institute a chillingly efficient system of border checks, citizen registration, data access, and domestic road blocks, all of which were interconnected by data banks and communications links. Although the terrorism was quickly stopped, many control mechanisms were not.

Additionally, the rules had a tendency to spread. It was soon recognized that privacy laws had a loophole: international data transfers permitted the evasion of data protection laws. In Sweden, for example, a data file on any employee is subject to protection from disclosure to third persons. However, if a Swede works for a foreign firm, it would be possible that the data would be transmitted to the headquarters of the firm, where it would be less protected. Conceivably, therefore, some countries could set themselves up as "data havens" in order to attract businesses determined to circumvent privacy laws. Although these threats were more theoretical than real, they led to a movement to "harmonize" data protection practices or to restrict the flow of sensitive data in the absence of such harmonization.

The Organization of Economic Cooperation and Development (OECD) was instrumental. In 1979, the OECD drafted a first set of guidelines for its member states: Data collection should be limited to necessary information obtained lawfully, and, where appropriate, with consent; data should be accurate, complete, up-to-date, and relevant to the needs of the collector; use of the data ought to be specified at the time of collection, and its disclosure should be in conformity with the purpose of collection; assurances must be made against unauthorized access, use, and disclosure; and data should be open to inspection and correction by the individual to whom it refers.[17]

The Council of Europe incorporated the OECD guidelines in the 1980 Convention on the Protection of Individuals with Regard to Automatic Processing of Personal Data. The convention affected all transborder data flow among European countries and with other countries, such as the United States. This made American firms with international business activities nervous, since the convention provided that any country could restrict the transmission of data to another country that did not have data protection legislation comparable to its own. Since firms conducting international transactions generally prefer to have uniform procedures for transactions in various countries, procedures were likely to conform to the strictest of the national rules.

---

[17] Organization of Economic Cooperation and Development, 1979.

In 1992, the European Commission adopted a directive establishing basic telecommunications privacy rights for its member states. The draft included restrictions on unsolicited calls, calling number identification, and use and storage of data collected by telephone carriers for electronic profiles.[18] It mandates that holders of data pay for security measures in order to bar unauthorized access. It also prohibits the creation of electronic profiles of individuals utilizing data concerning their purchases or other actions, and it bars transfers of data to non-EC member countries unless those countries have adequate data protection rules.[19]

Among Third World countries, Brazil has been particularly active in data and telematics issues. Instituted during the years of military dictatorship, the thrust of Brazil's policy was evident in the statement of its then top information officer, who combined both the civilian and military and functions of that term.

> The administration [i.e., the restriction] of TDF [transborder data flows] appears to be an effective government instrument for the creation of an environment that makes the emergence of an internationally viable national data-service industry possible. By itself, such an industry would have had great difficulties in overcoming the obstacles of a completely "laissez-faire" environment. The country's TDF policy altered that situation.[20]

A license had to be obtained before establishing international data links. Applications for foreign processing, software import, and database access were rejected if domestic capability exists. The policy was strongly embraced by the Brazilian military dictatorship and its business and industrial allies, and it was admired around the world as an assertion of national sovereignty by many observers who would otherwise feel no kindness toward right-wing juntas.

In the United States a generally more pragmatic approach to legislation, and a case-oriented decision process administered through the judiciary and the regulatory agencies, have led to the tackling of specific data abuses when they became apparent rather than to comprehensive laws. This has led to a less systematic approach than in Europe, and to a variety of ad hoc federal and state legislation. Typically, they addressed a narrow and specific issue of concern.[21]

---

[18] Gilhooly, 1990, p. 1; CEC, 1990, p. 5.

[19] Oster, Patrick; Galen, Michele; Schwartz, Evan, *Privacy vs. Marketing: Europe Draws the Line*, Business Week, June 3, 1991.

[20] Pipe, 1984b.

