
Fred W. Weingarten

Follow this and additional works at: http://repository.jmls.edu/lawreview

Part of the Communications Law Commons, Computer Law Commons, Consumer Protection Law Commons, Internet Law Commons, Legislation Commons, Privacy Law Commons, and the Science and Technology Law Commons

Recommended Citation

http://repository.jmls.edu/lawreview/vol21/iss4/2

This Article is brought to you for free and open access by The John Marshall Institutional Repository. It has been accepted for inclusion in The John Marshall Law Review by an authorized administrator of The John Marshall Institutional Repository.
COMMUNICATIONS TECHNOLOGY: NEW CHALLENGES TO PRIVACY

FRED W. WEINGARTEN*

"Shadows on the wall have caught your whispers, and brought them to my ear."
- Charles Dickens, Oliver Twist

INTRODUCTION

In the last two decades, worry over the impact of information technology on personal privacy has been concentrated on computerized data bases — on how information about people is handled. Important reports and laws such as the Health, Education and Welfare ("HEW") Commission Report, the Privacy Act of 1974, and the Privacy Commission Report have been concerned with data collection, storage and use. Therefore, the privacy debate has been addressed to questions such as: What may be collected? Who may collect it? What use may be made of it? Who may it be shared with? And, what "stewardship" must the holder of personal data exercise over its integrity and confidentiality? Today, these questions are still pertinent and remain unresolved in many areas of privacy policy.

However, while attention has been directed to the increasing power and scale of computerized data banks, a revolution in communications technology has redirected policy attention to another issue that has been pertinent for a long time—the protection of personal communication channels. The revolution, driven by developments in

* Program Manager Communication and Information Technologies, Office of Technology Assessment, United States Congress.

The views expressed in this article are those of the author and do not reflect the views of the Office of Technology Assessment, The Technology Assessment Board, or the United States Congress.

1. I will not offer a comprehensive definition of privacy, but the principal concern in this paper is with "information privacy" and not with the protection against physical intrusion of the body, privacy of the home, and so on.


5. For more detail and history of data privacy, see Office of Technology Assessment, Electronic Record Systems and Individual Privacy (1986).
fiber optics, satellites, and digital transmission, marks a change in the basic technology underlying telephonics. Furthermore, the increasing use of alternative modes of communication such as home cable, electronic mail, and facsimile transmission, have engendered new services. The protections of telephone and the mail have been eroded or eliminated, while some new media such as electronic mail are not protected at all. In addition, media such as cordless and cellular phones seem particularly vulnerable to unwanted eavesdropping. These problems have raised the following fundamental policy questions: Under what circumstances do people have the right to establish or use confidential channels for their personal communications? What responsibility does the Government have to protect their rights to do so? Under what circumstances may that confidentiality be legally breached, and by whom?

This paper is concerned with how Congress addresses such policy questions. It examines three examples of privacy policy issues raised by new developments in technology—restrictions on wiretapping, employer monitoring of employees, and provision of technical protections. Based on three reports released by the Office of Technology Assessment over the last two years, the focus of this paper is privacy policy, particularly at the federal level. Of primary importance are the social goals of what we wish to achieve as a society, and law as a mechanism for achieving them. It raises some important issues for which legal solutions will be difficult to establish.

SOCIETY AND SECRECY

We assume that an important characteristic of privacy in a free society is the ability to communicate in confidence or to share secrets selectively. The closed door and window, and the whisper in the corner assert this desire, which is a social convention even when not protected by law. Furthermore, we commonly expect that confidentiality depends on agreement with the person with whom we communicate, based on the nature of the information communicated. For instance, information exchanged between clients and professionals can be protected. The law protects certain communications, such as those between a client and a lawyer, doctor and a patient, or priest and a confessor. We also expect, however, some degree of confidentiality from our bankers, librarians, teachers, and others. Social mores dictate (however weakly) that personal confidences not be repeated or publicized.

However, as soon as the parties to a communication move apart physically and must use some intermediary technology to pass their

6. This intermediary technology refers to both artificial constructs, such as cars,
messages, agreements between them cannot alone guarantee privacy. The channel through which the message moves must, itself, provide some measure of protection. For example, the Government protects first class mail by the postal statutes, and protects the telephone call by a series of laws against wiretapping and other unauthorized eavesdropping.

