Privacy in Telecommunications: Markets, Rights, and Regulations

Part II: Policy Approaches

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. This second installment discusses statutory and regulatory approaches to privacy problems. The final installment, to be published next quarter, analyzes the process of private bargaining over privacy.—Ed.

As new technological options emerge, new opportunities are created along with new privacy problems. How can such problems be dealt with?

There have been two traditional policy approaches—centralized general protection and decentralized ad hoc protection. The first, followed primarily by Western European countries, is to pass comprehensive (omnibus) data protection laws and establish institutionalized boards which impose fairly rigorous and increasingly internationally-coordinated protection on information collection and data flows.[1] The second, followed by the United States, has been to deal with specific problems, one at a time, and with different approaches across the country.

Europe

In Europe, advances in data processing led in the 1970s to fears about the abuse of information storage. The ability of computers to hold vast amounts of information, to centralize data collection, and to retrieve and disseminate information rapidly had the potential to make computer technology an effective tool for government control and business power. Government investigations could rapidly correlate an individual's medical history, financial transactions, consumption patterns, travel information, reading habits, and more. In the process, a "1984"-like surveillance state would become possible. Fears were based on the technological notion of computers as vast centralized mainframes, a notion that 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, often electronically interconnected. This change has reduced the need for

1070-3683/95/$3

centralized storage and has shifted the problem of protecting individual privacy from one of data storage to one of data communication.

Protective legislation on electronic data collection and storage began in Europe with a law in the German State of Hesse (1970) and a national law in Sweden (1973). From there, legal action spread to most of Western Europe. Most countries adopted a uniform national law, with an independent specialized agency for enforcement and regulation, including registration or licensing of data files that include personal information, access and correction rights for individuals, limitations on use and disclosure, and a structure for the internal management of databases.[2]

Though the origin of concern over privacy was the potential 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 were typically less severe. 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, political terrorism by the so-called Baader-Meinhof group prompted the German police to institute a far-reaching 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 mostly stopped, many control mechanisms were not abandoned.

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 certain 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, 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.

In 1979, the Organization of Economic Cooperation and Development (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.[3]

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 achieved binding status after its ratification in 1985 by a majority of Council of Europe members. 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 quite 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. Theoretically, any country could restrict the flow of data to other countries by the simple device of raising the level of its own privacy protection.

Europe-wide efforts at ensuring privacy continued with a 1989 Council of Europe recommendation on protection of personal data used for employment purposes. Employers would now be required to consult with workers on collection and use of information, type of data stored, and access of outside groups to personal data.[4]

In 1990, the European Commission issued a draft directive that established basic telecommunications privacy rights for its 12 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.[5]

A revised draft was adopted in October 1992.[6] This EC directive:

- Prevented firms from keeping personal data or identification numbers without the prior approval of the individual in question.
- Allowed individuals to withdraw their consent at any time.
- Allowed civil damage claims in response to violations of privacy rules.
- Mandated that holders of data pay for security measures in order to bar unauthorized access.

- Prohibited the creation of electronic profiles of individuals utilizing data concerning their purchases or other actions.
- Barred transfers of data to non-EC member countries unless those countries had adequate data protection rules.[7]

This last requirement could have a significant impact on data protection outside the EC.

France

In 1974, a Commission on Information Policy and Civil Liberties was established within the French Ministry of Justice to regulate databases and protect individual privacy. Subsequently, in 1978, a law on Information Processing, Files, and Civil Liberties was passed that became effective two years later. It affects domestic databases and cross-border data flows. The law attempts to regulate biased and unfair methods of data collection and prohibits the recording of information on race, politics, religion, union membership, and so on. The law also acknowledges the individual's right of access to his or her information, imposes the obligation to correct false or incomplete information, and sets rules for its distribution.

All data systems must be registered with a special agency, the Commission National d'Informatique et Liberté (CNIL). CNIL is an independent administrative authority, similar in some ways to independent American regulatory commissions, and, as such, it is a rare body in French administration. A majority of its 17 members are chosen by judicial and parliamentary bodies. The commission can issue advisory opinions about data protection and data processing, which are then subject to judicial review by the higher administrative court, the Conseil d'Etat.