[21] A 1990 example is a Congressional bill for monitoring of computer bulletin boards by the host system operators in order to prevent use for illegal activities.

Most of such statutes were either aimed at particular industries (for example, credit rating bureaus), or at the conduct of governmental agencies, or they dealt with flagrant abuse such as computer break-ins.[22]

Thus, contrary to often-held views in other countries, numerous laws protecting data and privacy exist in the United States, and some of them are quite far-reaching, especially in terms of access to state files, and limits on such files.

Nevertheless, U.S. privacy legislation remains considerably less strict than European law in the regulation of private databases, and the coverage of American governmental organizations by privacy law is not comprehensive. Although the Privacy Act of 1974 restricts collection and disclosure by the federal government, and vests some responsibility in the Office of Management and Budget, only a few states and local governments have passed similar fair information practices laws for their agencies. The U.S. has no government agency specifically charged with data protection similar to the centralized data protection commissions or authorities established in European countries, though proposals have been advanced in Congress.

A synthesis of the comprehensive European and the ad-hoc American approaches is to formulate a set of broad rules or principles applicable to a sector of the economy, or to a set of issues. This was the direction taken by the New York Public Service Commission on the issue of telecommunications privacy.

The New York Public Service Commission's approach in 1991 went well beyond the problem-specific approach. It issued, after a proceeding initiated by the author, a set of broad privacy principles applicable to the whole range of telecommunications services under its jurisdiction.[23]

A similar approach,that of privacy principles, was recently taken by the Federal Government's high visibility Information Infrastructure Task Force, in the report by its Privacy Working Group, which issued a set of Principles for Providing and Using Personal Information. But that report is virtually devoid of a discussion of a market mechanism in protecting privacy, or in integrating such mechanisms in its privacy principles.

---

[22] Shaffer, David, *Ban on Recording Telemarketing Upheld*, St. Paul Pioneer Press, March 29, 1993. (For example, the state of Minnesota banned the use of automatic dialing equipment. The United States Supreme Court let stand a Minnesota Supreme Court decision upholding the ban despite arguments that such a law violates constitutional free speech protection.)

[23] See *Proceeding on Motion of the Commission to Review Issues Concerning Privacy in Telecommunications*, Case 90-C-0075, State of New York Public Service Commission, March 22, 1991.

IV. MARKETS IN PRIVACY?

The reflexive approaches to privacy problems has been regulation, or denial. Are there other options?

First, there is the possibility of self-regulation, where an industry agrees to restrict some of its practices. Realistically, though, self-regulation is rarely voluntary (unless serving an anti-competitive purpose): it usually occurs only under the threat of state regulation, and it can therefore be considered a variant of direct regulation.

The practice for the state to control and protect privacy is a natural response in the telecommunications field, given its history as a state-controlled monopoly. It has led to a view of privacy problems largely as an issue of rights, and the question is how to create such rights in the political, regulatory and legal sphere. Such a view is appropriate in the context of privacy rights of the individual against the state. But the same cannot be said for the privacy claims of individuals against other individuals. The allocation of rights is only the beginning of a much more complex interaction. Some people may want and need more privacy than others. Privacy, by definition, is an interaction in which the informational rights of different parties collide. Different parties have different preferences on "information permeability" and need a way to synchronize these preferences or be at tension with each other. This would suggest that interactive negotiation over privacy would have a place in establishing and protecting privacy.

How should one analyze the role of bargaining over privacy? It is useful to consider as a framework for discussion the economic theorem of Nobel laureate Ronald Coase, a Chicago economist. Coase[24] argues that in a conflict between the preferences of two people the final outcome will be determined by economic calculus and (assuming reasonably low transaction costs) result in the same outcome *regardless* of the allocation of rights.[25] If the final result is the same, who then should have the rights? According to Coase, it should be the "least cost avoider," i.e., the party who can resolve the conflict at the lowest possible cost.