Of course, personal privacy is not the only reason for the public interest in protecting the confidentiality of communications. The increased reliance of government, business, and other social institutions on electronic communication means that all of these users are increasingly vulnerable to unauthorized intrusions. The costs of such intrusions can be extraordinarily high — the collapse of financial markets, the blacking out of the electrical power distribution grid, or the failure of the nation's air traffic control system. Social reliance on information technology, in turn, raises the privacy stakes for individuals as more business transactions and other types of personal data are transmitted electronically. Thus, providing secure communications is increasingly important.

On the other hand, secrecy is not always viewed as a positive attribute. The open flow of information is important in a democracy to spread ideas and share scientific and other data. In contrast, spies, thieves, and environmental polluters want to work their mischief in secret to hide their conspiracies from those who would attempt to stop them.

Consequently, as members of a democracy, we demand that many activities that affect the public interest be open to scrutiny. Freedom-of-information and government-in-sunshine laws at both the federal and state level impose openness on the processes of government. The securities laws require financial disclosures by publicly held firms. The first amendment protects the ability of the press to "spill the beans" by publishing secret information without prior restraint. Such laws and regulations are predicated on the idea that the citizenry should know some information in spite of other people's desires to keep it secret.

In turn, the government claims the right to intrude on secrecy when the public interest is great enough. For example, enforcing the law, collecting taxes, and conducting a census are legal activities re-

and the institutional structures that directly serve it, such as state licensing agencies or systems of traffic laws. Pencil and paper is a form of technology, as was the Pony Express.

7. Technology can intrude into intimate communications as well. Powerful listening devices, miniature microphones and video cameras, pocket-size voice stress recorders, and so on have made even the confidential whisper vulnerable to unwanted eavesdroppers.

quiring that the government sometimes penetrate walls of secrecy, regardless of individual wishes.

Public policy to protect communications privacy, therefore, needs to establish and maintain a careful balance between both goals, preserving confidentiality and providing for public scrutiny. It does so by: 1) establishing protected lines of communication; and 2) by providing procedures for deciding whether a demand for access outweighs the need for confidentiality and, when warranted, permitting that access.

PUBLIC INTEREST

The various legal structures that the government has established to protect communications show five basic underlying principles that motivate policy making. Unlike the laws themselves, these principles seem to be independent of historical change. These principles persist, despite changes in technology and, even to some extent, in social values. They are as follows:

1. *Some protected channels must be made available.*

   It would be impossible to offer legal protection to all communications that take place between people at a distance. People shout to one another in crowded places. They communicate over electronic bullhorns and notes on bulletin boards. What is important is that some different kinds of protected channels be available. Variety is important. The fact that first class mail is protected does not mean that telephone lines do not need protecting.

2. *The channels should be "universal."*

   These protected channels must be easily available. A channel serving only a few selected urban areas, or one so expensive as to be unavailable to many people, cannot be said to be serving the broader social need for confidential communication, useful as it may be to the narrower community. This test will grow in importance because communication systems are becoming far more "tailored" than they have been in the past.

   In the past, a big city corporation used the same telephone system and the same first class mail system that a poor rural farmer used. Currently, technology is moving toward a proliferation of private and public specialized services that are tailored to specific needs. The security of these systems may be of public interest and need protection. Nonetheless, protecting these specialized channels does not necessarily answer the need to also provide security to me-
dia more broadly available to the public.

3. **The channels must offer some innate security.**

   Providing legal protection for channels that are inherently wide open to eavesdropping, with which the user is essentially shouting from the rooftops, is futile. In some cases — the electronic bullhorn or a bulletin board in a public area — the openness is obvious to any speaker and listener. With other technologies, such as cordless phones which can be overheard on a nearby FM radio receiver, the exposure is less apparent, particularly to individuals who are not experts in the technology or those on the other end of a phone line who are unaware of the type of phone they are using.

