Chapter 4

Electronic Mail Surveillance

Chapter 4

Electronic Mail Surveillance

SUMMARY

The public expects and is provided with a high standard of protection against unauthorized opening of first-class letter mail when in paper form and delivered by the U.S. Postal Service. Constitutional provisions, case law, and postal statutes and regulations collectively provide such protection. However, when mail is sent in electronic form, the existing protections are weak, ambiguous, or nonexistent.

Electronic mail is a relatively recent marriage of computer and communications technology that makes it possible to send, transmit, and receive mail in electronic form. If desired, the electronic output can be printed out in hardcopy and delivered by the USPS or private carrier. But electronic mail also permits terminal-to-terminal communication where the message is never in paper form. Various private companies now offer electronic mail services.

OTA found that there are several discrete stages at which an electronic mail message could be intercepted and its contents divulged to an unintended receiver:

1. at the terminal or in the electronic files of the sender,
2. while being communicated,
3. in the electronic mailbox of the receiver,
4. when printed into hardcopy before mailing, and
5. when retained in the files of the electronic mail company for administrative purposes.

At each of these stages, OTA found that technological protections vary. Some, like encryption, are still perceived as relatively costly and difficult, though becoming less so. Existing law offers little protection. Portions of the Communications Act of 1934, Title III of the Omnibus Crime Control and Safe Streets Act of 1968, Postal Reorganization Act of 1970, and Foreign Intelligence Surveillance Act of 1978 may apply to some portions of the electronic mail process. But overall, electronic mail remains legally as well as technically vulnerable to unauthorized surveillance.

The interception of electronic mail at any stage involves a high level of intrusiveness and a significant threat to civil liberties. The investigative value of intercepting electronic mail will vary. But, traditionally, paper mail has been afforded a high level of protection from interception.

OTA identified three policy options available to Congress:

1. legislate a high level of protection across all stages of the electronic mail process so that electronic mail is afforded the same degree of protection as is presently provided for conventional first class mail;
2. legislate different levels of protection at different electronic mail stages; and
3. do nothing at present, pending further technical and case law developments.

INTRODUCTION

Written communications that are sent between two parties via first class mail receive a high standard of protection against unauthorized opening. This has been well established by both case law, 13x *Parte Jackson* (1877),[1] and postal statutes and regulations. More and more often, however, substantive communications between two or more parties are not written and sealed in an envelope, but are being typed into a computer system and sent by means of telecommunications. The merging of computers and telecommunica-

[1] Upheld the requirement of search warrants as a condition for opening sealed mail. Applied fourth amendment protections on that class of mail for which customers pay a certain rate to send in a sealed envelope or package.

tions opens up many possibilities for faster, cheaper, and more accurate communications. However, it also raises many questions about privacy and the security of such communications against unintentional or intentional tampering.

When electronic mail is being transmitted in data form across wires, it does not come under the purview of either Title III of the Omnibus Crime Control and Safe Streets Act of 1968, which prohibits only aural interception, or Section 605 of the Communications Act of 1934, which prohibits interception of radio transmissions. Interception of digital messages for purposes of learning the contents or altering them is prohibited by the criminal provisions of the Foreign Intelligence Surveillance Act (FISA); however, the scope of such prohibitions is unclear. When electronic mail is in the computer memory of the sender or receiver, there are presently no specific Federal laws prohibiting acquisition of that information, although theft laws may apply as might the Computer Fraud and Abuse Act of 1984 with respect to Federal computers. Moreover, it can be argued that an individual would have a fourth amendment expectation of privacy against Government access to the message. If the message was printed into hardcopy and mailed, then the postal statutes should protect the confidentiality of the message. If the electronic mail company retains a copy of the message for administrative or backup purposes, the individual may have no legal recourse to protect the information from additional access.

BACKGROUND

During the last few years, electronic mail began to develop a significant commercial market. It is expected that market popularity will increase as competition brings prices down and more services and improvements in existing services, especially in the connections between personal computers and electronic mail systems, are offered.[2] The main attraction of electronic mail is that it reduces, if not eliminates, time that is spent in exchanging information over the phone or via the U.S. Postal Service or a courier service. The current adage is that electronic mail eliminates telephone tag. With time, however, the major part of the electronic mail market may be substantive messages, e.g., documents and working papers that would normally be sent through the traditional mail system. Informal messages that would normally be conveyed via phone calls may, in the long run, account for a smaller part of the market.[3]