Let us apply this discussion to privacy, using the example of telemarketing. Both of the parties to a telephone solicitation call attribute a certain utility to their preference. For example,

---

[24] Ronald Coase, *The Problem of Social Cost*, The Journal of Law and Economics 3 (October 1960) 1-44.

[25] If the final result is the same, who then should have the rights? According to Coase it should be the "least cost avoider," i.e. the party who can resolve the conflict at the lowest possible cost.

it may be worth $3 to the telemarketer to have an opportunity to talk to the consumer. If necessary, she would be willing to pay a potential customer up to that amount.

Conversely, assume that the consumer would be willing to pay -- grudgingly for sure -- up to $4 to the telemarketer to keep her off the phone. The $4 is the value he places on his privacy in this instance. Thus, if the telemarketer has a legal right to call the consumer at home, the latter would "bribe" her not to call in order to keep his peace and quiet.

The basic decision on regulatory rights is either to prohibit unsolicited telemarketing calls, or to permit them. But regardless of which rule is adopted, the call will not take place, because under our numerical example the value of privacy to the consumer is greater than its interruption is to the telemarketer. But if for some reason the value to the telemarketer would rise, say to $6, the consumer could not pay her enough not to call; and conversely, if the telemarketer would have no initial right to make unsolicited calls, she would pay for the consumer's cooperation by a payment of $4 or more, so that the call is accepted.

In other words, the distribution of the legal rights involved may largely determine who has to pay whom, not whether something will happen. Thus the law does not necessarily determine whether telemarketing calls actually take place, it only affects the final wealth distribution. This interactive concept is often difficult to grasp if one is used to think in absolutes of black-letter law. Common law, in contrast, has recognized transactions from the beginning. Indeed, the original legal cases which established the tort of privacy were not based on a finding that the plaintiff had a right to privacy, but instead that the plaintiff had a right to be adequately compensated.[26]

For privacy transactions to occur, however, there are several prerequisites. They include:

- sufficiently low transaction costs
- a legal environment that permits transactions to be carried out
- an industry structure which permits transactions to occur
- symmetry of information among the transacting parties
- no "market failure", i.e. no growing instability in the market.[27]

---

[26] Posner, at 255. The early cases developing the tort of privacy often involved the use of a person's likeness in commercial advertising without permission or offer of monetary compensation. e.g., Pavesich v. New England Life Ins. Co., 50 S.E. 68 (1905)(The unauthorized use of a man's photo in an insurance advertisement).

[27] For a discussion of the limitations, see Noam, Eli M., *Privacy in Telecommunications: Markets, Rights, and Regulations,* Office of Communication, United Church of Christ, April 1994, 5M.

- The ability to create property rights, or to exclude.

Courts have been reluctant to grant property rights to personal information outside of the case of luminaries. In one case,[28] *Avrahami vs. U.S. News & World Report*, a gutless court[29] managed to hold for two organizations that exchanged subscriber name lists without permission, even though Virginia Code 8.01-40 (Michie 1999) clearly provided that "Any person whose name, portrait, or picture is used without having first obtained written consent of such person... for advertising [ ] pictures for the purposes of trade, such person may maintain a suit... to prevent and restrain the use thereof." The statute also permitted the aggrieved party to recover actual and punitive damages.[30] The court held that the inclusion of a name was "too fleeting and incidental", and that a person's name was not personal property. An appeal may be brought before the Virginia Supreme Court.

This reluctance of courts (and probably of legislatures) to recognize property rights in residual information is not surprising in light of the role of direct marketing in the economy. However, property is only not established from above by formal statutes or court decisions, but also from below, by the simple mechanism of an individual's ability to exclude others. Good fences create good neighbors, and good transactions as well. Electronics makes this increasingly possible. Such access control creates the possibility of bargaining, by transforming information from a "public good" (like a light house's flashing) to a private good (like a flashlight).