   The security need not be very strong. The glue on a first class envelope does not deter a person determined to open it surreptitiously. However, in contrast to the post card, the envelope does require some effort to open. A seal must be broken. The seal, thus, announces the intention of the sender that the letter be treated as a private communication. Coupled with the first class postage, the letter notifies a potential intruder that the message has legal protection under federal law.

4. **The protections are predictable and known.**

   One of the common concepts stemming from wiretapping legislation is “expectations of privacy.” Could the participants in a communication act as if they expect that their message is private? Is that expectation a reasonable one? Did they use a channel, such as first class mail that provides known protection, or at the other extreme, did they post messages on a wall along a public road? The law offers protection only to people who take steps to protect themselves.

   The corollary of this expectation, however, is that a communicator must be aware of the vulnerabilities of a medium. For example, if a phone conversation has less protection when carried over a microwave or other radio link than when carried over copper wire, a communicator would need to know which medium he is using in order to choose the appropriate one. Without knowledge, users cannot act in their own interest. This information, however, is not generally available because the phone company routes transmissions among various media based on their own constantly changing priorities.

   Another type of problem is that new services, such as electronic mail, may appear analogous to old ones, but not enjoy the same protections. When the postal service was marketing the now-defunct ECOM electronic mail service, it was defined and marketed as a
form of first class mail. Yet at two steps of the process, the message was in printed form, open to inspection, and handled by postal service employees. If the service lasted long enough, a case would likely have arisen regarding a law enforcement request to stand at the elbow of postal employees and scan ECOM messages. Would the courts have protected ECOM as first class mail, or would they have declared it to be a new messaging medium with no statutory protection? It seems reasonable to assert that citizen’s expectations of confidential communication should not depend on their degree of technical literacy nor be based on choices that are out of their hands.

5. \textit{Claims for a right to eavesdrop must be balanced.}

Unless the government grants absolute privacy protection, some formal mechanism is needed to adjudicate the legitimacy of demands of others for access. Standards need to be established and, in some instances, a proper authority for deciding must be assigned.

If the claimant is a government agency, tradition argues for a formal procedure to weigh claims on a case by case basis. In the other situations, it may be possible to negotiate between parties utilizing certain \textit{a priori} principles as guides. For instance, many employers now have the technological means to monitor their employees. It is currently an open question whether law or a less restrictive, privately arranged covenant would be more effective in balancing employee privacy against employer rights to monitor performance in the workplace. In the United States, such private codes and agreements now cover data base privacy in the private sector.

\textbf{THE TECHNOLOGICAL REVOLUTION}

Just as microelectronics transformed computers, communications technology has also burgeoned. Satellite and optical technologies have also played a critical role in the transformation. Together, they changed profoundly what kinds of information communications networks carry, how they carry it, and what happens to it within the network.

There are many ways to characterize technological change in communications. Four characteristics are particularly pertinent to privacy and confidentiality.

1. \textit{Digitally coded information.}

Communications engineers, if asked, might say that the most important change taking place in their field is “digitization.” Digi-
tization refers to a basic change in the way information is coded for transmission through communication channels. Many media, such as telephones, radio, and phonograph records were originally intended to carry sound. In older “analog” encoding, content was reproduced in these media in a wave form analogous to the original sound. In a phone line, electrical voltage rose and fell in a pattern like a sound wave. On a record, the groove tracked by the needle moved back and forth, again in a pattern analogous to the original sound. Digital encoding, however, corresponds to the way information is processed by computers. This new technology converts all information to a stream of discrete numbers encoded as discrete pulses called “bits” (somewhat similar to the way in which Morse code converts letters in the alphabet to discrete series of dots and dashes).

To engineers, digital encoding means more efficient, accurate, and reliable communication, but with many other important implications. For instance, in digital encoding, all information “looks” the same to the network. Computer data, voice, video, electronic mail, or facsimile images, all travel over the channels as a stream of information bits. Unlike analog encoding, which required a separate medium for each communication device, digital encoding uses a common format to form a single communication network.

2. “Intelligence” in the network

Since digital data is a form directly usable by computers, digital transmission has allowed the computer to be embedded in the communication network. These computers control the flow of information as it moves from point-to-point through the network. In addition, these computers can also modify the form and even the content of the information. Finally, these computers can also store the information. Even so-called “signalling” information — the information generated by the system that describes the communication and establishes its path from sender to receiver — is itself now stored and transmitted around the network in digital form.