There are currently a number of providers in the electronic mail marketplace. The U.S. Postal Service (USPS) was an early entrant into the electronic mail market offering two services: E-COM (Electronic Computer-Originated Mail), which was aimed at the domestic business market; and INTELPOST (International Electronic Post), which provides high-speed facsimile service by satellite between the United States and Europe. E-COM has been terminated, and INTELPOST, while still operating, is little used.[4]

Commercial ventures in the electronic mail market have proven more successful and more varied. MCI is now one of the largest electronic mail companies offering both direct computer-to-computer messaging and mixed systems that combine electronic input and transmission with hardcopy output and delivery. One reason MCI can offer inexpensive ef-

[2] *See EMMS Newsletter,* May 1, 1985, p. 1.

[3] David Roman and Stan Writen, "Electronic Mail: Faster Than a Speeding Bulletin," *Computer Decisions,* July 1984, vol. 16, No. 9, pp. 146-160.

[4] See James Bovard, "Zapped by Electronic Mail," *Across the Board,* June 1985, p. 42; House Committee on Government Operations, "Postal Service Electronic Mail: The Price *Still* Isn't Right," House Rep. No. 98-552, 1983; and House Committee on Government Operations, " I NTELPOST: A Postal Service Failure in International Electronic Mail," House Rep. No. 98-675, 1984.

ficient services is that it owns a low-cost, long-distance telephone network.[5] In the spring of 1984, Federal Express entered the electronic mail market with its Zapmail service which provides 2-hour delivery of facsimile copies for up to five pages of text. ITT has targeted its DIALCOM services, including computer-to-computer electronic mail, telex, telegram and courier delivery, into large corporations and the Federal Government. The White House, for example, uses DIALCOM for electronic mail communications with some 22 Federal agencies. GTE Telemail has also been successful in the corporate marketplace. The Source and CompuServe provide an array of computer information services, including electronic mail and various electronic bulletin boards.

As generally used, electronic mail refers to messages that are sent between computer terminals via telephone lines.[6] This does not merely include terminal-to-terminal systems, but also can be interpreted to encompass telegraph, telex, teletext, facsimile, voice mail, and mixed systems that electronically transmit messages, some of which may be subsequently delivered by the postal system or a courier service. A brief description of each of these is presented below:

. Telegraph: A system that transmits one-way electronic messages along circuits within a network of central and branch telegraph offices, where the electronic messages are translated by the receiving operator into typed messages that are hand delivered or telephoned to the recipient.

- Telex: Commonly used for international communications, this telegraph exchange system consists of: a teletypewriter terminal to translate and interpret messages into code; special telegraph circuits designed to carry the code; and a teleprinter to print the communication. Each subscriber is individually issued his or her own telex line and number that a caller dials to send messages that are keyed into the teletypewriter terminal. The message is then transmitted to the receiver's automatic teleprinter. For international telex communications, satellite channels or transoceanic submarine cables are used.

  Current Telex systems, such as the "InfoMaster," can offer delayed message delivery and a multiple address message system, while "FYI News Service" subscribers can receive general news, financial, market, and weather-related bulletins.
- Teletext: This communication system delivers text and graphic messages sequentially in one direction over a television broadcast signal or cable which are then received by a display terminal, like a television set. The receiving terminal exhibits the message on the display screen, and can store or delete the message after viewing. Similar systems that can receive as well as send messages (e.g., home banking or shopping) are known as videotex.
- *Facsimile:* Unlike the telex, this system converts a page of text or images into data. Once the input data is scanned and translated into code, ordinary telephone lines can carry the transmission to a recipient's terminal to be decoded and printed for hardcopy distribution. As an added feature, some facsimile machines, such as the "FaxPak," offer store-and-forward capability.

  A typical facsimile system can transmit a page in 4 to 6 minutes, while more advanced systems can transmit the same amount of information in a few seconds.
- *Voice Mail:* Voice mail is a computer-based system designed to digitize voice from an analog signal for the purposes of relaying short messages or instructions. Like a sophisticated digital phone-answering machine, messages can be stored and forwarded, edited, retrieved, or distributed to a list of users. Future systems are being designed to incorporate options such as voice to text conversion.
- *Electronic Mail:* This computer-based message system can be divided into two categories. In the first, an electronic message is transmitted between two or more

[5] See Bovard, op. cit., p. 46; and Lawrence J. Magid, "Electronically Yours," *PC World,* June 1984, pp. 48-54.