V. EXAMPLES FOR THE MARKET APPROACH

A. Telemarketing

As we discussed, because privacy and access are of value to parties in a telemarketing transaction, exchange transactions will emerge once they become technically feasible. How could this happen on a practical level? Signaling technology and telecommunications equipment provide now the capability to select among incoming calls electronically. This creates the precondition for access control by individuals, namely information about the calling party, which

---

[28] Commonwealth of Virginia, Circuit Court of Arlington County, At Law No. 95-1318, June 13, 1996.

[29] The court found that direct marketing accounted in 1995 for approximately one billion dollars in revenues.

[30] In New York, property rights in one's likeness and name go back to the turn of the century. See New York Civil Rights Law 8850, 51., enacted 1903.

until now enjoyed the stealth of anonymity. Information is power, or rather it is worth money. Once this choice of avoiding calls is available to the called party without loss of important incoming calls, callers must offer incentive to be admitted. Friendship, family ties, reciprocity, useful information business -- or a financial payment. What will therefore inevitably emerge is a system of individualized access charges.

Such a system might be described as **Personal-900 Service,** analogous to 900-service in which the caller pays a fee to the called. The caller would be automatically informed that the customer charges telemarketers for his time and attention.

Individual customers could set different price schedules for themselves based on their privacy value, time constraints, and even the time of day. They would establish a "personal access charge" account with their phone or an enhanced services provider, or a credit card company. By proceeding, the telemarketer enters into a contractual agreement. The billing service provider would then automatically credit and debit the accounts in question.

Such a system will probably have a negative impact on the business of telemarketers. Currently, they "externalize" some of their costs by accessing customers at home at no charge to themselves other than their operating cost. Right now, consumers do not yet have the means to make the telemarketer compensate them for their attention. (In television, the audience gets at least to view an entertainment, sports, or news program.) Under personal-900, telemarketers will be forced to pay more for consumer access.

Consumers will benefit from the payment they receive for accepting calls. Some might even become "professional call-receivers," though telemarketers will no doubt refine ways to select the most likely buyers. Telemarketers will become more selective in who they try to reach, and spend more money on "fine tuning" their customer list. Technological tools to refine their search are intelligent agents sent out to find interested and affordable targets for solicitation.

Markets in access will develop. Consumers will adjust the payment they demand in response to the number of telemarketer calls competing for their limited attention span. If a consumer charges more than telemarketers are willing to pay, he can either lower access or will not be called anymore. Prices could vary by time of day.

Consumers will bear some of the portion of these costs. First, by way of higher prices for telemarketed products. The extent to which these costs can be shifted by telemarketers to buyers depends on the relative elasticities of demand and supply. Where telemarketers are in

strong competition with other forms of marketing, and where consumers are price-inelastic, telemarketers will bear most of the added cost.[31]

B. Wireless Transmission

Market forces may also be able to resolve the unauthorized eavesdropping of wireless communication systems such as cellular and cordless telephones. True, such monitoring is illegal for cellular calls (though not for cordless phones), but it is widely practiced by scanning hobbyists as well as investigators. Just ask Prince Charles.

Eavesdropping is inefficient because it forces the participants in a communication to disguise the content of their transmissions, or to seek other ways of communicating. Thus, there are incentives for cellular service providers or equipment firms to offer scrambling devices.[32]

Encryption systems require extra equipment and may increase the amount of spectrum required for a given quality and information content of a signal. Customers who value privacy sufficiently will be willing to pay for the increased resource cost.[33]

C. Data Banks

Companies often sell or pass along information about their customers to others, for a variety of purposes. Insurance companies want to know the accident and medical history of new applicants; stores, whether new customers are credit-worthy; employers, whether job applicants have criminal histories; doctors, whether a patient has brought a malpractice suit in the past; and so on.[34]

---

[31] One might argue that telemarketers will attempt to avoid absorbing this added cost by increasing their prices and then advertising a "fictitious" discount in return for a customer giving access rights. But such a practice will not succeed in a competitive environment where the initial price increases cannot be sustained.