A database must be registered with CNIL so that the commission will be able to analyze it. A declaration must state the purpose of the database, the nature of the personal data collected, and its sources and destinations. By 1987, the number of registered data banks was already almost 50,000. Simplified procedures were available for routine personal data such as payroll, banking accounts, utility billings, and mailing lists.

The first case in which the CNIL recommended criminal prosecution involved the Swedish ball bearing company SKF and its French subsidiary. During a labor dispute, the company was occupied by trade unionists, who discovered a notebook with 600 entries on employment applications for the years 1971 through 1982. Although the data collections had been discontinued and were not electronic, the CNIL recommended prosecution. Another case that nearly led to criminal prosecution involved an infraction by the Communist trade union, CGT, which had used the automated payroll list of the electric and gas company for mailing election materials on the eve of workers' council elections.[8]

In 1986, CNIL required that caller identification services in a fiber optic trial had to include a blocking function. Call-by-call blocking was also included in the French ISDN service, Numeris, in 1988, and protections were instituted in the Mestel and Minicom electronic messaging services.[9]

In 1989, CNIL prevented the Fiat company in France from transferring personnel records to its home office in Italy until the automaker promised to continue applying French data protection requirements to the records once they arrived in Italy. One year later, CNIL began negotiating for protection of personnel records that IBM began moving between France and the United States.[10]

Data protection laws can have unintended and paradoxical results. The case of the French section of the human rights organization, Amnesty International, presents an example. The organization maintains personal records on "prisoners of conscience" and victims of capital punishment and torture. French data protection law prohibits personal files from including information on prison sentences or convictions. Such information, however, is fundamental to Amnesty International's activities. The law also prohibits the recording of information about the racial, political, philosophical, religious, or union affiliation of individuals, all of them essential to Amnesty's work. Under the French law, personal information collected can be transmitted only to the few countries that have similar data protection laws. But the essence of AI's work is to disseminate information widely about prisoners of conscience, and this would be impossible under a literal reading of the law.

In proposing a solution to these problems, a study group of international data protection commissioners recommended the creation of a committee to deal with "bona-fide international organizations pursuing humanitarian goals or defending human rights on an international basis, such as Amnesty International or the International Red Cross."[11] Yet, the selection and certification of such organizations enables government

authorities to certify some organizations as worthy and humanitarian and to deny such certification to others.

Germany

As mentioned, the State of Hesse enacted the first data protection law in 1970; in 1977, a national law was passed. The discussion of data privacy in Germany in the 1970s was colored by a fierce debate over how to contain a small group of political terrorists. Data issues were described as a choice between *Datanschutz* versus *Tatenschutz* (protection of data versus protection of criminal deeds). The political left was concerned with worker protection. Law-and-order conservatives, on the other hand, pushed for elaborate police matching of various databases. They also supported a national machine-readable personal identification card that would permit the tracking of individual movements. This led to an anti-data-collection backlash. The 1983 national census was opposed by many groups, and, in an important decision, the Federal Constitutional Court invalidated the holding of the national census on the novel grounds of "informational self-determination."

The use of data laws was not confined to matters of privacy. It also provided a lever in other disputes. A 1984 decision of the German High Court for Industrial Relations required the express consent of a workers' council for the introduction of a computer system that would be used to collect information on the performance of data technicians. The decisions gave unions some influence over computerization where it affects employment security.

In 1988, telecommunications regulations were instituted that provided some protection in calling identification and collection of subscriber data through ISDN. Data compiled on the national BtX videotex may be used only for billing and must be erased six months after collection.[12]

United Kingdom

Spurred by the Council of Europe's Convention on Data Protection which the United Kingdom signed in 1981, the United Kingdom passed the Data Protection Act of 1984. The act required the registration of data banks containing personal information and set other limitations on data collection and access.[13] The duties of the registrar include the establishment of public files of data users and data-processing bureaus. The registrar is also an ombudsman for complaints of data abuse and inaccessibility of records. Data subjects have the right to a copy of the data held about them, and if such information is not provided, they may complain to the registrar or to a court, both of which are empowered to order access. There is also the right to compensation for damages resulting from inadequate data security precautions. By 1990, approximately 153,000 companies and organizations with computerized lists of information on individuals had registered with the home office, representing 130,000 data users.[14]

In 1987, the United Kingdom also adopted a Model Code of Practice for telecommunications service operators that forbids unauthorized dissemination of data on users.