The incorporation of computer intelligence into the communication system opens up a wide variety of new services and modes of operation and changes the way in which old ones can be delivered. It also vastly increases the ability of the network to collect and retain information about the messages that flow through it. Both of these changes in the network have important privacy implications, as we will see later.

3. Growth in electronic transactions

As communications technologies have changed, the services of-
ffered over them become central to the commercial processes of our society. In addition, the every day transactions of life are increasingly captured and communicated electronically. Examples include: banking at automated tellers (ATM’s) that are connected with the central computer system of the bank, often through a network that services multiple banks and bank cards; routinely processing credit card sales on automated readers at the store so that the reader can check for credit availability and record sales on a remote computer serving that card; selling items over cable television channels by use of the telephone; and when two-way cable is more common, the entire transaction will take place over the cable network. Beyond retail applications, business is now moving toward what is called the “Electronic Data Interchange” through which most commercial transactions among firms—orders, invoices, payments, and so on—move electronically, using no paper.

Most of the transactions mentioned above concern finance—the exchange of funds, and automation of sales transactions. The network, however, will soon carry the more textual material of commerce, bids and offers, acceptances, contracts, and so on. Virtually anything that now exists on paper and moves physically will probably move electronically in the near future—doctors exchange X-rays and medical records, schools exchange transcripts and test scores, and scientists exchange experimental data.

4. Industrial change — Privatizing

Finally, due to many factors, including deregulation and the introduction of competition in the phone industry, the ownership and control of communication networks became very complex. These and other changes mean that a communications system is now a complex assembly of technology and institutions put together and operated by a wide variety of firms.

A simple transaction may start at a terminal owned by the originator, pass through a local network, then a private or public switched network, a long distance line, and another sequence of regional and local networks at the other end, until it arrives at the receiving terminal. For some applications, the message may have been diverted to a computerized information service offered by someone else. In such a situation, questions such as where a message is located, which legal jurisdiction it occupies, and who is responsible for it can be difficult, even impossible, questions to resolve.

**Policy Challenges**

Technological change has challenged privacy law in several
Communications Technology

ways. Examples in this section will show three ways in which policy needed to adapt.

Wiretapping—Legal Bypass

The first automated telephone switch was allegedly invented by an undertaker who was concerned about operators intercepting calls from potential customers and redirecting them to his competition. Clearly, users are always concerned over the confidentiality of telephone calls. Section 605 of The Communications Act of 1934 affirmed the desire to keep phone calls private with the words, "[n]o person not being authorized by the sender shall intercept any communication and divulge . . . the content." No specific legislative history exists for this section, but the Supreme Court ruled in 1938 that the words prohibited all wiretapping, even when conducted by the federal government. Congressional attempts to clarify the status of federal wiretapping failed, but the government continued the practice, arguing that section 605 did not prohibit wiretapping per se, but it prohibited the interception of information together with divulgence outside the government.

In 1968, Congress enacted the Omnibus Crime Control and Safe Streets Act of 1968 ("Act"). Reacting to both growing public concern over government surveillance and the perceived need for government investigative agencies to intercept communication, Title III was inserted in the Act to "[protect] the privacy of wire and oral communications, and . . .[delineate] . . . the circumstances under which the interception of wire and oral communications may be authorized." The Act protects the privacy of oral conversations in situations where the person has an "expectation" of privacy, and provides strong criminal penalties for unauthorized surveillance. Controlled exceptions are made for; 1) law enforcement; 2) monitoring by the telephone company for service quality; and 3) conversations in which one party has consented to surveillance. In addition, the law enforcement exceptions are subject to strict procedural requirements, and a court order is mandatory.

Another law that deals directly with the privacy of conversations is the Foreign Intelligence Surveillance Act of 1978 ("FISA"). This law covers interceptions for foreign intelligence and domestic counter-intelligence purposes. FISA is broader than the Crime Con-
trol Act because it covers a wider range of communications. It is, however, more restricted because it applies mainly to surveillance for foreign intelligence purposes.