[32] For example, GTE has released since 1991 an encryption system for the cellular-consumer market. GTE Mobilnet developed the system because some customers -- mostly government accounts and defense contractors -- were concerned about the use of scanners that can monitor radio waves over which mobile-telephone signals.

[33] A special problem of privacy in mobile communications is that the person initiating the call to a mobile customer does not pick its privacy level, and may be entirely unaware of any jeopardy. This "negative externality" suggests that some form of a signal which alerts such a caller to the presence of radio-segments in the transmission path.

[34] The consumer information business is a multi-billion dollar a year business, centered around credit bureaus such as Equifax, TRW, and Trans Union. It has been estimated that the average American is on 100 mailing lists and 50 databases. Fisher, Susan E., *What do computers know about you? Personal information too readily available*, PC Week, Information Access Company; Vol. 8; No. 6; Pg. 156, February 11, 1991

In America individuals, firms, and governments have a substantial right to collect and redistribute personal and financial data about individuals. One could conceive of a market transaction system by which consumers offer companies payments to delete such information or refrain from distributing it. But could such a system work? In any transaction, both parties remain with information about it. The problem is not usually that a party saves that information, but rather that it disseminates it to others. The regulatory approach restricts some of these transfers. Could a market work instead?

The answer is usually "no" today. And only "maybe", in the future.

The reason for this can be found in the logic of reselling information. In many cases the holder of information about a second party could share that information with a third party at a higher price than the resulting reduction in value to him. Take, for example, a piece of credit history information on individual A that is worth $5 to B so long as B retains the information exclusively. If B distributes the data to another party, C, the direct value of the data to B may not be diminished at all, or perhaps drop a bit to, say, $4. (It is one of the peculiar economic properties of information that it can usually be shared without any or only little loss of usefulness to its holder. The exceptions are business and trade secrets.) Suppose C, too, is willing to pay up to $4 for the same information, because it is of similar usefulness to him. Then the total value to B of not destroying the information is $8. And why stop at two beneficiaries? B could resell the information also to D, E, etc. So could C. In each case, the reduction in value of the information to one of its holders may be less than what another party will gain by obtaining it.

Hence the information will spread. Accordingly, the subject of the information, individual A, might have to expend a significant amount of money to prevent B from spreading the information. If it is of use to a hundred firms, each valuing it at say $4, it would take a $396 "bribe" for A to keep B from reselling it. If a resale of information is possible, B and C would market the same information about A, and they will drive down its price to the marginal costs of distribution. In that case, the information would spread greatly, but it would also be cheaper for A to bribe B at the outset. Yet all B would have to do is to contractually assure, in the transaction with C, against resale.

A could attempt to stop personal data from getting released to a third party by preferring to do business only with firms that agree to destroy such data. But companies would charge customers higher prices to compensate for the lost information resale. Furthermore, once many

companies start refusing to sell information, each will have less information than before and hence a greater business risk, which would be reflected in the price. In effect, firms would charge for withholding the information through their product or service prices.

At the same time, any effort by A to pay a high price to B for non-revelation will likely raise the value of the information to B, C, etc -- what is A trying to hide, anyway? And, wouldn't A have to pay a similar bribe to C, too, if the information reaches it? Thus, the more important the information is to more parties, the less affordable is a market transaction to purchase privacy. Only where information is of little use to others, or only to a very few, are privacy transactions likely.

An example is a video store. Such a business could advertise that its policy is to guarantee privacy. It would gain customers, and since the information is not usually very important to many other parties, it would lose little (the interest in political figures and celebrities is an exception). In contrast, it is hard to imagine a credit card company willing to be compensated for non-disclosure to other credit-extending firms. The value of preventing credit-fraud is so great to so many firms that any payment to undermine the reporting system would have to be quite high. Yet video-store disclosure is prohibited by law, while credit-reporting is legal. The reason is probably that the loss of information-value was low for video-viewing and nobody therefore mounted a fight against such legislation, while politicians running for election were particularly sensitive about the issue.