Other European Countries

It had been estimated that the average Swede was registered in about 150 governmental computer databases. This situation led to a special government commission and subsequent legislation in 1973, the first nationwide comprehensive privacy law anywhere. The law set up a Data Inspection Board for administration and policy development that had the right to grant permits for the maintenance of personal data files. A Data Policy Commission (subsequently the Information Policy Commission) was created to include representatives of federal agencies, political parties, the private sector, unions, employers, and local authorities.

Also in 1973, Denmark passed one of the most specific data transfer laws in Europe.[15] A Data Surveillance Authority must provide a license for any database to be collected or transmitted abroad. The authority also reviews proposals for international communication links to assure that data flows will not lower Denmark's standard of privacy protection.

Austrian legislation illustrates how data protection laws can potentially operate as a nontariff barrier. In most respects, Austrian privacy law is similar to other European nations, but to transmit personal data abroad, a license must be obtained from the Austrian Data Protection Commission. For countries where similar data protection standards exist, no license is required.[16]

Industrial Policy and Data Flows

It is impossible to discuss privacy and data protection without reference to their trade implications. In matters involving databases and processing, the United States long enjoyed a head start. In 1983, worldwide revenue from on-line data services was about $2

billion, of which the United States accounted for more than three-quarters.[17] In terms of database usage, the United States had an even greater lead. As with most information produced initially for a domestic market, the marginal cost for the export of databases is low. With an early start and a substantial domestic customer base, such databases provide tough competition for foreign systems.

Given this advantage, many American firms feared that data protection was, in part, economic protectionism in favor of local firms. A Canadian study found that, in 1985, the value for imported computing services was about $1.5 billion, which could fund an estimated 23,000 jobs in the Canadian data-processing industry. With greater frankness than is normally offered, the study conceded that issues of privacy and protectionism are closely intertwined. The report found that the major problem inherent in flows of Canadian data to the United States is "not one of privacy of Canadian data subjects being invaded by data about them being stored in the United States. It is rather that data processing in the communications business may be lost to Canadians as a result of this foreign flow."[18] To combat this trend, the Canadian Banking Act of 1980 required that customer data be processed and stored in Canada, thereby forcing U.S. banks to duplicate their hardware and software instead of relying on existing data-processing facilities across the border.

Among Third World countries, Brazil has been particularly active in data and telematics issues, and its policies, instituted during the military dictatorship, have received wide publicity. A license had to be obtained from the special Secretariat for Informatics before establishing international data links. Applications for foreign processing, software import, and database access were rejected if domestic capability existed. The rules were an attempt to strengthen and develop the domestic industry. The policy was strongly embraced by the Brazilian military dictatorship and its business and industrial allies, and it was admired around the world by many observers who would otherwise feel no kindness toward right-wing juntas.

United States

Legal and historical traditions, as well as economic motivations, explain the disparity between European and American conceptions of privacy protection.

In the United States, public concern about private data protection is less intense than it is in Europe. The United States has fewer centralized government operations and hence less centralized data generation on individuals than do most European countries. Furthermore, in the United States, certain forms of data surveillance of individuals do not exist: for example, residence registration or personal identity cards.

These conditions, coupled with a generally more pragmatic approach to legislation, a case-oriented judicial decision process, and the presence of regulatory agencies, have led to the tackling of specific data abuses when they became apparent, rather than through the use of comprehensive laws. There has been a less systematic approach than in Europe, and a variety of ad hoc federal and state legislation has been passed. Most of the statutes narrowly address particular industries (e.g., credit information bureaus) or the conduct of governmental agencies, or they deal with flagrant abuses such as computer break-ins.