Despite these legislative efforts, the protection that Congress clearly intended remained short-lived and ambiguous because the technological revolution in communications had already begun. The vulnerability of the Omnibus Crime Control Act lay in the application to "oral" (voice) and "wire" communications. The Act also refers to "aural" interceptions. As a result, other types of content (computer data, electronic mail, transactions, and even video) and radio-based media (cordless and cellular phones, etc.) were not covered. In addition, courts were not inclined to extend the concept of "aural" interception to include digitally encoded transmission.2

As a result, even normal voice telephone communication, electronic mail, and computer data transfer rapidly moved out from under coverage of the law. If Congress was to see its previously expressed intent to protect electronic communication survive, it needed to take remedial action. Congress, therefore, aware of this growing gap between intent and effect, crafted a law that it hoped would be more resistant to technological change. On June 23, 1986, the House passed H.R. 4952.13 This bill eventually became the Electronic Communications Privacy Act ("ECPA"),14 which the President signed into law on October 21, 1986. The ECPA extended protection to most electronic communications by outlawing unauthorized interceptions and creating a system for authorizing official interception.

In drafting the bill, Congress dealt with three basic concerns: (1) criminal justice agencies concern that their ability to conduct investigative surveillance would not be unduly hindered; (2) radio amateurs and CB scanners concern that their existing, and historically legal, freedom to monitor public airwaves would not be taken away; and (3) finally, in what seemed to some to be a tangential issue, concern over whether or not to sanction private interception of cable satellite signals.

The last two concerns illustrate the value conflict that arises when stringent restrictions threaten those listening to "public airwaves." Basically, common carrier technology and its traditions of privacy has moved into competition with broadcast technology and its tradition of open airwaves. The telephone system has for many

12. Courts puzzled many technologists with a legal distinction between what were essentially only different encoding techniques, internal to the system and transparent to any user.
13. The Senate passed an amended version on October 1, 1986.
years used microwave for long distance carriage of voice. However, microwave operates as a beam along a line; and therefore is not useful for broadcast. Now, some cordless phones broadcast in an FM spectrum, and some cellular telephone channels operate in television frequencies. Satellites are hybrid, carrying both telephone and television programming. Although satellite transmission of television is intended as a distribution to broadcast stations and cable head ends, the beam covers a large amount of territory and can be picked up by relatively low cost dish antennas.

The ECPA strives for balance in several ways. First, it expands coverage to a wide variety of new electronic applications and technologies. It extends protection to private networks and covers electronic mail and transactional information when it is stored in the system, not just when it is in transit. In return, the law adds flexibility with regard to criminal justice requests for wiretaps and other electronic surveillance. For instance, the law extends the number of felonies accounted for and expands the number of officials who can request taps.

The ECPA made other accommodations to the radio spectrum. The radio link for cordless phones was exempted. Unauthorized interception of satellite transmissions known and intended to be private was proscribed, but the right to receive unencrypted signals intended for rebroadcast was established for private use.

Technology creates new opportunities for monitoring.15

The case of ECPA is one of the clearest examples of technology sidestepping legal purpose and legislation forcefully reestablishing these purposes. The next example, employer surveillance of employees, does not yet have such a clear resolution, and may take many years to achieve one. In this case, technology has not sidestepped precedent; rather it has provided new monitoring capabilities for which few or no precedents exist.

Building computers into telephone systems incorporates far more "intelligence" in the network. Switches, the devices that direct traffic through a network, are now digital computers, ranging in size from huge central exchange switches to small, office PBX's. Since they are computers, they can do far more than switch messages. For example, these digital computers can recognize patterns, process information, store it for later use, and print out reports detailing activity on the network. These capabilities mean that the switch can be used to monitor phone usage automatically and selectively.

Furthermore, many of these local switches are owned and operated by the firm, not by the phone company. Hence, the employer is monitoring his own system rather than the public switched network. This important distinction allows the employer access to the full capabilities of the switch.

Finally, due to the steady growth of office automation, more work is done by more employees on the communication system. The future of office work is not using just the telephone, but full office systems for word processing, shared desk calendars, information retrieval, electronic mail, and so on, all carried through a local network controlled by a company owned and operated switch. As a result, millions more employees at every level of the corporation (as well as more of the work they do) are exposed to supervisory monitoring.