Even if A could pay B to withhold the information, it may not be possible in practical terms. One of the characteristics of information is that its exclusivity is almost impossible to acquire once multiple parties have access to it.

Any negotiating approach will only work for transactions between individuals and businesses. If the information is obtained by government, fewer market-based incentive exists to prevent transfer of the data. This is one reason why government agencies are becoming so active in selling information to others. They have little to lose. Where else could one go to get a driver's license?[35]

---

[35] Additionally, data bank activities include several negative externalities, Rothfeder, Jefferey, *Privacy for Sale, How Computerization Has Made Everyone's Private Life an Open Secret,* Simon & Schuster, New York, 1992. For example, incorrect information contained in data banks. For the database providers, such inaccuracies, while bothersome and somewhat reducing the database value, may not justify the cost of attaining great accuracy. Yet for the data subject, the cost of an inaccuracy can be very high. Thus some transactions of data transfer between two parties take place more often than is truly efficient, taking all costs and benefits into account.

Currently, there is a right to collect, distribute and utilize personal data. What then if the rights were reversed and one would have to get a person's permission before retaining, transferring or utilizing personal data about him? If the information is of value to a bank and other credit institutions, they would acquire it by compensating the customer. Given the collective value of the information, such transaction would be likely. Hence, the information would be circulating. Consumer would be richer than before, but the information would be, in effect, still in the public domain.[36]

In conclusion, for personal data banks containing information about individuals, market transactions are either unlikely where the information is of use to many others, or it will be acquired by them. In either case the personal information, if valuable, becomes public information. For the future, one possibility that may help alleviate this problem is the emergence of encryptions.

D. Encryption

For markets in personal information to exist, it is necessary to protect that information from appropriation by others.

With digital technology, methods of protecting information with encryption have become powerful and convenient. Encryption goes back for thousands of years. It emerged primarily for the first electronic computers being the impetus as part of national security work, and spread to civilian computer applications. Encryption became popular with the release of the Data Encryption Standard (DES) to the public in 1977. DES is a 56 bit single key algorithm. To send a message to B using DES, A needs to define a key that will be used by the encrypting algorithm. In order to retrieve the message, B needs to give the decrypting algorithm the exact same key that A used to encrypt it. This leaves open the risk that the key is intercepted, and anyone knowing the key can decrypt the transaction.

Dual key systems solved this problem. In this system, anyone who want to receive a message has a "public" key. If A wants to send information to B in a secure way, he can encrypt it using B's public key. But the encrypted message can be decrypted only by using B's

---

[36] One obstacle is that consumers will have to police companies to make certain that they do not utilize information without first making compensation. This difficulty could be dealt with the assistance of a service provider who would run "key word" searches to determine if a person's name and personal data are utilized for any uncompensated purpose. This, however, would also raise a new type of privacy concerns.

"private" key. Thus, there is never a need for the risk-laden transmission of private keys.

Dual-key encryption software has appeared with the spread of the Internet : Pretty Good Privacy (PGP) employs dual key cryptography and is distributed free of charge for private use. Business users pay. Privacy Enhanced Mail (PEM) uses DES encryption along with a dual key algorithm to secure mail transmission.

According to International Resource Development, the U.S. data encryption market has have grown from $384 million in 1991 to an estimated $946 million in 1996.[37]

Where information is protected by encryption it is more marketable. Ironically, the U.S government, for reasons of law enforcement and national security, has opposed easy and fully secure encryption, thus reducing the ability of individuals to control access to their information, to establish property rights, and to create the foundation for markets.