Contrary to often-held views in other countries, many laws protecting data and privacy exist in the United States, and some of them are quite far-reaching. The so-called Buckley Amendment, for example, permits students a remarkable access to files that are kept on them by public or private schools and universities, even to letters of evaluation.[19] Similarly, the Freedom of Information Act gives the public extraordinary access to government documents, excluding only information that is deemed vital to national security, to the protection of confidential sources or the conduct of an ongoing criminal investigation, or that contains trade secrets of other firms.[20]

Nevertheless, U.S. privacy legislation remains considerably less strict than European law in the regulation of private databases. Also, the coverage of American government organizations by privacy law is not comprehensive. Although the Privacy Act of 1974 restricts collection and disclosure by the federal government, only a few states and local governments have passed similar fair information practices laws. The Privacy Act requires each federal government agency to issue a public notice on its recordkeeping activities. The Office of Management and Budget (OMB) coordinates the government's efforts in this area, and the protection covers all data files, electronic and conventional. The Privacy Act explicitly protects only U.S. citizens and permanent residents, thus excluding foreign nationals, whose personal data is "exported" from their national place of employment to U.S. headquarters. Furthermore, the United States has

no government agency specifically charged with data protection similar to the centralized data protection commissions or authorities established in European countries, although proposals have been advanced in Congress for creating such a body.

U.S. federal data protection requirements cover only consumer credit and reporting agencies and educational and financial institutions. Several states have similar requirements. Under the Fair Credit Reporting Act of 1970, individuals have the right to access their credit rating files, to have corrections inserted, and to know the sources of information in credit files.

Whereas the European approach is to protect data by making its collection and security requirements specific, in the United States, the abuse of information rather than its collection is the target, and harm must be shown for laws to be applied.[21]

Constitutional Principles

The term "privacy" does not appear in the U.S. Constitution. The concept of a "right of privacy" is based on judicial interpretation.

The relevant constitutional provisions are:

- First Amendment—freedom of speech and association, individual autonomy.
- Fourth Amendment—protection of persons and property against unreasonable search.
- Fifth Amendment—freedom from self-incrimination.
- "Penumbral or implied rights" referring to the foregoing amendments as well as the Third (protection of the home), Ninth (reserving right to the people), and Fourteenth (deprivation of liberty).[22]

The constitution protects individuals or businesses only against governmental action. Such protection does not normally exist with respect to actions by private parties, such as telecommunications carriers or others (although some constitutional protection may apply if "state action" is involved).

Even with respect to government, the evolution of a constitutional protection for privacy has been an uneven process, and its meaning is particularly hard-fought in the context of birth-control, abortion, and reproduction.

Until 1967, telephone wiretapping did not require a warrant. Today, beeper tracking devices on public streets are permissible without warrant, although a warrant is required if the car enters a private garage. Helicopter overflights by police of private property to take pictures are lawful. The court test has been users' expectations of privacy. But this permits a process of erosion: the more one gets used to monitoring of calls or transactions, the less legally protected they become. Establishing and protecting privacy expectations is hence a key issue in privacy protection.

The courts have protected the following privacy considerations, among others:

- Not to have information regarding prescription drugs or medical procedures maintained in an individually identifiable fashion.
- Not to have membership in (controversial) organizations disclosed.
- Protecting reputational dignity against libel and breach of privacy.

Federal constitutional provisions afford only limited privacy protection with respect to government actions, and hardly any with respect to private actions. A few state constitutions have explicit protection of privacy that provide more protection than the U.S. Constitution (examples are Alaska, California, and Florida). The omission of privacy provisions leaves most of the issues to statutory or regulatory treatment. For example, in 1976, the U.S. Supreme Court rejected a constitutional right to bank records privacy, whereupon Congress enacted the Right to Financial Privacy Act in 1978.

Federal statutes and cases deal primarily with electronic surveillance and privacy of information. Some of the most important include the following.

Electronic Surveillance

(1) The Communications Act (1934), Section 605, "No person not being authorized by the sender shall intercept any communication and divulge...the contents...."
(2) *Katz v. United States*, 389 U.S. 347 (1967), overruling *Olmstead v. United States*, 227 U.S. 438 (1927), established the necessity of warrant and criteria of probable cause for wiretap, discussing "reasonable expectation of privacy." (Similarly, *Berger v. New York* [1967] overturned the New York wiretap statute as not particular enough in describing time, place, or subject.)
(3) The Omnibus Crime Control Act (1968), Title III, prohibits law enforcement agencies from using electronic surveillance of conversations except

under court order. Title III permits wiretaps when: (a) a warrant has been issued, (b) when there is the consent of at least one party to the conversation, (c) in an emergency, (d) when the President ordered it to protect the national security, and (e) only when there are no less intrusive means. State laws on wiretapping are specifically allowed. A majority of the states by 1986 had such laws.[23]

(4) The Foreign Intelligence Surveillance Act (1978) regulates electronic surveillance of U.S. citizens, in the United States, for foreign intelligence and counter-intelligence purposes. *U.S. v. U.S. District Court*, 407 U.S. 297 (1972), held that warrant and probable cause requirements had to be satisfied even for national security wiretaps.