Traditionally, there has been little legal protection of employee privacy on the job. In the first place, work is done on the employer’s premises. Secondly, the employer owns the phone system and it is the firm’s business that is, in theory, being conducted over the system. Finally, the employer is reasonably considered to have an interest in and a right to monitor work done by employees, to ensure quality and quantity and to protect against theft and fraud. Therefore, under federal law, an employer may place a television camera on the shop floor or monitor telephone service.

The policy question is whether technology has shifted power to the employer to such a degree that balances have now become necessary between employee privacy rights and employer needs for monitoring. Those balances may be struck through federal or state law, civil law, or as the result of contracts or voluntary agreements on standards of practice in the private sector.

To date, little has been done to establish any protections. One of the problems is that modern technology has provided a wide variety of monitoring and surveillance tools. Some of these tools are information technology, but many are not. Drug testing, AIDS testing, genetic testing, polygraph, voice stress analyzers, psychological testing, and so on are only a few of the other technologies available to supervisors for use with their employees.

As a result, Congress has been asked to consider the issues raised by these technologies on a piecemeal basis. Bills restricting employer use of the polygraph have passed both houses (as H.R. 1212 and S. 1904) and have been signed into law this year. A bill requiring a beeper tone during telephone service monitoring is under

16. An interesting exception is the case of federal employees. Since the employer is the federal government, employees have protections against unreasonable searches under the fourth amendment to the Constitution.
consideration in the House of Representatives. The likely result of such case-by-case treatment is two-fold. It may lead to uneven treatment of comparable technologies, creating incentives to use other, less restricted technologies that may be equally or even more intrusive. For instance, restrictions on the use of polygraph may lead to increased use of psychological testing, voice stress recorders, or even controversial techniques such as handwriting analysis or astrology. Since most technology (sound or not) moves faster than the legislative process, treating particular cases can resolve only the most egregious problems.

Secondly, this type of policy response cannot deal with the overall cumulative effect of surveillance — that is, the growth of an oppressive workplace characterized by surveillance of phone calls and desk terminal use, urine and blood screening, psychological testing, video camera, and even brain wave monitoring. The negative impact of this combined surveillance on the dignity and autonomy of workers could be far greater than the sum of the individual parts, and provide a strong case for legal intervention, especially for workers with little bargaining power. Technology could be offering the tools for building a surveillance society in which everything people do and are as human beings is an open book to those who assert some “right” to monitor them.

Policy designed to protect employee privacy could take many forms, but a look at past developments of information privacy law suggests that three broad principles might guide its formation.

1. Use the least intrusive means to achieve the result.

Given that some legitimate reason exists to test or use surveillance methods on an employee, privacy interests would dictate that, other factors being roughly equal, the employer use the least intrusive method to achieve the desired goal, whether improving efficiency, controlling errors, stopping misuse of long distance lines, or improving the quality of customer service.

“Intrusiveness” could be measured in terms such as: Is physical intrusion of the body or collection of body fluids or tissue necessary? Is the procedure collecting more information than necessary to the particular purpose? Does the information collected extend beyond behavior at the workplace? Does the information collected include or permit inferences about political, religious, or other personal information that is traditionally granted particular protection in our society?
2. **Balance the degree of intrusiveness against public interest.**

Few would disagree that it is more important that an airline pilot be unimpaired by alcohol or drugs than that a gardener be clear headed, more vital that a senior employee in an intelligence agency be resistant to temptation than is a file clerk in a large civil bureaucracy. We want to be able to make distinctions among types of work and threats versus the intrusiveness of surveillance. Avoiding threats to public safety might outweigh protection of physical assets, which might outweigh improving customer service. Consequently, different degrees of intrusion would be acceptable, depending on the weighing of these public values.