Present encryption, however, does not solve the problem of *resale* of information to a third party C, once decrypted by the second party B. Solving that problem in the future would be a god-sent to every owner of information and copyright, but it is hard to conceive how it might be done securely. After all, a buyer of information cannot be stopped from memorizing and or photographing the de-crypted information on his screen and then reselling it.

Even so, giving A protection vis-a-vis B already goes a long way. It permits, for example for property rights in information about transactions between A and B to be held *jointly*. Both A and B hold keys to it, and therefore need each other's permission for their release. This would enable, for example A (a consumer) to require compensation from B (a credit card company) for releasing transaction information. It is true that B could copy information once it accessed it for one purpose, in other ways that were not authorized. But to do this in a systematic way to thousands of customers would be a foolish business practice.

The dual-key systems would permit also individuals to sell information about themselves directly, instead of letting various market researchers and credit checkers snoop in their demographics, personal history, and garbage cans. Individuals could keep a homepage with information about themselves. Anyone desiring that information could access this information through the payment of a charge. Individuals would define a set of access rights: their doctor only would be allowed to view medical records. Other categories of information would have free

---

[37] Hoffman, Lance J., Ali, Faraz A., Heckler, Steven L., "Cryptography Policy," *Communications of the ACM*, September 1994, Vol.37, No. 9, p. 109.

access, while others would be costly. Presumably, the more valuable information is to the buyer, and the more negative it is to the seller, the higher the price. Some information would be priced too high for voluntary exchange. This system would also allow an individual to keep track of who asked for the information. And, the reselling of the information would be authorized only by agreement of both key holders.

VI. SELLING THE RIGHT OF PRIVACY?

So far we have analyzed the role of markets in the provision of privacy in a largely pragmatic way -- will it work? Yes, in some cases. No, in other cases. But at least as important is the normative question -- *should* privacy be part of a market? While the market approach could be in many instances efficient on economic grounds and would differentiate according to needs, efficiency is not the only value to be concerned about. Just as there are economic trade-offs, so are there non-economic ones.

A distribution of privacy rights on a free-market basis would provide no protection for citizens against encroachment by the *state*. The only effective limits on government are those established through constitutional and statutory means. Therefore there would have to be two types of privacy rules, one for transactions among private parties, the other for transactions between private parties and the state. The former would be left, in part, to the market to allocate, the later would involve a constitutionally protected right. Yet the question may be asked whether such a bifurcation in the treatment of the most mobile of resources -- information -- is sustainable and practical.

Perhaps the most prevalent argument against markets in privacy is that efficiency is not the only societal goal. Thus, some resources, such as privacy allocations, might be in the category of inalienable rights that are protected from encroachment and "commodification" by the market system.

This position leads to several responses to the notion of transaction-generated privacy:

1. Privacy is a basic human right, and not subject to exchange transactions.
2. Consumers cannot correctly assess the market value of giving up personal information.
3. A transaction system in privacy will disproportionally burden the poor.

To state that privacy is a basic human right is a noble sentiment with which I am in

accord, but it does not follow that privacy therefore is outside the mechanism of transactions. As mentioned, a right is merely an initial allocation. It may be acquired without a charge and be universally distributed regardless of wealth, but it is in the nature of humans to have varying preferences and needs, and to exchange what they have for what they want. Thus, whether we like it or not, people continuously trade in rights. In doing so they exercise a fundamental right, the right of free choice.

In most cases, a person does not so much transfer his right to another but chooses not to exercise it, in return for some other benefit. An accused has the right to a jury trial, but he can waive it for the promise of a lenient sentence. A person has the freedom of his religion, but may reconsider in order to make his spouse's parents happy. One can be paid to assemble or not to assemble, to forgo bearing arms, travel, petition, or speak. Voluntary temporary servitude in exchange for oceanic passage has peopled early America. Students have the right to read faculty letters of recommendation written in their behalf, but they usually waive that right in return for letters they hope will have greater credibility.[38]

