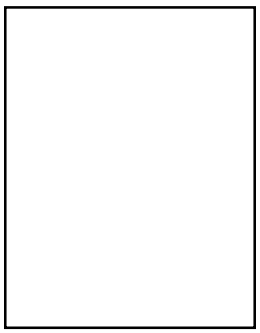
Privacy in Telecommunications: Markets, Rights, and Regulations

Part I: What is Privacy?

Eli M. Noam, Ph.D.



Dr. Eli M. Noam is Professor of Finance and Economics at Columbia University Graduate School of Business and Director of the Columbia Institute of Tele-Information. He has also served as Public Service Commissioner engaged in the telecommunications and energy regulation of New York State. His publications include over a dozen books and about 200 articles on domestic and international telecommunications, television, information, and regulation subjects. He served as a board member for the federal government's FTS-2000 telephone network of the IRS' computer modernization project and of the National Computer Lab.

Professor Noam received an A.B., a Ph.D. in economics, and a J.D. law degree from Harvard University.

This article is reprinted with permission from a monograph written by Dr. Noam and edited by Rev. Everett C. Parker of the United Church of Christ. Given the space constraints of NTQ*, we will publish the monograph in its entirety over the next three quarters. This first installment discusses what privacy is and when it should be protected. The second installment to be published in the 3Q95 issue discusses statutory and regulatory approaches to privacy problems. The final installment analyzes the process of private bargaining over privacy. —Ed.*

The technologies of the information age have brought both conveniences and conundrums. Among them is the jeopardy to privacy. It has been that way from the beginning of electronic media. In the earliest years of telecommunications, manual operators, party lines, and the absence of a warrant requirement for wiretapping created privacy problems.[1] The first American patent for a voice scrambling device was issued only five years after the invention of the telephone. There is evidence of wiretaps by private parties as well as governments fewer than 10 years after the introduction of the telephone.[2]

The New York Police Department has listened in on telephones since at least 1895. In 1916, this led to a public controversy about eavesdropping on a Catholic priest and on a law firm involved with competitors to J. P. Morgan & Co. for World War I munitions contracts.[3] Spurred by such disputes, relatively strong drives for telecommunications privacy developed over time, and were buttressed by legal protection.

Today, a new generation of communications privacy problems has emerged. There are several reasons for this development. Among them:

- An increasing number of transactions are conducted electronically. For example, in 1962, the U.S. federal government had 1,030 computer central processing units; in 1982, 18,747; and in 1985, over 100,000.[4] Today, the number is beyond counting.
- It has become easier and cheaper to collect, store, access, match, and redistribute information about transactions and individuals. In the past 20 years, the cost of access to a name on a computer-based

1070-3683/95/$3

mailing list has come down to about one-thousandth of its earlier cost.
- Transmission conduits increasingly include unsecured portions, for example, in mobile communications. This is offset, to some extent, by the proliferation of fiber transmission, which is harder to intercept than electronic transmission or focused microwave lines. However, a transmission path is only as secure as its weakest link, and any mobile segment is inherently insecure.
- 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.

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

- Intrusive telemarketing access to the home.
- Data collection about transactions using telecommunications, and the generation of personal profiles.
- The ability to determine an incoming caller's phone number and the use of such information in generating mailing lists.
- The monitoring of wireless mobile communications.
- Employers' monitoring of their employees.
- The ability of governments to control the encryption of communications.

And there is much more coming our way. For example, tiny mobile communication transceivers, together with the "portability" of access numbers, will continually connect telephone subscribers to the network. Their whereabouts, their comings and goings, and those of other telephone subscribers in the same location could be continuously ascertained.

Given that privacy is important to so many people, and given that information technology keeps raising new questions, what should be 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 telecommunications field, given its history around the world as a state-controlled monopoly. The value systems of telecommunications have been those of engineering, bureaucracy, and law, each reinforcing the view that there are "correct" solutions and "proper" procedures. Privacy problems in telecommunications are viewed largely as an issue of state-allocated rights—and the strategy question is how to create such rights in the political, regulatory, and legal sphere. Such a view has much to commend itself, but it is also deficient in that it 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.