3. **Apply “fairness” principles to surveillance and the data.**

Finally, if some form of employee surveillance is to be conducted, a set of principles needs to be agreed on to ensure fairness and concern for the dignity of the employees. Some questions that might be considered in setting those principles are: Should surveillance be secret or does the employee always have the right to know that he or she is under observation? Does the employee have the right to refuse the test of the surveillance? What are the penalties for so doing? What actions are to be taken based on the results of the surveillance? What rules cover the handling of the data collected by the surveillance? Is it destroyed, or is it preserved in the files of the personnel department, in the health department, or elsewhere? Is it reported outside the firm to some third party -- the press, law enforcement authorities, other potential employers, insurance companies, and so on? What rights does the employee have to challenge a finding or request further tests?

Clearly, the problems of privacy on the job transcend mere communications, computers, or other information technologies. However, this article argues that they all need to be solved within the context of some general "code of employee privacy protection." This code acknowledges the needs and rights of employers to know what is going on in their establishments and how their employees are working, but also establishes acceptable limits and procedures for determining what may be done, rules for the conduct of the monitoring, and policies for the handling of the data.

**NEW VULNERABILITIES AND TECHNOLOGICAL PROTECTION**

The final example is concerned not with direct federal protec-
tion of privacy, but with the role of the federal government in providing technology for securing communications to users in the private and public sectors.

Why the problem?

Communications systems are beginning to carry information of significant value. As technology develops, this will dramatically increase. By the turn of the century, most payments will be exchanged in electronic form between financial institutions and among their customers. Furthermore, other commercial transactions such as bids, offers, acceptances, and even contracts, will be negotiated and even "signed" electronically. Phone lines carry a wide variety of other commercial information of value, such as financial information, engineering designs, formulas, production schedules, and marketing plans.

Much of this information is highly valuable, both to the owner and to possible eavesdroppers. Using channels that are legally defined as private, but that only have some minimal technical protection, therefore, would be insufficient. Some users need access to more sophisticated techniques for protecting their information assets. Protection is not the only requirement. To engage in commercial transactions electronically, we need methods for authenticating sources, "signing" and dating documents, and "sealing" messages. These technologies are, for the most part, some form of encryption — transforming them in such a way as to be unreadable until they are decoded with a "key."

Why Government?

In general, if a market for something exists, we usually expect that firms will appear to meet that need without government intervention. Yet, in this case, the federal government is already deeply involved in policies that affect the ability both of firms to develop safeguards, and of users to employ them. For example, in the area of communication security, the government has expertise that may be generally hard to duplicate in the private sector. Military and diplomatic offices are primarily concerned with high level communications security to protect the transmission of very sensitive national security information.

Also, some standardization and certification is necessary. If information systems must interconnect easily with each other, then security techniques, especially those that encode information, need to be compatible. If users know the connection well in advance, and that it will not change from day to day, then a locally chosen, idio-
syncratic technology satisfies their needs. But if users must interact with any of a number of terminals, owned by different organizations, in order to establish a link at any time, the coding techniques must be predictable and known. In addition, since encryption is an extremely sophisticated technology, most consumers have no practical way to evaluate the level of protection offered by any device on the market. These problems both suggest that users need some form of standard and certification system to assure the level of protection they install.

Finally, while some national security applications of safeguarded technologies are classified, some government agencies are sensitive about the export of non-classified technology. In addition, to the extent that certain government agencies engage in the interception of foreign communications, otherwise known as signals intelligence, they have a natural interest in assuring that highly effective encryption not be easily available to those targets of interest. Export controls cover non-classified technologies, including encryption devices. These controls are an important consideration for a multinational corporation needing to communicate with foreign sites.

A Different Type of Balance

Although a general consensus exists that the government should play a role in providing safeguarded technology because of both the vital need in the community and special expertise of the government, it still needs to strike another type of balance. This balance, involving the conflicting interests of national security interests, civil government users, and private sector users, needs to be struck in three areas.

Research & Development Funding and Publication

The state of the art in security technology continues to improve, mostly in response to similar advancements in the ability to penetrate the barriers created by similar advancements in that technology. Debates have arisen over the proper role of the government in funding research and in controlling the publication of results. Should the government encourage research in the private sector or should it restrict such developments mainly to government research laboratories? Should basic science agencies such as the National Science Foundation fund security research, or should it confine its support to agencies such as the National Security Agency that have specific charters that protect communications? These questions are still unresolved and under debate.

