COMMUNICATIONS PRIVACY: IMPLICATIONS FOR NETWORK DESIGN

Marc Rotenberg

"To think that a bit of paper, containing our most secret thoughts, and protected only by a seal, should travel safely from one end of the world to the other, without anyone whose hands it had passed through having meddled with it.

—Ralph Waldo Emerson
(1803–1882)

The American jurist Louis Brandeis described the right of privacy "as the most comprehensive of all rights and the right most cherished by civilized men." The French political theorist Francis Lieber praised "The sacredness of epistolary communion." Privacy has been described by some as the "kernal of freedom," and the right from which other freedoms flow.

The roots of privacy protection go at least as far back as the Athenian democracy. The Greek statesman Pericles described the virtues of a private life, free from public scrutiny. In a famous oration before the people of Athens, Pericles extolled the virtues of democratic society and then stated, "Not only do we conduct our public life as free people but we carry the same spirit in our daily relations with one another. We are not angry with our neighbor if he does what pleases him, and we don't glare at him for his harmless actions even if they are an annoyance to some."

Although privacy as a legal right is traditionally associated with Western liberal countries, privacy is also described in the literature of many countries around the world. So widespread is the desire for privacy protection that several of the recently established democratic governments in Eastern Europe and the former Soviet Union have included the right of privacy in their new constitutions.

The protection of privacy is the central concern for a communications network. Communications privacy allows users to transfer information that might otherwise not be disclosed. Where privacy cannot be assured, the value of a communications network diminishes significantly and users are likely to seek other channels to exchange information. In a properly functioning network, the protection of confidentiality should be assumed. Exceptions should arise only in extraordinary circumstances.

Communication services are more highly valued when privacy can be assured. Where privacy protection falls below a certain threshold, migration from the network is likely to occur since privacy assurance allows organizations to retain control of trade secrets and details of business operations. Anonymity may also increase economic risk-taking since certain investments may be curtailed if the identity of the investors is known.

A difficult social question, and an intriguing economic problem, is whether it would be efficient to charge users for privacy protection. It is conceivable that privacy protection could be priced for users along a spectrum so that the protection of a message would be in direct proportion to the price charged. However, such schemes might introduce new transaction costs and create inefficiencies if they require users to conduct additional negotiations where two parties do not enjoy the same level of protection. Multiple levels of privacy protection might also lead to unnecessary segmentation, particularly in networks that are intended for broad public use.

Communications Privacy

The protection of communications privacy is a subset of privacy protection that is concerned primarily with the exchange of personal information between multiple parties. Traditional models for communications privacy are based on the exchange of information between two parties, though in computer network environments, messages are oftentimes exchanged between multiple parties. This trend toward message exchange among multiple parties reflects in part the transition from a time when a physical message, such as a letter, was transferred from one party to another to the current era where electronic messages are routinely sent to multiple parties.

In communications networks, the right of privacy might be delineated into three separate interests: confidentiality, anonymity, and data protection.

Confidentiality. This refers to the expectation that information will be moved between two parties without disclosure to a third party. A confidential communication exhibits the property that its content and existence is known only to the parties to the communication. Assuming that a communication is confidential, subsequent disclosure can be attributed to either the sender or the recipient of the message. Where a communication occurs between multiple parties, the expectation of confidentiality may be diminished as it is more difficult to determine who is responsible for subsequent disclosure.

The legal basis for confidentiality has several roots. There are special relationships where the guarantee of

a legal right of privacy is considered necessary to strengthen a social relationship and to promote the exchange of personal information. In the common law countries, such as the U.S. and the U.K., these relationships may include communications between lawyer and client, wife and husband, and doctor and patient. Additional areas where common law recognizes an interest in protecting communications is banking and other forms of trusteeship. Sometimes these obligations are expressed through legislative enactment, such as the Electronic Communications Privacy Act, a law that restricts the circumstances when an email service provider may disclose private email.