Current practice also often fails to distinguish between political rights that protect the individual from the state, and those rights that define the relation of private parties with each other.

Privacy among individuals is an interaction in which the rights of different parties collide. **A** has a certain preference about 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 recent 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 conventional "consumers versus business" or "citizens versus the state" analyses suggest. In this case, different parties have different preferences on "information permeability" and need a way to synchronize these preferences not to be at tension with each other. This would suggest that interactive negotiation over privacy would have a place in establishing and protecting privacy, either as a substitute or a complement to direct regulation. Thus, potential policy practices may range from strict regulatory controls to bargained-for transactions.

The suggestion that open markets may be capable of dealing with privacy dilemmas may be taken by many as counter-intuitive. Personal privacy, they would say, is infringed upon by entrepreneurs, not protected by them. Only the state can protect the public's privacy needs. Thus, we balk at the idea that market transactions can also provide personal privacy.

While this article will not suggest that markets can provide a solution to every privacy issue, and certainly not to those where the state is the intrusive party, it will argue that a bargaining mechanism can be utilized much more than in the past.

Therefore, this article will analyze the potential for market-based responses to the privacy threats that are

emerging with the rapid evolution of telecommunications and diverse network structure. We will attempt to identify when exchange transactions can and cannot be relied upon to resolve various privacy issues, where their functioning requires initial government action such as the creation of rights, and where a regulatory response is necessary. We will discuss an institutional means to weigh the approaches to protection. We will also discuss whether markets should be involved at all in privacy issues.

Arguments Against Privacy

In the information sector, individual privacy consists of two distinguishable but related aspects:

(a) The protection against intrusion by unwanted information. This is sometimes termed "the right to be left alone,"[5] 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 to proprietary protection accorded to other forms of information through copyright laws,[6] and to security of information about oneself from tampering by others.[7]

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

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

"Privacy Protects Antisocial 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 traditionalist societies do not value a private sphere, since they often subordinate individuals to the demands of rulers or societal groups.[8] The recognition of a private sphere is one of the touchstones of a civilized and free society.[9]

"Privacy is Costly to the Economy"

Privacy protection raises 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, risk increases, 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 since much of it has no protection through property rights, it must be protected through confidentiality or secrecy.[10] To permit its easy breach would lead to a lesser production of such information.[11]

Because of this possibility, one leading legal scholar, Professor (now Judge) Richard Posner, has advocated that privacy in business communications deserves greater protection than privacy of personal information. Posner argues that the former is necessary for "the entrepreneur to appropriate the social benefits he creates," while privacy in personal information is usually desired only to "conceal discreditable facts."[12]

Taking a different approach, it has been shown in a theorem by Kent Greenawalt and Eli Noam that, under normal conditions, information of value, once released to one person (or to very few persons at most) will spread—in the absence of collusion—to all participants.[13] Hence, the absence of privacy protection to stem outflow of information will lead to suboptimal production of such information.

Similarly, anonymity may increase economic risk-taking. In that sense, privacy protection acts as a spur to investment, just as the protection of limited liability helps corporate investments. Unfortunately, illegal activities are also made easier.

The loss of privacy also 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 is the enormous complexity involved in assuring the secure transfer of information and the restriction of access to it. The use of disguises and segmentation is inefficient, because any coding system and limited

access is costly in terms of time, effort, and transmission capacity, and leads to increased errors in communication and interpretation.

Partly in response to economic and social needs, many transactions have been accorded special informational protection known as "privileges," e.g., between husband-wife, attorney-client, patient-doctor, citizen-census taker, penitent-clergy. The theory is that the protection of information in important relationships is socially or economically more significant than the ensuing inconvenience to others. For example, the patient-doctor privilege increases the overall health of the community members by permitting an uninhibited exchange of information,[14] and the attorney-client privilege ensures that the justice system is protecting the rights of defendants by permitting them to place full confidence in the attorney.

