Chapter 6

Confidentiality and Security Issues With Office Automation

Contents

Chapter 6

Confidentiality and Security Issues With Office Automation

Protection of privacy or confidentiality in recordkeeping (and security measures to accomplish such protection) is a concern that has continued from the constitutional era of quill, pen, and copybook through the invention of the telegraph, telephone, typewriter, microphone, duplicating machine, large-scale manual filing systems, teletype, electric accounting machinery (EAM), and first-, second-, and third-generation computers. How much data about individuals and groups is needed? Who will use the data? How does one determine what information about oneself should or must be made available to others? What uses will be made of the information?[2] The third phase of office automation—small computers linked or networked—further raises these questions, as the ubiquitous placement of computing devices in offices gives more people more opportunities to access records.

[1]This chapter as a whole draws on a report to OTA, *Privacy and Security Issues in the Use of Persona) Information About Clients and Customers on Micro and Persona) Computers Used in Office Automation,* prepared by The Educational Fund for Individual Rights, Alan Westin and Lance Hoffman, principal investigators, 1985.

[2]Alan Westin, "New Issues of Computer Privacy in the Eighties," Proceedings *of IFIPS World Congress,* Paris, France, 1983.

PRIVACY, CONFIDENTIALITY, AND SECURITY–DEFINITIONS

Since analysts from various fields and disciplines write about privacy and security issues, there are differences in the use of terms and concepts by these practitioners. In the broadest sense, privacy is a set of values dealing with individuality, autonomy, personal space, and personal information.[3] Privacy deals with the rights of an individual to limit others' access to information about oneself, and the social or legal rules by which such claims are accepted or rejected in particular contexts. Viewed as a desirable attribute of the data and the way it is handled, this is better termed "confidentiality' '—the protection of privacy. Security deals with a data-collector's capacity to safeguard the existence and integrity of the data it has collected and to provide the proper degree of confidentiality as set by organizational or legal policy.

Confidentiality and security are related but not synonymous. Confidentiality addresses the use of data about individuals. Security is concerned with the accidental or intentional theft, modification, or destruction of data. Breaches of security may compromise privacy; for example, the theft of a mailing list stored on magnetic tape is a result of poor security and may compromise the privacy of individuals on that list. The breaches of security may also be unrelated to privacy or confidentiality.[4]

Respect for privacy in office automation involves three components:

1. Data collection—what personal information is relevant, necessary, and socially acceptable for an organization to collect to carry out its missions?
2. Protection—when should an organization record and preserve identified personal data, who should have access to it within

[3]For a general discussion of privacy and how it is defined and used in policy see, Priscilla M, Regan, "Personal Information Policies in the United States and Britain: The Dilemma of Implementation Considerations, *Journal of Public Policy,* vol. 4, No. 1, 1984, pp. 19-38.

[4]A representative discussion by EDP experts of the relation between privacy and security considerations appears in Alexander Gaydasch, Jr., *Principles of EDP Management* (Reston, VA: Reston Publishing Co., 1982).

the collecting organization, and under what circumstances can it be released outside the organization to third parties?
3. Notice and access–when can the subject of data collection know that an identified record has been created about him or her, have the right to examine the record, and be able to challenge the accuracy, completeness, or proper use being made of the record?

Survey evidence suggests that American:~' concerns about privacy are rising. A Louis Harris Survey indicated that during the period of 1970-78 American concern about the hvi~- sion of privacy rose from about 33 to 64 percent.[5] This public concern was a factor in bringing about Federal privacy legislation. There was also a shift in employee attitudes about the prerogatives and responsibilities of employers with regard to employee data, adding further impetus to Federal policy activity. By 1983, another survey by Louis Harris[6] indicated that the proportion of the public concerned with privacy had increased further, from 64 to 77 percent.

This chapter is concerned with both confidentiality and security issues raised as more and more organizations introduce new office technologies, in both the private and public sectors. While privacy or confidentiality and security are interrelated, this chapter first discusses confidentiality and privacy issues, then security issues in the protection of personal and client data.[7]

[5] *The Dimensions of Privacy: A National Opinion Research Survey of Attitudes Toward Privacy*, conducted for Sentry I ɲ-surance by Louis Harris & Associates and Alan Westin, 1973.

[6] Louis Harris & Associates, Inc., *The Road After* 1984: *The Impact of Technology on Society-A Nationwide Survey of the Public and Its Leaders on the New Technology and Its Consequences for American Life.* Harris study No. 832033, 1984.

[7] Confidentiality and security of data involved in off-shore sourcing of data-entry work are discussed in ch. 8. Issues of software security are being addressed in another OTA report, *intellectual Property Rights in an Age of Electronics and Information* (winter 1985). Issues related to the security of Federal information systems are being covered in the OTA report, *implications of Federal Government Information Technology* (winter 1985). Privacy issues in electronic surveillance are covered in *Electronic Surveillance and Civil Liberties*, OTA-CIT-293 (Washington, DC: U.S. Government Printing Office, October 1985).