Anonymity. Anonymity is the right of an individual to decide whether to disclose his or her identity to another. The right of anonymity is an important element of privacy protection. Privacy includes the ability to decide when and under what circumstances to disclose identity. In public settings, anonymity may protect the ability of individuals to move freely and without obstruction. Anonymity is also associated with the freedom to express unpopular views.

In many settings, the disclosure of identity is not a necessary condition for communications, or even for a business transaction. For example, a person who calls a government agency for information or a business to inquire about a product need not disclose her identity. Similarly, network users who "ftp" a site typically don't need to disclose their identity. In some circumstances, services may require that anonymity be preserved to be viable. Health services for those needing assistance with alcohol, drugs, depression, unexpected pregnancy, or sexual identity may rely on a promise to guarantee anonymity to ensure the viability of the service.

In some network settings, anonymity may be a difficult principle to protect. Access to information resources may require the disclosure of identity to promote security. However, for currency-based service delivery, the identity may be withheld if a mechanism exists to exchange information for value. Public payphones that use either cash or telephone cards (not credit cards or "calling" cards) are examples of widely available communications service that provide anonymity.

Data Protection. This refers to those principles regarding the collection, use, and disclosure of personal information. Data protection principles were originally developed for the protection of personal information contained in discrete record systems. Over time, data protection principles have been extended to communications networks. These principles are discussed in more detail in the section on the OECD Guidelines.

A fourth interest has been raised in the context of communications networks but may not play a substantial role in future network environments. This is the interest in seclusion, sometimes called "the right to be let alone." The reason this interest may become less significant over time is that network messaging design have all tended toward the batching of requests. In telephone networks, dedicated phone answering machines and voice mail systems allow users to group messages and to respond at a convenient time. However, targetted advertising, based on user profiles, may become more intrusive than other forms of advertising. Communications technologies that may raise intrusion problems include those requiring a real-time response, such as beepers.

Exceptions of Privacy Protection

National law and international treaties generally recognize certain exceptions to the protection of privacy. These exceptions proceed from the assumption that communications privacy is absolute except where there is legal authority to intercept a message or to obtain information about the record of the message.

The first exception is when consent is obtained from the person whose personal information would not otherwise be disclosed. When the information refers to a record that is linked to a single individual, such as a medical history or a financial record, consent need only be obtained from the record subject. However, when the information concerns the existence or content of an electronic communication, then consent is more problematic. In some countries, it is permissible to obtain consent from only one party to the communication. In other countries, both parties must grant consent. In the U.S., there are states that observe both "one-party" and "two-party" consent rules. Since the "two-party" consent rule protects the privacy interests of both parties, it is generally preferred.

The second exception is for criminal investigations. In such cases, a government agent may seek to obtain records of communications, to monitor communications, or to restrict the use of communications networks. In many countries such investigations may be undertaken only in the context of a specific criminal matter and pursuant to authority of an independent agency. Constitutional governments generally prohibit by law the unrestricted gathering of electronic communications.

Overly broad searches through electronic record systems typically elicit strong public criticism. In one widely reported incident in the U.S., the police searched through the records of 803,000 phone users in a large metropolitan area to determine who had called a particular reporter regarding the misconduct of a large company. The head of the company, who initiated the investigation, later expressed regret for his decision.

The third exception is for the maintenance of the network. Thus, electronic service providers are permitted to monitor communications on a limited basis to test network services and to ensure the continued operation of the network. A related exception is the right to disclose information when it is "necessary" to render the service. For example, a communications carrier may be required to transfer information about a call to another carrier so that the call may be completed, or to send billing information to another party for delivery to the customer. This may be considered necessary to render the service.

Content and Record Distinction

In communications networks, both legal and technical protection distinguish between the content of a message and the record of a message. In

In the U.S., the Supreme Court has said that a telephone call is entitled to **a reasonable expectation of privacy,** *however, the numbers a caller dials* **are not entitled to similar protection.**

a telephone network, for example, the content of a telephone call is rarely disclosed while transactional information may be more freely available. This is an area of considerable dispute. In the U.S., the Supreme Court has said that a telephone call is entitled to a reasonable expectation of privacy, however, the numbers a caller dials are not entitled to similar protection. Following the Supreme Court's decision, Congress determined that such information should be entitled to protection and a law was passed in 1986, the Electronic Communications Privacy Act, to accomplish this goal.