Because of the technical nature of cryptography, basic research
Communications Technology

in computer science and mathematics can have direct application to security techniques that make it very difficult to keep basic civilian research cleanly separated from defense work. As a result, even when the work is not classified, or defense agencies do not fund it, the government has attempted to restrict publication. These attempts at restriction include classifying patent applications and invoking the International Traffic in Arms Regulations ("ITAR") and other export control laws that restrict the export of technical data.\(^{18}\)

Standards and Advice

Congress and the executive branch have heavily debated the issue of whether they should concentrate the standard setting and advising roles, both with the private sector and civil agencies, in the National Security Agency ("NSA"). Giving the NSA this responsibility would certainly provide strong protection of defense interests. Opponents argue against it on three grounds. First, the NSA would conduct an area of standard setting critical to the private sector at least in partly in secret, with no or limited opportunity for public input and debate. Second, that type of control over civilian and civil government communications is inappropriate for a defense agency. Third, defense agencies do not necessarily have the expertise in or sensitivity to private and civil sector needs. In fact, given a signals intelligence mission, they have incentives not to provide strong, effective technologies to the outside world.

Both the NSA and the National Bureau of Standards ("NBS") had responsibilities in the past for developing standards and advising the civil authorities on the use of secure technology. For example, the NBS developed and promulgated the Digital Encryption Standard ("DES") in 1977.\(^ {19}\) This work was based on an algorithm developed by IBM, and the NSA consulted closely with the NBS in the development of the algorithm.

More recently, a presidential order, National Security Decision Directive 145 ("NSDD 145"), vested control over developing and approving standards in the hands of NSA. Congress subsequently passed the Computer Security Act of 1987.\(^ {20}\) This puts responsibility for private and civil sector security in the hands of the NBS and

---

18. For a more detailed history and current status of the debate over publication controls, see Wilson, Federal Control of Information in Academic Science, JURIMETRICS, 283-96 (Spring 1987); Landau, Primes, Codes, and the National Security Agency, 30 NOTICES AM. MATH. SOC., 7-10 (January, 1983); Weingarten, Controlling Cryptographic Publications, 2 COMPUTERS & SEC., 41-48 (January, 1983).


attempts to re-establish balance. Of course, until the Computer Security Act is interpreted and implemented by the administration and some experience has been gained, the degree to which a balance has been struck will be open. It is not an issue that has been resolved easily in the past.

**Exports**

United States policy also affects the development and use of security technologies through export controls. The primary purpose of export controls is to deny advanced technology with military uses to potential adversaries. Controls, however, can also have negative affects on United States interests, both by denying markets for producers and by denying multinational firms the ability to use them in their own operations.

A multinational firm, such as a major bank that operates a world-wide communications network and wishes to secure it, faces a serious problem because restrictions can prevent export of encryption technology for installation at the foreign end of the line. There is some degree of irony to this conflict of interests. While national security is invoked to prevent the export, the very same purpose would also favor protecting sensitive international United States commercial communications.

Congress has attempted to relax restrictions, particularly in cases where alternate and comparable foreign technology is available. For example, some types of devices based on the DES can be exported, although they are on a control list and require a license for export. The NSA recently proposed a standard to replace the DES, and would not allow this new standard’s export. This disallows its use in international banking.

**Conclusion**

Given the proliferation of communication-based information systems, policies to preserve the privacy of information stored in data banks are useless unless the confidentiality of the communications are protected. But it has become a complex policy problem. Past attempts to protect communications privacy are undermined by rapid changes in technology. In addition, major improvements in monitoring capabilities have created entirely new and unprecedented issues. Resolving some of the policy problems has also brought defense and national security arguments into the privacy debate in a major way.

On the other hand, unlike the data privacy debate that has
tended to pit private interests against those of the commercial sector, in this case both interests appear to coincide. The same policy that serves to protect personal privacy on a phone line also protects the commercial transfer of valuable assets. The passage of ECPA illustrates that alignment because the ACLU, banks, and the information industry all supported the legislation. Similarly, civil liberties groups and commercial interests also supported the Computer Security Act. It may be that these debates have been a starting point for a broader consensus on the need for protecting privacy in an "information age."