[6] Bovard, op. cit., p. 42.

terminals and remains in an electronic format. In the second, the message is transmitted electronically, but then converted to a hardcopy format to be delivered by traditional mail or courier service. To use a typical electronic mail system, a personal identifier number, password, the recipient's account number, and message are keyed into a terminal. This information is transmitted to a central computer and stored for viewing at the recipient's convenience. Electronic mail systems can send, receive, file, recall, edit, and store textual or graphic messages.

- *Electronic Bulletin Board:* An electronic bulletin board is an electronic mail service (or the equivalent computer-based information service) with a public or private electronic mailbox that is accessible to several persons. A public bulletin board usually is open to many or all subscribers and/or persons with a general password. A private bulletin board is limited to persons with special passwords.

The emergence of electronic mail has raised a number of policy issues, for example: what standards should be used so that competing electronic mail systems can be compatible; should regulations for common carrier systems and private systems be the same or different; and what range of services can or should electronic mail systems offer?[7] Such issues concerning market structure, services, and regulation are beyond the scope of this report. However, issues concerning the security and privacy of electronic mail systems are germane to this study. Indeed, some believe security and privacy issues are critical to the widespread acceptance of electronic mail as a communications medium. The contents of electronic mail communications are of interest to the same parties that are interested in the contents of first-class mail communications. Thus, Government officials might be interested in accessing or maintaining surveillance of electronic mail messages for investigative purposes. Private parties might be interested in electronic mail surveillance for various competitive, personal, and/or criminal purposes.

[7]For discussion of telecommunications and industry structure issues see Raymond R. Panko, "Electronic Mail," *Datamation*, vol. 30, No. 16, Oct. 1, 1984, pp. 118-122; Robert E. Kahn, Albert Vezza, and Alexander P. Roth (eds.), *Electronic Mail and Message Systems–Technical and Policy Perspectives* (Arlington, VA: American Federation of Information Processing Societies, 1981): and issues of *EMMS Newsletter*.

FINDINGS AND POLICY IMPLICATIONS

1. There are at least five discrete stages at which an electronic mail message could be intercepted and its contents divulged to an unintended receiver: at the terminal or in the electronic files of the sender, while being communicated, in the electronic mailbox of the receiver, when printed into hardcopy, and when retained in the files of the electronic mail company for administrative purposes. Existing law offers little protection.

From a policy perspective, the laws that might be extended or drafted will vary by these five stages because of the historical development of telecommunications and privacy law. Moreover, the technological protections that are available will also depend on the stage of the communications process. Therefore, each stage needs to be analyzed separately to discern policy problems and policy options."

Terminal or Electronic Files of Sender.–At this stage, messages could be intercepted by accessing the computer system of the sender for purposes of reading the message or altering its content. In the case of interception by Government officials, the individual would probably be successful in arguing that he or she had a fourth amendment expectation of privacy in the contents of computer files. Although these are not "papers" in the traditional sense, they are arguably the computer-age equivalent. They are also stored within a

[8]See *ACLU Focus Paper on Electronic Mail*, Jan. 29, 1985, for a similar discussion.

computer file that belongs to the individual, perhaps not in a tangible property sense, but at least in an intangible one, depending on the storage arrangement. If the computer was at home, the individual's expectation of privacy would be greater than if it was an office computer, but use of passwords and access codes would indicate that the individual took precautions at the office to ensure an expectation of privacy. The fourth amendment status of messages held in the computer file of the sender could be clarified by statute. The FBI reported that on the occasions where it has had to acquire information from a data bank, it secured a search warrant as it would have done before going into a residence looking for information.[9]

In the case of private parties accessing electronic mail in the terminal of the sender, there is no specific statute that would protect the confidentiality of the message. At this time, State laws probably offer more protection than Federal laws. Theft laws might apply under some circumstances, although these are framed in terms of physical breaking and entering, and in terms of tangible property. Computer crime laws may also offer some protection against unauthorized private access.

There are also some technical measures that can be adopted to protect the contents of a computer file. Sophisticated password and/or key systems can be used to deter unauthorized access. Audit trails can be developed to detect unauthorized access. Although such systems may not be foolproof, their use will give additional legal weight to someone arguing that their computer mail files are expected to be private.