The retention and disclosure of transactional information for telecommunications networks is also a matter of differing opinion. In the U.S., telephone companies routinely disclose detailed billing information to customers. These records include the date and time of call, the location of the call, and the amount charged.

This practice is not generally followed by other service providers. In Europe, for example, detailed billing information is not available or where it is available, the last four digits are not disclosed. NTT in Japan offers a range of privacy options for customers. Customers may choose to receive complete call detail information, partial call detail information, or no call detail information at all.

Regarding the retention and disclosure of this information, there are competing consumer and privacy interests. It is believed that the delivery of this information provides consumers with better accounting for network usage, and, where multiple carriers offer services, to select more competitive options. This information also permits companies to monitor network usage and to assign costs to clients where appropriate.

Forms of Protection

In the area of privacy protection, schemes may be divided between technical and legal forms of protection. Technical forms seek to reduce the risk of interception of communication, unauthorized access to records of communications, or to conceal the identities of the parties to a communication. Technical schemes also include design principles, policies, and practices.

Legal forms of protection establish rights that are enforceable in law. These rights typically allow for the recoupment of damages from private parties, criminal fines, or restrictions on the use of the unlawfully gathered information where the transgression occurs by the government.

Legal protections are likely to clarify the underlying privacy interests, but are also likely to encounter problems in practice where messages move between different countries and through different jurisdictions. For this reason, technical safeguards are particularly important for international networks.

European phone systems, as well as networks in Japan, Australia and South America, make extensive use of "phonecards." These are value-added cards that may be used to purchase telecommunication services. They are transferrable and contain no personally identifiable information.

From a communications privacy viewpoint, phonecards are a good technology. They protect anonymity since they do not require the disclosure of the user's identity. They also satisfy data protection goals since no personally identifiable information is generated. With regard to confidentiality, phonecard networks do not necessarily provide any greater protection than other networks. However, since the identity of a particular user would be difficult to determine, the likelihood of interception is diminished.

Phonecards diminish vandalism, reduce repair requirements, and can even be sold for advertising. Regarding this last benefit, NTT in Japan prints a wide range of cards for advertising purposes and British Telecommunications prints advertising for the Wimbledon tennis championships and Hilton hotels on the face of the cards.

Cryptography

One of the primary methods to promote communications privacy is cryptography. This is the procedure of taking a plaintext communication and then encoding it into cyphertext. Messages encoded in this manner should be useful to only the sender and the intended recipient.

All cryptographic schemes rely upon a "key." The key allows the person in possession of the message to decode it. Broadly speaking, there are two different key encryption schemes. The first is the private key scheme. The second approach is the public key scheme.

The private key scheme relies on the existence of a single, secret key which is used both to encrypt and decrypt messages. An example of private key encryption (PKE) is the Digital Encryption Standard (DES), which is a popular secret-key encryption algorithm originally released in 1977 by the National Bureau of Standards in the U.S. It was the first cryptographic algorithm openly developed by the U.S. government. The problem with DES and PKEs generally is transferring the key. There

must be a pre-existing channel to transfer the keys which is itself secure.

In the public key scheme a user has both a public key, which is published in a directory similar to a phonebook, and a private key, from which the public key is derived. This has an advantage over private key systems since it is not necessary to exchange keys before messages can be decrypted. A popular public key system is RSA.

A related use for cryptography is the authentication of messages. Using public key encryption, a user can encrypt a message using his or her own private key. The recipient of the message can then determine the authenticity of the messages by using the sender's public key.

To be effective, standards must be established so that users in different networks will be able to exchange messages. Anything less than a full implementation makes it inconvenient and inefficient for users and reduces use and diminishes privacy. Because there are strong incentives to interconnect networks, it is expected that standards for encryption will develop rapidly.