"There is no Demand for Privacy"

This objection views privacy as an elite concern. But, to the contrary, attention to privacy is widely shared. For example, according to information from the New York Telephone Company, in 1989, 34% of all Manhattan residential households and 24% of all New York State residential households had unpublished telephone numbers at subscribers' requests. Most policemen, doctors, or judges, to name a few professions, have unlisted numbers. On the West Coast, the spread of "unlisting" is increasing further, reaching 55% in California![15] A 1988 Massachusetts survey of the main consumer complaints found them topped by telemarketing and promotional mailings.[16] And when Pacific Bell planned in 1986 to sell subscribers' information such as new phone orders, more than 75,000 complaints were received, and the company backed off.[17]

Countervailing Interests to Privacy Protection

It is counter-productive to the protection of privacy to engage in single-issue advocacy. There are other legitimate societal interests that must be balanced against privacy. Some have already been touched upon. Others include:

(1) *Freedom of the press, freedom of information, access to government records.* An individual's privacy sphere may conflict with the desire of the press to publish details about individuals, and with the public's right to know.[18]

(2) *Law enforcement and administrative efficiency.* Surveillance, electronic data collection, and computer matching can be powerful tools to combat criminal or terrorist activities, and can counteract the increasing financial and technological sophistication of offenders.

(3) *Consumer protection.* The itemized billing of long-distance calls is helpful to telephone users.

(4) *Economic freedom.* Any protection that is not based on voluntary exchange transactions may reduce the ability to offer or procure certain services and equipment features.

(5) *Reduction of business risk.* Vendors or credit companies would assume less risk with greater access to records about customers, employees, and suppliers, and obtain more immediate feedback to their marketing actions. The result could be better service, reduced losses, and lower prices.

(6) *Increase in the cost of information.* Privacy protection may raise the cost of information search, storage, and transmission, making information-based transactions more expensive.

(7) *Efficiency and innovation.* The cost of providing privacy protection may discourage or delay new services or make them more expensive. Technology retardation may result from protection of privacy.

(8) *Operational ease.* Communications operations may be affected by privacy protection. The concept of a network is based on the sharing of resources, including information. Coordinating the interaction of multiple networks may be made more difficult by imposing privacy protection that limits such sharing, e.g., of computer database connections.

(9) *Personal mobility.* Communications technologies present opportunities for great personal mobility (for example, through cellular telephones, or by calls that automatically track individuals as they travel from one location to another), which could be limited if the database intelligence needed for these systems were constrained.

(10) *Conflicting privacy interests.* Privacies of several parties to a communication may clash. For example, a called party's desire to be "left alone" and be protected from harassment may conflict with the calling party's desire for anonymity.

(11) *Affordable basic telephone rates.* Revenue from new services may help keep basic telephone rates low. If such services are restrained or delayed by

privacy protection measures, revenues that could contribute toward basic rates may not be generated.

(12) *National uniformity*. If state-specific privacy provisions are adopted, the ability to provide nationwide services may be impaired.

(13) *Open networks*. The opening of networks and their unbundling provides for equal treatment of all, such as enhanced service providers competing with local exchange companies.[19] To achieve a "level playing field," such competitors want to receive customer information that is available to the telephone company.

Technology's Threat to Privacy

What are some of the actual or potential threats to privacy of new communication and information technology? Obviously, some are unknown. Who would have thought 20 years ago that teenagers would send out destructive virus programs attacking corporate data banks around the world? But some privacy jeopardies are known, and others can reasonably be expected.

Wireless Transmission

(1) *Cellular and micro-cellular telephony*. Monitoring of conversations is possible, with the stationary party often unaware that its call is being transmitted over an open over-the-air segment to the mobile receiver. It is also possible to track a subscriber's travel path by using data on which cells were activated.

(2) *Cordless telephones*. Monitoring of conversations by a nearby radio receiver is possible, as is the unauthorized use of a subscriber's telephone number by someone accessing the line with a cordless telephone operating at the same frequency.