(5) The Privacy Protection Act (1980) prohibits the search of press offices and files if there is no one in a press room who is suspected of a crime.

(6) *U.S. v. Knotts*, 103 Supreme Court 1081 (1983), allows without warrant the tracking of movements of electronic beeper location devices over public streets. However, *U.S. v. Karo*, 104 Supreme Court 3296 (1984), holds that trailing a subject into a private house by use of an electronic location beeper does violate the Fourth Amendment. In general, the Supreme Court has been reluctant to extend the Fourth Amendment to new technological devices.

(7) The Electronic Communications Privacy Act (ECPA) (1986) holds that probable cause is needed to obtain an order to intercept non-aural communications. It overturns *Smith v. Maryland*, 442 U.S. 735 (1979), and determines that transactional data such as telephone toll records are private and subject to federal wiretap law restrictions.[24] Primary application is to electronic mail, cellular telephones, pagers, and data transmission. It also permits a person or entity providing public wire or electronic communications services to divulge the contents of the communication only to the intended recipient, and to no other person. (Telephone company identification devices such as pen registers and "trap-and-trace" devices are included in the prohibition, reversing a 1978 Supreme Court decision holding that pen registers are not covered by the Fourth Amendment.)

The ECPA also diminished privacy protection because it narrowed the Title III "content" definition to exclude information about "the existence of a communication" and the "identity of parties." Governmental access to this usage data requires a warrant but provides for no advance notice. Moreover, providers of communications services are permitted, without restriction, to reveal such usage to any non-government entity.[25] The act also broadened the grounds for government interception, and so in some ways liberalized government access.

The act protects a variety of radio signals from warrantless interception by governments or by private individuals. Radio signals include those which are encrypted, transmitted through a common carrier, or constitute a portion of a cellular phone call, but do not include cordless telephone conversations. Stiff penalties are specified if private interceptions are made for illegal commercial gain (e.g., insider trading). Lighter penalties are specified for idle eavesdroppers.

Information Privacy

(1) The Freedom of Information Act (1966) requires public access to federal records and documents, unless specifically exempt. Two such exemptions are for "personnel and medical files and similar files" and law-enforcement files "the disclosure of which would constitute a clearly unwarranted invasion of personal privacy." Also exempted are national security information, internal agency rules, exemptions from other statutes, business information, inter- and intra-agency memoranda, records of financial institutions, and oil well data.

(2) The Fair Credit Reporting Act (1970) requires credit agencies to allow consumers to review credit records. Credit agencies can only share credit information with authorized customers, but "authorized" means anyone with a "legitimate business need." A *Business Week* report showed there is little effort to screen "authorized customers."

(3) The Bank Secrecy Act (1970) allows the federal government to require financial institutions to maintain records on customers. But access is governed by existing legal processes.

(4) *Rowan v. Post Office Dept.* (1970) upheld a federal statute which gave recipients of U.S. mail the right to insist that their names be removed from a mailing list if they receive unsolicited mail which they find sexually offensive. The court rejected the argument that a vendor's rights include the delivery into the home of unsolicited material. As the court stated, "the asserted right of a

mailer...stops at the outer boundary of every person's domain."

(5) The Crime Control Act (1973) requires state criminal justice information systems to protect privacy and security of information.

(6) The Equal Credit Opportunity Act (1974) limits the information that creditors can collect, including race, color, region, sex, and marital status.

(7) The Privacy Act (1974) prohibits federal agencies from allowing information they have gathered to be used for another purpose. Loopholes allow sharing. This act temporarily set up the U.S. Privacy Protection Commission.

(8) The Family Educational Rights and Privacy Act (1974) (Buckley Amendment) requires educational records to be made available to students and limits disclosure to third parties.