A separate problem in the deployment of cryptographic methods is the prospect that national governments will seek to restrict privacy-enhancing technologies where they conflict with communications surveillance activities.

Legal Agreements and Policies

Many current policies for communications protection follow from international agreements developed for the general purpose of data protection. These international instruments include the Organization for Economic Cooperation and Development (OECD) Guidelines of the Protection of Privacy and Transborder Flow of Personal Data, The Council of Europe's Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data, and the United Nations Universal Declaration on Human Rights, particularly Clause 12. More recently, the European nations have sought to develop a harmonized framework for data protection throughout the European Community. It is likely that this directive will have a substantial impact on the development of international privacy policy.

OECD Guidelines

In 1978 the OECD, which is made up of two dozen countries including much of Europe, the U.S., Canada, Japan and Australia, instructed a Group of Experts to develop Guidelines on basic rules governing the transborder flow and the protection of personal data and privacy. The initiative was based on the belief that disparities in national privacy legislation might create obstacles to the free flow of information between countries, thus having serious repercussion on the economies of the OECD Member States. The principle aim of these guidelines was to facilitate the harmonization of the national legislation of OECD Member States.

The OECD Guidelines on the Protection of Privacy and Transborder Flow of Personal Data were adopted in 1980 and are today generally considered the primary reference for international agreements for privacy and data protection. The guidelines incorporate eight basic principles.

- The Collection Limitation Principle states that the collection of personal data should be obtained by lawful and fair means and with the knowledge and consent of the record subject.
- The Data Quality Principle states that personal data should be relevant to the purposes for which they are to be used, and should be accurate, complete, and timely.
- The Purpose Specification Principle states that the purpose for which personal data are collected should be specified not later than at the time of data collection and the subsequent use should be limited to those purposes.
- The Use Limitation Principle states that personal data should not be disclosed for secondary purposes except with the consent of the data subject or by authority of law.
- The Security Safeguards Principle states that personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, or disclosure of data.
- The Openness Principle states that there should be a general practice of openness about developments, practices and polices with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use.
- The Individual Participation Principle states that data subjects should be allowed to inspect and correct personal data.
- The Accountability Principle states that a data controller should be held accountable for complying with measures which give effect to the preceding principles.

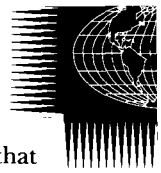
Taken together, these principles are intended to ensure that those organizations which collect personal data will take appropriate steps to safeguard personal information.

Although the OECD Guidelines are widely followed by public and private organizations around the world, several criticisms have been expressed. These include the absence of a clear enforcement mechanism, inadequate attention to commercial incentives to sell personal data, and no consideration of the misuse of personal indentifiers.

The Council of Europe Convention

In 1981 the Council of Europe adopted the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data. The Convention incorporates principles similar to the OECD Guidelines. The Convention states that "Personal data to be automatically processed shall be: (a) obtained and processed fairly and lawfully, (b) stored for specified and legitimate purposes and not used in a way incompatible with those purposes, (c) adequate, relevant, and not excessive for the purposes for which they are maintained, (d) accurate, and where necessary, kept up to date, and (e) preserved in a form which permits identification of the data subject for no longer than required for the purposes for which those data are kept."

The Convention is not intended to be a self-executing document. The goal is to encourage countries to de-



velop privacy legislation in accordance with the principles formulated in the Convention.

Universal Declaration of Human Rights

The Universal Declaration of Human Rights was proclaimed by the United Nations General Assembly in 1946. It is a powerful statement of the global aspiration of respect for human rights and expresses general principles of international law. Its provisions have been incorporated in many constitutions around the world.

Article 12 of the Universal Declaration states that "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."

One privacy concern that grows out of the Universal Declaration which may have some bearing on privacy protection and the use of identifiers in communications networks is the protection of personal names and identity. For example, where national governments seek to impose the use of a universal identifier, such as a Personal Identification Number (PIN) or Social Security Number (SSN), concern has been expressed that this will undermine cultural identity and the freedom of minority groups.