In Transmission.—At this stage, messages can be intercepted by tapping into the wire over which the message is being sent, breaking into the fiber optic cable, or intercepting satellite or microwave signals. Regardless of the technology used to transmit electronic mail messages, existing law offers little protection against unauthorized interception. Title III of the Omnibus Crime Control and Safe Streets Act would not require Government officials to get a court order before setting up a tap because electronic mail is sent in digital form. Voice mail may be protected under Title III, depending on the interpretation accorded aural communication. (See chapter 3 on telephone surveillance.) Section 605 of the Communications Act of 1934 would not apply unless the electronic mail was being communicated via radio signals, which is rarely the case. Additionally, the purviews of Title III and Section 605 are limited to common carrier communications. Electronic mail systems that use private carriers, e.g., internal company mail systems, would not come under either act. The criminal penalties of the Foreign Intelligence Surveillance Act may prevent Government officials from intercepting digital communications, but it is unclear if these penalties apply to interceptions other than for foreign intelligence purposes.

Again, there are some technical measures that can be used to protect the integrity of a message during transmission. The message can be encrypted using the data encryption standard (DES) or some other code that scrambles or packages the message in a way that makes it difficult to decipher. However, encryption has been expensive and time-consuming on both ends, although costs are dropping.

In the Electronic Mailbox of the Receiver.—At this stage, messages can be intercepted by breaking into the computer terminal of the receiver, if the receiver has one that is used as an electronic mailbox, or into the computer terminal of the electronic mail company where an individual has rented his or her mailbox. In either case, the individual should have a fourth amendment expectation of privacy against Government interception. This expectation will be higher if the mailbox is in the individual's *own* computer terminal, but because renting implies property rights the expectation should also apply if the mailbox is held on the company's terminal. Protection against private party interception would depend on the coverage of theft laws and computer crime laws.

When Printed Into Hardcopy Before Mailing.—Once mailed, the contents of the enve-

[9]Floyd Clarke, remarks at OTA Workshop, May 17, 1985.

lope would receive the same protections that are accorded first class mail. However, there would be no legal protection for the message during the time it was being printed out and before it was put into the envelope. During this time the individual would be dependent on the policy of the electronic mail company and the discretion of its employees.

When Retained by the Electronic Mail Company for Administrative Purposes.-All electronic mail companies retain a copy of the message both for billing purposes and as a convenience in case the customer loses the message. Based on the reasoning in *United States v. Miller, 425* U.S. 435 (1976), where the Court ruled that records of financial transactions, including copies of personal checks, were the property of the bank and that an individual had no legal rights with respect to such records, it is possible that an individual would not have a legal basis from which to challenge an electronic mail company's disclosure of the contents of messages or records of messages sent.

The issue of the privacy of personal information retained by a third party is not unique to electronic mail. It is important to note, however, that access to the administrative files of electronic mail companies can reveal a great deal of information about an individual-the substance of communications, the record of persons communicated with, and the locations of sender and receiver.

The question of the legal status of electronic mail information retained by the company is presently before the courts in a case in which the Government subpoenaed transactional and substantive records of The Source (Source Telecomputing Co.) related to M.V.S. Associates, Inc., Elite Fleet, Inc., and/or Leo Radosta. Leaving aside the questions of the possibly excessive breadth of the subpoenas, the legal question appears to turn on whether The Source is merely the temporary custodian of records, in which case an individual can use fifth amendment protections to prevent disclosure.'" Regardless of what the courts may decide based on the facts in this case, the issue requires attention.

2. The interception of electronic mail at any stage involves a high level of intrusiveness and a significant threat to civil liberties. The investigative value of intercepting electronic mail will vary. But traditionally, paper mail has been afforded a high level of protection from interception.

In order to determine the implications for civil liberties of intercepting electronic mail and the governmental interest in such interception, the electronic mail process as a whole needs to be evaluated in terms of the dimensions developed in chapter 2 (see table 6). This will aid in determining if there is a level of protection against interception that should be guaranteed, regardless of the stage in the process at which the message maybe intercepted.

In terms of the nature of the information, electronic mail surveillance can include both the content of specific exchanges of information, and transactional information concerning the time of the communication and location of the parties. Both types of information may be of a personal nature.

Electronic mail communications generally are intended to be private communications between two parties or among a specified group. The technology employed will allow different degrees of privacy, i.e., personal computer to personal computer communications are inherently more private than electronic mail company to hardcopy delivery communications. Despite the variations in technology, electronic mail communications (including private electronic bulletin boards) usually are intended for private consumption, with the notable exception of public electronic bulletin boards that are open to a broad range of subscribers or users.

In terms of the scope of surveillance, interception of electronic mail communications can be quite broad depending on the extent to which electronic mail is used by a particular individual. Interception of a large volume of electronic mail communications may well be construed as a fishing expedition.