(9) In *U.S. v. Miller* (1974), the Supreme Court ruled 5 to 4 that bank customers can have no legitimate "expectation of privacy" in bank records.

(10) The Right to Financial Privacy Act (1978) limits federal access to customer records in banks. This law does not apply to state or local governments and allows exceptions for the FBI and U.S. attorneys.

(11) The Tax Reform Act of 1976 requires that tax returns and personal information collected by the IRS may not be released without the individual taxpayer's permission. It also limits IRS access to some sources by requiring notice and an opportunity to challenge.

(12) The Electronic Funds Transfer Act (1980) provides that institutions must notify customers of third-party access to customer information on electronic funds transfers.

(13) The Paperwork Reduction Act (1980). The Office of Management and Budget must approve federal agency efforts to collect information. Federal requests for information must disclose why it is requested, how it will be used, and whether providing the information is voluntary or mandatory.

(14) The Debt Collection Act (1982) requires that due process protection must be met before information on an individual's federal debt may be revealed to a private credit bureau.

(15) The Cable Communications Policy Act (1984) restricts cable operators' collection and disclosure of personally identifiable information regarding cable service and restricts government surveillance.

(16) The Computer Fraud and Abuse Act (1986) makes illegal entry into computers to obtain classified information a criminal act.

(17) The Budget Deficit Reduction Act (1984) requires states to correlate tax, medical, and social security records in order to receive federal funds for welfare programs.

(18) The Video Privacy Protection Act (1988) forbids video retailers from selling or disclosing rental records without customer consent or a court order. This act is known as the "Bork bill," because Robert Bork was the subject of video store revelations in 1987 by the City Paper while a nominee for the U.S. Supreme Court.

(19) The Computer Matching and Privacy Protection Act (1988) restricts federal agencies from using computer matching of data to verify eligibility for benefits programs or for collecting delinquent debts.

(20) The Employee Polygraph Protection Act (1988) prohibits lie detectors in random testing of private employees and in pre-employment screening.

(21) The Telephone Consumer Protection Act of 1991 allows the FCC to create rules that prohibit the use of automatic telephone dialing systems or artificial or pre-recorded voice devices to deliver messages without the prior express consent of the called party. It also allows the FCC to prohibit the sending of unsolicited advertisements to telephone facsimile machines. (In May 1993, a U.S. District Court ruled that the act was an unconstitutional restriction on protected commercial speech.[26])

(22) The Cable Television Consumer Protection and Competition Act of 1992 adds to the previous requirement (1984 Cable Act) that cable operators must protect each subscriber's "personally identifiable information" (PII). Now, cable operators must also protect PII acquired through "any wire or radio communications service provided using any of the facilities of the operator that are used in the provision of cable service."[27]

(23) In addition to statutory protection, there is a whole array of judicially-imposed orders regarding trial and pretrial proceedings including limitations on public and press access to discovery materials and hearings and sealing certain records for purposes of protecting trade secrets, as well as more personal privacy issues.

Privacy Principles

A synthesis of the comprehensive European and the ad hoc American approaches to privacy protection is to formulate a set of broad rules or principles that can be applied to a sector of the economy or to a range of issues. This was the direction taken by the New York Public Service Commission in its consideration of telecommunications privacy through a proceeding initiated by this author.

The commission's approach in 1991 went well beyond the problem-specific method. It issued a set of broad privacy principles applicable to the whole range of telecommunications services under its jurisdiction.[28] They include, among others:

- Privacy should be recognized explicitly as an issue to be considered in introducing new telecommunications services. It needs to be spelled out and disclosed for new services, to the extent foreseeable.
- Carriers offering a new service that compromises current privacy expectations would generally have to bear the cost of providing a means of restoring the lost degree of privacy.
- People should be permitted to choose among various degrees of privacy protection.
- Unless a subscriber grants informed consent, subscriber-specific information generated by the communications service should not be used for purposes other than billing.