EC Directive

As the European Community moves toward a harmonized economic system with a single currency and a federated government, the member nations have indicated a commitment to develop a single framework to protect the transborder flow of personal data. The Commission of the European Communities has put forward a proposal concerning the protection of the individual in relation to the processing of personal data. It is an effort to build on the existing OECD Guidelines. It also seeks to create an enforcement mechanism and to establish rights for data subjects where companies seek to sell personal information.

The Draft Proposal Concerning the Protection of Personal Data in the Context of Public Digital Telecommunication Networks was promulgated by the Commission in 1990. The Commission stated that the "effective protection of personal data and privacy is developing into an essential precondition for social acceptance of the new digital networks and services." The Commission further said that privacy protection "must be an essential component of the Community's telecommunications policy which aims at securing for the European citizen the full benefits of advanced telecommunication services, as the Community moves towards an environment which will be substantially richer in information than before."

The directive contains several provisions which mirror the OECD Guidelines. It also includes certain additional measures. Telecommunications organizations are admonished not to store information after transmission except where required by law of a Member State. The directive requires that "traffic data stored in the switching centers of the telecommunications organization must be erased after termination of the call unless the data are anonymised or are required for billing or other legitimate purposes." The directive recommends that itemized billing statement exclude the last four digits of the called number.

The directive makes two important recommendations for the "Caller ID" service. First, it states that subscribers should be able to withhold the disclosure of the subscriber's phone number through a "simple technical facility." Second, the directive indicates that the subscriber should be able to permanently withhold disclosure of the number when application is made. Third, the directive recommends that call recipients should be able to apply for permanent elimination of the identification of all incoming calls and must also be able to limit the acceptance of incoming calls to those which identify the calling subscriber's number. The directive permits the limited override of the calling party where the subscriber has received malicious calls or upon court order. In the case where the subscriber has received malicious calls, the directive indicates that caller identification information should be made available directly to the public authority charged with the prevention of criminal offenses. The directive also covers electronic recording and unsolicited communications.

MPT proposal (Japan 1989)

The Ministry of Posts and Telecommunications (MPT) has developed a set of principles based on the OECD Guidelines for the protection of communications privacy. The Guidelines on the Protection of Personal Data in Telecommunication Business (1991) set out a framework for privacy protection and include several principles that would be useful for computer networks.

The guidelines began with a restatement of the Fair Collection principles: "The collection of personal data in connection with the provision of telecommunications services should be limited to the extent necessary to provide the intended service." There follows a set of principles, similar to the OECD Guidelines, that cover Collection of Data, Use and Disclosure of Data, Proper Management of Data, Access to Data, and Accountability.

It should also be noted that Japan has one of the strongest constitutional provisions regarding communications privacy. The Japanese Constitution states that "Freedom of assembly and association as well as speech, press and all other forms of expression are guaranteed. No censorship shall be maintained, nor shall the secrecy of any means of communication be violated."

National Law

Countries may develop through their legal systems certain procedures and customs to protect communications privacy. Traditionally these laws take the form of restrictions against wire surveillance by government agents. General laws for the protection of privacy are found throughout the world. These include the Privacy Protection Act (Japan), the Law on Informatic and Freedoms (France), Federal Data Protection Act (Germany), the Privacy Act (U.S.), the Data Protection Act (U.K.).

These laws vary in their scope, purpose, and impact. Some follow a data protections scheme, where a particular agency is charged with oversight of privacy protection. Others are not self-executing and rely upon enforcement through the courts. There are also privacy laws that address particular subject areas. In the U.S., these include, records of cable subscribers, video tape purchases, and email.

Quasi-Legal Protection

An additional category of protection includes professional codes of conduct, industry codes, and other forms of self-regulation. For instance, the ACM has an explicit code of conduct which covers the privacy of personal records. The American Library Association (ALA) does so as well.