(3) *CT-2*. These cordless *public* phones, introduced in the United Kingdom under the designation of "Telepoint," permit surveillance by a nearby monitor of calls at any such public phone location.

(4) *Pagers and beepers*. The monitoring of caller locations and the collection of information about the message volume of a particular called party are possible.

(5) *Satellite and terrestrial microwave transmission*. This generally permits easier monitoring than do wirelines.

Switch-based Services

(6) *Voice mail* creates the potential for unauthorized access to messages by third parties, permits the unwanted retention of old messages, and raises access rights by the employer.

(7) *Remote routing of calls* can be accomplished by an unauthorized person, or a non-consenting party may have its calls rerouted.

(8) *Bridge or conference calls* allow silent listening-in by unannounced parties.

(9) *Information safety deposit boxes* may allow unauthorized access to a wide variety of personal information.

Terminal Equipment

(10) *Facsimile machines* allow unsolicited messages to enter the premises of the called party (and at the latter's expense of paper).

(11) *Automatic dialers* generate unsolicited and intrusive "junk" calls that at times cannot be disconnected.

(12) *Answering machines* may present the opportunity for access to messages by unauthorized parties. Routine taping of incoming calls is also possible.

(13) *Speakerphones* can leave the caller unaware, in the absence of a signal, that there is an audience to what is believed to be a private conversation.[20]

(14) *Picturephones* make it possible for the receiving party to sell a resulting video recording of the conversation.

(15) *Remote metering and telemetry* can be intrusive (warrantless entry).

(16) *Passive monitoring devices* allow information gathering, such as voice stress metering, over a telephone without notice to the tested individual.

Networks and Transmission

(17) *Broadband networks*, as now planned, include a bus-type architecture as a technical solution to local fiber distribution. This creates, in effect, a "party line" with the potential for diverting signals by unauthorized parties in the distribution system.

(18) *Packet and asynchronous transmission* (ATM) presents the possibility of a diversion of packets, similar to the broadband network problem. There can be identification of sender and recipient of packets by other parties with access to the header part of the packet.
(19) *Interactive or addressable video broadband services* could permit billing records that contain viewing information like that outlawed in the "Bork bill" for video stores.[21]
(20) In *Narrowband ISDN*, the use of the "D-channel" could provide transaction and signaling information to unauthorized parties.
(21) *Intra-organizational private networks* possess the capability to track employee calls, and their physical presence, location, and productivity (e.g., the number of key-strokes, call handling time, total time on phone). They permit eavesdropping on conversations without notification to employees or to non-employee third parties.
(22) Through *call forwarding*, re-routing of one's calls to a non-consenting third party can intrude into that party's privacy. Where remote re-routing is possible, an authorized access can divert telephone calls and lead to their interception.

Information Services

(23) Use of *electronic mail/bulletin boards* by fringe groups has led to Congressional bills requiring the monitoring of bulletin boards by the computer systems operators.
(24) *Dial-it services* facilitate the creation of lists of their users.
(25) *Videotex and audiotex* allow records of pages or programs used by a subscriber to be collated to create a profile of business transactions and personal habits.
(26) *Videotex gateways* could enable carriers to monitor information pages and transactions used by subscribers.
(27) *Data banks* permit recording of personal data, and access to them by third parties, including unauthorized ones; permit matching of different records to establish profiles; and could be altered surreptitiously by outsiders, including through the use of a "virus" program.[22]
(28) *Personal information services* with name-based data may be abused by unauthorized entry of names. (In New York, names in computer-based dating services were disclosed in an unauthorized fashion.)

New Information Services

(29) *Remote accessing to directory information.* AT&T plans to offer users nationwide (and later international) access to local telephone listings.
(30) *Central-office-based information safe deposits.* Telephone companies are considering offering customers electronic storage space for information such as medical and financial records. Potential unauthorized access raises security and privacy concerns.