The use of privacy principles creates rebuffable presumptions, in contrast to strict laws. This dichotomy will be discussed in the next article. ntq

---

[1] E. M. Noam, *Telecommunications in Europe* (London: Oxford University Press, 1993).
[2] G. R. Pipe, "International Information Policy: Evolution of Transborder Data Flow Issues," *Telematics and Informatics*, Vol. 1, No. 4 (1984):409-418; and R. Turn, ed., *Transborder Data Flows: Concern in Privacy Protection and Free Flow of Information*, Vol. 1 (Washington, DC: American Federation of Information Processing Societies, 1979).
[3] Organization of Economic Cooperation and Development (1979).
[4] "European Data Base Searches Chapter than Using U.S.," *Transnational Data and Communications Report* (TDR), Vol. 6, No. 8 (1983), p. 423.
[5] D. Gilhooly, "EC Tackles Privacy," *Communications Week International* (July 16, 1990):1; and Commission of the European Communities, *Concerning the Protection of Personal Data and Privacy in the Context of Public Digital Telecommunications Networks* (June 5, 1990).
[6] H. Rowe, *UK: Personal Data Protection New Draft Directive* (London: Reuters Textline, Lloyd's List, May 21, 1993).
[7] P. Oster, M. Galen, and E. Schwartz, "Privacy vs. Marketing: Europe Draws the Line," *Business Week* (June 3, 1991).
[8] F. Kuitenbrouwer, "CNIL Warns Against Breach of Privacy Act," *Transnational Data Report*, Vol. 8, No. 5 (1985):226-227.
[9] H. P. Gebhardt, "The Legal Basis of Data Protection and Data Protection in the Field of Telecommunications in Seven Countries," *ITU Telecommunications Journal*, Vol. 57, No. 1 (1990):40.
[10] Oster, et al., "Privacy vs. Marketing," p. 124.
[11] *Transnational Data and Communications Report*.
[12] Gebhardt, "The Legal Basis of Data Protection and Data Protection in the Field of Telecommunications in Seven Countries."
[13] B. Niblett, *Data Protection Act 1984* (London: Oyez Longman, 1984).
[14] *Sixth Report of the Data Distribution Registrar* (London: Her Majesty's Stationery Office, June 1990).
[15] M. B. Feldman and D. R. Garcia, "National Regulation of Transborder Data Flows," *North Carolina Journal of International Law and Commercial Regulation*, Vol. 7, No. 1 (1982):1-25.
[16] R. T. Wigand, "Transborder Data Flow and Its Impact on Business and Government," *Information Management Review*, Vol. 1, No. 2 (1985).
[17] G. Anderla, *The International Data Market Revisited*, Report to the Second Symposium on TBDF, OECD (October 1983), p. 5.
[18] Turn, *Transborder Data Flows*.
[19] 20 USCS § 1232g(c), General Requirements and Conditions Concerning Operation and Administration of Education Programs: General Authority Records; Privacy; Limitation on Withholding Federal Funds (1993).
[20] 5 USCS § 552 Title 5, Government Organization and Employees (1993).
[21] Feldman and Garcia, "National Regulation of Transborder Data Flows."
[22] Justice William Douglas wrote, in *Griswold v. Connecticut*, of constitutional privacy rights as found "in penumbras formed by emanations."
[23] In 1988, there were more court-sanctioned wiretaps in New York than in any other state. *Privacy Journal*, Vol. XV, No. 12 (October 1989):3.
[24] See J. Berman and J. Goldman, *A Federal Right of Information Privacy: The Need for Reform* (Benton Foundation, 1989) for a useful general treatment of the issues and compilation of relevant statutory and case law.
[25] See J. E. Katz, "U.S. Telecommunications Private Policy," *Telecommunications Policy* (December 1988):357-360, for particular detail and analysis of ECPA and also the more generally valuable analysis of electronic privacy issues.
[26] *Moser v. Federal Communications Commission*, D.C. Ore., No. 92-1408-RE, 5/21/93; see 61 LW 2387.
[27] Communications Act § 631(a)(2)(B); 47 U.S.C. § 551(a)(2)(B). See C. D. Ferris, F. W. Lloyd, and T. J. Casey, *Cable Television Law: A Video Communications Practice Guide*, Vol. 1 (New York: Time Warner Books, 1993), p. 17A-14.
[28] State of New York Public Service Commission, *Proceeding on Motion of the Commission to Review Issues Concerning Privacy in Telecommunications*, Case No. 90-C-0075 (March 22, 1991).