The Code of Ethics and Professional Conduct for the ACM states that "An ACM member shall consider the health, privacy and general welfare of the public in the performance of the members work." The guidelines further state that "An ACM member, whenever dealing with data concerning individuals, shall always consider the principle of individual privacy and seek the following: To minimize the data collected; To limit authorized access to the data; To provide proper security for the data; To determine the required retention period of the data; To ensure proper disposal of the data."

The preliminary code for the International Federation of Information Processing (IFIP) makes data protection a central provision of individual professional ethics: "Information Technology Professionals have a fundamental respect for the privacy and integrity of individuals, groups, and organizations. They are also aware that computerized invasion of privacy, without informed authorization and consent, is a major, continuing threat for potential abuse of individuals, groups, and populations. Public trust in informatics is contingent upon vigilant protection of established cultural and ethical norms of information privacy."

Some industries have developed codes of conduct for privacy protection to regulate activities by members. The Direct Marketing Association advises members that "An individual shall have the right to request whether personal data about him/her appear on a direct marketer's files and to receive a summary of the information within a reasonable time after the request is made. An individual has the right to challenge the accuracy of personal data relating to him/her. Personal data which are shown to be inaccurate should be corrected." (DMA Guidelines, Article 4).

However, there is a substantial question regarding the adequacy of these self-regulatory mechanisms, and particularly the DMA Guidelines. In 1990, when a direct marketing product was proposed that did not satisfy Article 4, the Direct Marketing Association took no action. Criticism of the product by consumer and privacy organizations led to the withdrawal of Lotus Marketplace.

Library organizations have developed the strongest voluntary code to protect personal privacy. This is not surprising. Libraries view the protection of confidentiality as a primary obligation of libraries.

The Code of Ethics for the American Library Association states that "Librarians must protect each user's right to privacy with respect to information sought or received, and materials consulted, borrowed, or acquired."

Library policies on record confidentiality should be considered in the design of network services.

U.S. Wiretap Law

The wiretap law in the U.S. is based on the premise that individuals have "an expectation of privacy" in electronic communications. The law requires that government agents obtain a special warrant from a court before an interception may be undertaken. The requirements for such a warrant are particularly rigorous, and the police must demonstrate that other investigative methods have been exhausted or could not succeed. The wiretap law also provides civil penalties where individuals conduct an illegal interception.

Today, the U.S. wiretap law stands as a model of how constitutional principles developed before telephones were invented and are carried forward into an era where computers are ubiquitous. The history of the wiretap law in the U.S. also reveals the curious twists and turns that occur in a legal system based on both judge-made law and legislative rule making. It also suggests how legal systems attempt to catch up to technological developments.

In 1928 the Supreme Court considered the question of whether the Fourth Amendment to the Constitution, which prohibits unauthorized searches and seizures, also restricted interception of telephone communications. The Supreme Court ruled that it did not, though Justice Brandeis, the author of a famous 1890 article on the right of privacy, dissented from the Court's opinion and said that the Constitution should protect new forms of communications. Partly in recognition of the concerns expressed by Justice Brandeis, when Congress passed the Communications Act of 1934 a provision was included which said, "No person not being authorized by the sender shall intercept any communications and divulge . . . the contents." Then the Supreme Court ruled in 1938 that the Communications Act prohibited all telephone wiretapping, even when done by government officials. However, the Department of Justice said the law did not in fact restrict wiretapping by government agents. The President also issued an executive order which permitted wiretapping for national security purposes. As a result, wire surveillance was often undertaken without clear legal authority.

The next dramatic development occurred in 1967 when the Supreme Court, in a case called *Katz vs. United States,* reconsidered its 1928 opinion and decided the Fourth Amendment did protect telephone communications against interception. The following year Congress passed legislation to permit wire surveillance by law enforcement agents, but only when a number of conditions were satisfied, including a requirement that agents "minimize" the collection of information they obtain as a result of the wiretap. The law also said that

It is conceivable that **privacy protection could be priced** *for users* **along a spectrum** *so that the protection of a message would be in direct proportion to the price charged.*

communication service providers were expected to assist law enforcement in executing lawful warrants, but there was no expectation that telephone companies would design networks to facilitate wire surveillance.