These departures from textbook civics are socially undesirable if the rights in question were given up under some form of duress, for example if in a single-employer town workers must agree not to assemble as a condition of employment. But when an informed, lucid, sober, and solvent citizen makes a choice freely, the objections are much harder to make. They then boil down to a transaction being against public policy, often because it affects others outside the transactions (i.e. "negative externalities"). To make these transactions illegal, however, does not stop many of them, if there are willing buyers and sellers, but it makes them more difficult and hence costly. The extent of the success of such a ban depends, among other factors, on the ability of the state to insert itself into the transaction. In the case of privacy, which by its nature is an interactive use of information, such insertion is difficult. All it usually takes is to make the information transaction consensual. And if it becomes illegal to offer compensation to obtain consent, one can expect imaginative schemes to circumvent such a prohibition. After all, we now have over 3.0 lawyers per thousand population, up from 1.3 in 1970.[39] Indeed, the success

---

[38] Votes are not formally for sale, but candidates and parties vie with each other in making promises to benefit voters and interest groups, and if they renege on their part of the bargain, they may be punished at the next election. That is the theory.

[39] Epstein, Richard, *Simple Rules for a Complex World*. Harvard University Press. Cambridge Press, 1995, p.3.

of government enforcement would then depend on intrusive actions by the state into private transactions. As important as privacy is, it will not necessarily override other values, such as free choice, the right to know, and the right to be left alone.

A second objection is that consumers have asymmetric knowledge relative to businesses about the value of their personal information, and that they consequently would be exploited (Gandy, 1996). The holders of this view discount the information-revealing process of competition. They must assume chronic oligopolistic behavior by business firms. Because such asymmetry in information would exted to all other dimensions of transactions as well, this view, to be consistent must be deeply skeptical of informed consent in consumer transactions generally.

The third objection to transactions in privacy is that they disproportionally harm the poor. Here, it is believed that it is especially those suffering from financial pressures and ignorance will sell their privacy rights to rich individuals and institutions. It is, of course, true that a poor person's priorities may often not include privacy protection. (In other cases, however, the opposite may hold and poor people need privacy more than those who can afford to create protective physical and organizational walls for themselves.) On the other hand, the same poverty condition may also make a poor person an unattractive target for a commercial intrusion. Telemarketers will prefer to make a pitch to individuals who can afford their products. The poor are best helped by money; to micromanage their condition through restricting their right to transact may well end up a patronizing social policy and inefficient economic policy. This leads to a conclusion that privacy, being a broad umbrella for a variety of issues, cannot be dealt with in a single fashion. Where transactions are not forthcoming, indicating a structural market failure, (perhaps due to monopoly or high transaction costs) , or where negative externalities are large, regulations can be appropriate that reflect the policy preferences of the community for privacy and as well as for other values. But it must be recognized that, given the initial logic of the exchange transactions, they will find a way to assert themselves in other ways, thus undercutting the actual effect of the restriction and leaving them more in the nature of a societal statement of intent.

But where the level of privacy protection can be readily set by free exchanges among individuals there is no reason for state intervention, and one should instead strive to eliminate constraints against such transactions.

Those who believe that the market approach to privacy protection is overly generous to

business violators of personal privacy might fiind themselves pleasantly surprised because the tools of access control will have shifted the balance of power to individuals and to the protection of privacy. Indeed, it will be the business users of personal information who will end up objecting to transactions. They are, of course, worried that while they (together with politicians and parties) have today relatively free access to individuals or to data about them, a system where they might have to pay compensation in return for consent might become expensive. They are correct, but what can they do about it? Access to an individual, even if sanctioned by law, will require the latter's cooperation. Right now, individuals do not yet have effective means to make those desiring personal information compensate them. But the tools to change this, such as encryption or caller identification, are here or near. Soon, equipment makers and communications service providers will enable consumers to conveniently sell access. And when this happens, those marketers who claim to live by the free market will also have to play (and pay) by its rules.