[10] See: *Couch v. United States, 409* U.S. 322 (1973) and *Bellis v. United States, 417* U.S. *85 (1975).*

It is very difficult for an individual to determine if electronic mail has been intercepted, regardless of the stage at which it is intercepted. While in the terminal of the sender or mailbox of the receiver, audit trails and passwords can help in detecting interceptions or attempted interceptions. While being communicated via the telecommunications system, it is virtually impossible for the individual to detect interception. If someone attempts to intercept the message while it is physically being mailed, the post office might detect such an attempt and, if so, might inform the individual. The individual's ability to detect interception of mail while it is retained in the files of the electronic mail company will likewise de penal on the cooperation of the company.

The pre-electronic analogy for electronic mail is probably quite direct—first class mail. Traditionally, first class mail has been accorded a high level of protection from interception.

The governmental interest in intercepting electronic mail will, of course, vary based on the purpose of the investigation, the degree of suspicion, and whether or not other means have been attempted to secure similar information. However, given the high threat to civil liberties posed by interception of electronic mail, it appears that the governmental interest in interception would have to be quite compelling.

3. OTA identified three policy options that are available to Congress. The first would be to legislate a similar level of protection across all stages of the electronic mail process. The second option would be to accord different protections according to perceived differential impacts on civil liberties at particular stages. The third option would be to do nothing.

These three policy options are briefly discussed below.

Option A.–Based on the analogy to conventional first class mail and the level of intrusiveness that interception of electronic mail entails, Congress could provide the same degree of protection for electronic mail that it presently provides for conventional first class mail. Using this as an operating assumption, Congress would need to pass legislation that included the following:

- Prohibition on unauthorized access to an individual's computer file or individual's electronic mailbox unless a court order has been obtained. Two levels of court order may be appropriate. For purposes of intercepting the contents of a file, a court order could be obtained for national security, domestic security, and law enforcement purposes if there is probable cause to believe the individual is implicated in illegal activity. For purposes of determining the transactions the individual engaged in, the requirements for a court order could be the same as for a mail cover (monitoring the names and addresses on the outside of the envelope). The same standards would apply regardless of whether the mailbox was in a personal computer or held by an electronic mail company.
- Prohibition on unauthorized interception of data communication. Although the analogy is still to first class mail, the vehicle for protection is more likely an amendment to Title 11 I that would protect all data communications transmitted over wire.
- Establish the rights of the individual and responsibilities of the company when information is retained by the electronic mail company. The "Subscriber Privacy' provisions of the Cable Communications Policy Act of 1984 may serve as a model. Although it is premature to judge the effectiveness of the "Subscriber Privacy" provisions of this act, comments on the enforcement scheme are in order. In general, the subscriber is dependent on the cable company for information regarding the potential conflicts between the company's practices and the individual's privacy. For example, the company is to inform the subscriber of the uses and disclosure of personally identifiable information. Practically speaking, this may just mean that at the time the individual signs

the contract, he or she is given a sheet of paper containing the company's general policies. The individual may or may not understand, or even read, the information.

The act does place restrictions on the cable company's collection and disclosure of personally identifiable information, but the restrictions are very vague. For example, "A cable operator may disclose such information if the disclosure is necessary to render, or conduct a legitimate business activity related to a cable service or other service provided by the cable operator to the subscriber." From a surveillance standpoint, the act does require a Government entity to obtain a court order for access to personally identifiable information. The court order must offer evidence that the subscriber "is reasonably suspected of engaging in criminal activity and that the information sought would be material evidence in the case. The individual must be given "the opportunity to appear and contest such entity's claim."

Option B.—Under this option, Congress could decide that stages one and three (the terminal of sender and electronic mailbox of receiver) should be accorded more protection because they involve places that are more Private and because it would be harder for individuals to detect interceptions unless they were maintaining fairly secure personal computing systems. Congress may not want to take any specific action with respect to the second stage (transmission), but leave it to the resolution of the aural limitation in Title III. Likewise, with respect to interception of information held by the electronic mail company, Congress may wish to treat, in a systematic fashion, all personal information held by third parties.

Option C.–Congress could continue to do nothing at this time and watch the development of the electronic mail market and evaluate case law development. However, there are costs in pursuing this option. The market developments seem clear and the time appears ripe for policy guidance before rights and responsibilities become more confused. Additionally, because of the number of stages at which electronic mail can be intercepted and the range of governmental interests in intercepting electronic mail, the case law development will most likely be very specific to the issues raised in particular cases, and will fall short of a national policy.