Since passage of the 1968 law there have been several significant amendments. In 1978 the Foreign Intelligence Surveillance Act (FISA) was passed. This law established legal standards and procedures for the use of electronic surveillance in collecting foreign intelligence in the U.S. This was the first legislative authorization for foreign intelligence wiretapping and other forms of electronic surveillance.

In 1986 the U.S. wiretap law was again amended. This time to extend the protection in the law to new forms of communication, such as digital networks and email. Provisions similar to those contained in the existing wiretap law were extended to new forms of communication.

Policy Frameworks

In the past several years several policy frameworks for the protection of communication privacy have been put forward. While these proposals do not carry the force of law, they set out useful principles that may be incorporated in future laws and technology designs.

During 1989 and 1990 the New York Public Service Commission studied privacy in telecommunications services. The proceeding was initiated by Commissioner Eli Noam who now heads the Columbia Institute for Tele-Information (CITI) at Columbia University.

The NYPSC proceeding has had a substantial impact on communications privacy policy in New York state and many other jurisdictions. Of particular interest were the factors identified by the Commission that have led to public interest in privacy protection, and the proposed privacy principles.

The study identified four factors that contribute to growing public concern about communications privacy. These are (1) the growth of electronic transactions, (2) the accelerated collection of personal information, (3) the dramatic increase in the number of communications carriers and service providers, and (4) the growing use of technically unsecured conduits for communications traffic, such as mobile communications.

The study then made several recommendations for future service offerings: (1) there should be no enforced reduction of network intelligence to protect privacy; (2) there should be adequate privacy protection for all users, "premium privacy" should be available for those with special needs; (3) privacy-promoting technologies should be encouraged; (4) users with needs for high levels of privacy should pay additional costs; (5) "The cost of restoring the status-quo in privacy protection should be borne by those who alter it," so that where a service such as "Caller ID" reduces the privacy of certain users, those subscribers who purchase the service should also carry the cost for re-establishing the privacy equilibrium; (6) privacy risks, particularly involving the disclosure of personal data, should be made known to users; (7) organizations that collect personal data should operate as "trustees" and protect the privacy rights of customers; and (8) there should be joint ownership on transaction-generated information.

Several of the NYPSC principles were later incorporated into a national communications privacy policy issued by the Minister of Communications in Canada in 1992.

Current Communication Privacy Concerns

In the past few years, several issues have arisen in the area of communications privacy. Although these are new developments, several of the principles previously described help to clarify the underlying privacy interests at stake.

The offering of the Caller ID service in the U.S., Canada and several European countries raised public interest in communications privacy. The service permitted the communications carrier to sell the number of the originating caller to the call recipient.

Two different analytical views of the privacy implications of the service arose. Under one approach, the privacy issues were viewed as the weighing of two competing privacy interests. According to this analysis, the call recipient had a greater privacy interest because the call originator had "intruded" upon the recipient. However, this view failed to take account of communications to parties that lacked a clear privacy interest, such as calls to a business or a government agency, or to electronic recording devices, such as voice mail services and answering machines.

Under a second approach, the privacy interest was seen in terms of the transfer of control over personal information. Here the concern was the ability of the carrier to sell data generated by the communication. Viewed in this manner, the service was generally viewed as a privacy loss for network users since control over personal data would be diminished. An additional concern raised was that if service providers routinely

transferred transactional information to a business who subscribed to the service, detailed profiles on users could be developed.

Regulatory authorities in the U.S. and Canada generally favored this second view and recommended strong restrictions on the use of the service. The policy debate surrounding Caller ID, and questions regarding the disclosure of personal data, are likely to continue as the service is offered in other countries in the near future.

One difficult problem that has arisen is the question of whether a network service provider should sell the transactional records resulting from an electronic communication. For example, in the U.S., several telephone companies sell lists to companies of callers to certain numbers. This is done to facilitate direct marketing.