Signaling and Network Management Information

(31) *Common Channel Signaling System 7.* This signaling system can provide transaction information about calling and called parties, with identification of name, address, and possibly other associated data.
(32) *Automatic Number Identification* (ANI)[23] allows customer identification of the calling party's number. This creates a powerful tool for telecommunications-based transactions. It permits the matching by users of calling party's other data records, reveals a caller's unlisted number to a callee, and permits selective treatment and service grading of incoming calls according to their geographical origin. It may chill certain calls, for example, to counseling services or to journalists. It is often asserted that ANI identification is analogous to asking for the name of a visitor before opening the door. This analogy is correct, but incomplete. An equally valid analogy would be to require buyers who enter a store or movie theater to fully identify themselves, and for such information to be kept on file as well as freely sold to others.
(33) *800 and 900 numbers* provide information about incoming callers to subscribers.

Locational Monitoring

(34) *Number portability* permits real-time identification of a subscriber's location.
(35) *Navigational systems/"trip-master" systems and "intelligent highways"* permit tracking of vehicle location and operation by driver, including speed, shifting points, idle time, etc.

(36) *Smart identification badges* permit monitoring of employees, and tracking their comings and goings, meetings with others, etc.
(37) *Passive beeper bracelets* permit monitoring of an individual's location through phone-based equipment. They are now used for house arrest as an alternative to incarceration, but could be used for employment supervision and for social service cases.

TRANSACTION INFORMATION

(38) *Itemized billing* enables unauthorized persons to gain access to the details of toll calls.[24]
(39) *Hotel customer telephone bills* are largely unprotected from inspection by hotel personnel and even by other guests.
(40) *General telephone service*. The nature and details of telephone subscriptions can be easily ascertained and modified by unauthorized parties, with no identification required at present.
(41) *Customer proprietary network information* (CPNI). User transactions over the telephone provide marketing data for carriers, which could also be sold to third parties.
(42) *Smart cards or credit card-like memory devices*, used for general-purpose charging, create a record of a consumption, telephone usage, or payment. A personal history could be established that would be available to a vendor (including a telecommunications carrier) at the next point-of-sale. If smart cards are used for government benefits, such as food stamps, they could monitor recipients' usage and movements. ntq

For a complete bibliography, please contact Technology Futures, Inc. at (800) 835-3887 or (512) 258-8898. This article was reprinted with permission of the Office of Communications, United Church of Christ, 200 Prospect Avenue, Cleveland, Ohio 44115-1100; (216) 736-2222. Reprints are available from the United Church of Christ for $5.00 per copy.—Ed.

---

[1] *Olmstead v. United States*, 227 U.S. 438, at 478 (1927).
[2] A. F. Westin, *Privacy and Freedom* (New York: Athenaeum, 1967).
[3] D. J. Seipp, *The Right to Privacy in American History* (Cambridge, MA: Harvard Program on Information Resources Policy, 1978), p. 78-3.
[4] D. E. Linowes, *Privacy in America: Is Your Private Life in the Public Eye?* (Chicago, IL: University of Illinois Press, 1989).
[5] *Olmstead v. United States*, 227 U.S. 438, at 478 (1927).
[6] The common-law copyright protection provided primarily that if one had not published information in one's own possession, no one else could take and publish it. This was similar to a trespass and conversion action (see S. D. Warren and L. D. Brandeis, "The Right to Privacy," *Harvard Law Review*, Vol. 4, No. 193 [1890]).
[7] Westin, *Privacy and Freedom*.
[8] On the history of privacy, see R. A. Posner, *The Economics of Justice* (Cambridge, MA: Harvard University Press, 1981); G. Simmel, "The Sociology of Secrecy and of Secret Societies," *American Journal of Society*, Vol. 11, No. 441 (1906); A. F. Westin, *Privacy in Western Society: From the Age of Pericles to the American Republic*, Report to the Association of the Bar of the City of New York, Special Committee on Science and Law (February 15, 1965); and Seipp, *The Right to Privacy in American History*. In the United States, privacy is often (but not always) a nonpartisan issue. The Privacy Act of 1974 was cosponsored by Senators Edward Kennedy and Barry Goldwater.
[9] 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."
[10] In the extreme, private information is so valuable to an individual as to make him a target for blackmail. See also J. Brown, Jr. and K. Gordon, *Economics and Telecommunications Privacy: Framework for Analysis* (FCC, OPP, Working Paper, 1980) for an economic perspective from the FCC.
[11] Posner, *The Economics of Justice*, pp. 231-347.
[12] *Ibid*., p. 248.
[13] K. Greenawalt and E. M. Noam, "Confidentiality Claims of Business Organizations," in H. J. Goldschmid, ed., *Business Disclosure: Government's Need to Know* (New York: Columbia University Press, 1980).
[14] Posner, *The Economics of Justice*, p. 297.
[15] For public views on privacy, see especially the Louis Harris/Alan Westin surveys of 1990, 1991, and 1992. The newest data show 83% of Americans concerned about privacy, and 53% very concerned (*Harris-Equifax Consumer Privacy Survey 1992*, Louis Harris and Associates in association with Dr. Alan F. Westin, Columbia University, 1992).

Another indication is provided by a survey conducted by American Express among its cardholders. Ninety percent felt that mailing list practices were inadequately disclosed, 80% that information should not be given to a third party without permission, and more than 30% believed federal legislation was needed to restrict the use of lists ("Privacy Study Reveals Lack of Consumer Confidence," *Direct Marketing*, December 1988, p. 8). American Express makes extensive use of the data that it has accumulated on its cardholders. According to *Fortune*, the company computers "maintain and update weekly a profile of 450 attributes—such as age, sex, and purchasing patterns—on every cardholder" (J. P. Newpert, "American Express: Service that Sells," *Fortune*, Vol. 120, No. 12 [November 20, 1989], p. 82.)
[16] Marchocki, "Prize Letters, Phone Spiels Top List of Consumer Beefs," *The Boston Herald* (January 5, 1989):47.
[17] "Pac Bell Backs-Off Selling Lists," *Alameda Times Star* (April 16, 1986):16.
[18] See the 1989 U.S. Supreme Court decision in *B.J.F. v. The Florida Star* U.S. 109 S. Ct. 2603 (1989), in which the court declined to hold the press unreachable by actions against its truthful reporting of the public school record when it violated state protection of privacy.
[19] FCC rules in the Second Computer Inquiry require that local exchange carriers, when authorized by a subscriber, disclose all "Customer Proprietary Network Information" (CPNI). However, unlisted and unpublished telephone numbers may not be released.
[20] This happened to former President Bush, who began engaging in a confidential political chat while being overheard by an audience of hundreds.

[21] According to New York Attorney General Robert Abrams, "Interactive cable television could generate the single largest repository of personal data and information in the history of the world." See D. H. Flaherty, "The Need for an American Privacy Protection Commission," *Government Information Quarterly*, I (1984):235-238.

[22] Florida enacted in 1978 the first state computer crime law, establishing property rights in computer data and barring unauthorized access and alteration. Since then, most states have passed similar statutes. Increasingly, computer data, processing, and services have been accorded the status of property.

[23] Closely related to Caller ID. A comprehensive legal analysis of ANI issues is provided in G. C. Smith, "Caller Identification Technology and the Right to Informational Privacy," *UCLA Law Review*, Vol. 37, No. 145 (1989).

[24] Here is how the Watergate investigators, ferreting out the dirty tricks of others, contributed their own. In their own words, "Bernstein had several sources in the Bell System. He was always reluctant to use them to get information about calls because of the ethical questions involved in breaching the confidentiality of a person's telephone records.... Without dwelling on the problem, Bernstein called a telephone company source and asked for a list of Barker's calls." C. Bernstein and B. Woodward, *All the President's Men* (New York: Simon and Schuster, 1974), p. 35.