Several privacy scholars have questioned this practice and recommended that a theory of joint ownership be developed so that any commercial benefit resulting from the sale of transactional records require the consent of both parties to the communication.

A related problem for communications privacy is the required disclosure of network information to competitors. In the U.S. it has been argued that competitive service delivery requires that network service providers disclose Consumer Proprietary Network Information (CPNI). While this policy may well promote the development of network services, it clearly has adverse consequences for privacy protection.

Government Restriction on Technology

There was a surprising development in the U.S. in 1992 when the Federal Bureau of Investigation put forward a legislative proposal to require all communications companies in the U.S. to design equipment so that remote wire surveillance could be undertaken.

The proposal was opposed by equipment manufacturers, service providers, and various privacy and civil liberties organizations. Criticisms of the proposal include the assessment that it would slow technical development, introduce new network vulnerabilities, increase costs for telephone customers, and increase the likelihood of wire surveillance by government agents.

Although it is unlikely that such legislation will be adopted in the U.S., it is foreseeable that national governments will seek to restrict development in communications technology. In the U.S. in April 1993, the White House announced a proposal for a split-key escrow cryptographic scheme that would allow the government to decrypt encrypted communications in voice networks. Several industry companies and cryptography experts have raised questions about the desirability of the plan. Whit Diffie, one of the creators of public key cryptography, commented that "the proposal doesn't contain a back door but a front door."

Personal Communication Networks

Personal communication networks (PCNs) have also raised new privacy issues. These are networks that assign specific numbers to users, rather than devices, who can then be located. A variation of the PCN issue is the use of Active Badges in the workplace. These devices are now in use in several computer labs and allow the ready location of particular individuals.

PCNs generally assume that each user in the network will be assigned a unique identifier. This is different from traditional telecommunications networks. In these networks, numbers are assigned to the phone instrument.

As a general matter, unique identifiers raise no special privacy concern. They are widely used by organizations in a variety of settings to ensure record accuracy. In communications networks, they may be virtually impossible to avoid. However, the unrestricted use of unique identifiers does raise privacy concerns. When a single identifier is used in multiple settings, it permits the exchange of personal information oftentimes without the individual's knowledge or consent. In Europe and in the U.S., there has generally been a presumption against the use of "universal unique identifiers," such as PINs or SSNs. Where such proposals have gone forward, it has been over the objection of privacy experts and system designers. Therefore, "unique unique identifiers" used in the context of transactional environments, such as network services, are preferred, while "universal unique" identifiers are likely to raise privacy problems.

A second question that has been raised about PCNs is the risk of geographical surveillance. Several commentators have said that "follow me, find me" systems are fine as long as the there is no additional risks if the person's physical location is known to others. Others say that what is needed is a system designed to "follow me, find me, and then leave me alone." Restrictions on some PCN capabilities might be appropriate to protect privacy and to ensure personal mobility. ◻

Bibliography

Commission of the European Communities. Proposal Concerning the Protection of Personal Data in the Context of Public Digital Telecommunication Networks.

Flaherty, D. Protecting privacy in surveillance societies: The federal Republic of Germany, Sweden, France, Canada, and the United States (Chapel Hill 1989).

Noam, E. Special Report: Telecomm Privacy Policy Elements. Transnational Data and Communications Report, (March 1990), p. 9.

Nugter, A.C.M., Transborder Flow of Personal Data Within the EC. Kluwer, Boston, Mass., 1990

OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

Rotenberg, M. In Support of a data protection board in the United States. *Gov. Info. Quart. 8* (1991), p. 79.

About the Author:

MARC ROTENBERG is Director of the CPSR Washington Office and an adjunct professor at Georgetown University Law Center. He also chairs the ACM Committee on Scientific Freedom and Human Rights. **Author's Present Address:** CPSR, 666 Pennsylvania Ave., SE, Ste. 303, Washington, D.C. 20003; email: rotenberg@washofc.cpsr.org