OFFICE AND DATA PROTECTION

Much of the rising concern about confidentiality and security has been occasioned boy the advent of computers and large data banks, and these concerns have repeatedly been subjects of congressional action, resulting in new laws.[8] End-user computing, in which many peo ple may access and use organizational databases, raises new questions about how claims to privacy can be respected and the confider~-tiality of information be assured. In a recent survey of privacy and security professionals, almost half, 47 percent, believed that as a result of the third phase of office automation there is a trend for broader or more detailed personal information to be collected.[9] Concurrently, this proliferation of computers is leading to decreasing compliance by managers with government-privacy regulations (45 percent). Networking, computer-based messaging systems and electronic mail will exacerbate these problems still further as personnel data can be circulated among more people.

Computer crime legislation passed in the 98th Congress established penalties for indi-

[8] In the mid-1960s, a Senate investigation was held to examine the kinds and amounts of personal information collected by the Federal Government. This investigation is considered by many to be the beginnings of the national expression of concern about the collection and use of computerized personal records systems. (U.S. Congress, Senate Committee on the Judiciary, Subcommittee on Administrative Practice and Procedures, *Government Dossier)* (Washington, DC: U.S. Government Printing Office, 1967).

[9] Westin and Hoffman, op. cit., 1985. This survey was not a representative sample of all types of organizations affected by office automation. Rather, the participants were chosen based on their reputation in computer and business circles as active, advanced, and unusually skillfull users of office-systems technology and as leaders in dealing with the employee-relations and organizational change aspects of new office technologies. However, there is a paucity of quantitative data on the extent of the privacy and security problems. Thus, the information reported from this survey should be treated as indicators of problem areas and not as indicators of the extent of the problem,

viduals convicted of theft, fraud and abuse associated with Federal computer systems. The first indictment and conviction under the new Computer Crime Act involved a person convicted of misrepresenting himself as a valid user of the computer system, establishing a super user code allowing future access to the computer he worked on and other systems to which it was linked.

As organizations rely more and more on computer-based information to conduct their business and to keep track of their personnel, the privacy rights of clients and employees must be considered. Coupled with the fact that the purchase and installation of microcomputer systems is often haphazard and uncontrolled within organizations, an appropriate degree of confidentiality is more difficult to assure when access to data is widely distributed. Personal information is required to effectively run a business, and with telecommunications linkages between computers and between organizations information can be collected in greater quantity and shared more easily. Client information can be processed at the client's workplace and sent via phone lines to the organization's computer system for processing. Office automation also raises questions about traditional security measures in central electronic data processing (EDP) environments. The purchase and use of computers in office automation is not controlled by a single department. Once microcomputers are linked with larger computer systems, any individual on the system has the potential for unlimited access and distribution of information.

Before the recent wave of office automation, the principle users of a computer system were professionals, and the two chief dangers were theft of funds or data by employees, and that of novices external to the organization breaking into the system. The dispersal of computers throughout an organization has extended accessibility to noncomputer-professionals. The computer professional's sociocultural system had within it values, beliefs, and concerns about privacy and security of information. Today, people who never participated in the sociocultural system of EDP environments, who have not been informed about the fine points of the law and ethics of protecting confidentiality or assuring data security, have easy access to an organization's databases. Violations can result from carelessness as well as through intent.

This chapter differentiates current office automation issues from the confidentiality and security problems that have been present in many organizations for two decades as part of an EDP system. This distinction between centralized and end-user automation is probably transient and likely to disappear as offices tie their small computers into the larger EDP systems highly integrated information systems. The transient nature of current systems is important for policy considerations later, and the distinction is useful in discussing new problems that arise with office automation.

Three developments in office automation are central to confidentiality and security issues, not only because they deal with the technological changes mentioned above, but with how the technology is procured and installed:

- the arrival of stand-alone word processors and text editors in the late 1970s, perceived as higher-order typing instruments and generally procured and controlled by office administration staffs or user departments;
- the move to widespread professional microcomputers, now available at prices and with features that allowed organizations to procure them for stand-alone work, and not only when linkage to on-line mainframes and minicomputers was involved. Generally, these machines were ordered by user departments; though often with EDP-department guidance; and
- the explosion of personal computers (PCs) in the early 1980s, for professional, sales, and executive use as stand-alone computing devices, and increasing linkage of such PCs to minis and mainframes. PCs in most organizations were ordered by individuals or by user departments, with limited guidance or control by EDP departments or central administrative service functions.

'Counterfeit Access Device and Computer Fraud and Abuse Act of 1 9X4, Public Law 98-473.

Each of these developments fostered new ways of carrying out office work. By 1984-85, each of these three original types of stand-alone terminal/software machinery were being linked to minicomputers and mainframes. This building of communication between computers makes possible access to central or distributed databases. In the survey of computer security professionals mentioned above, 64 percent believed that the spread of electronic mail and messaging systems poses a real problem in maintaining confidentiality. The ability to download (take data from) or upload (add data to) mainframe databases, using small computers, makes it possible for any employee with access to the building or computer to generate a file of personal information. Seventy-six percent of the survey respondents felt the automated office environment allowed more people physical access to workstations and disks as compared to earlier waves of automation. Finally, the interconnection of microcomputers allows the exchange of data within units or across units of the organizations, independent of mainframe system controls.

The following quote demonstrates the capabilities of the convergence of the various office technologies:

> In IBM we now have a world-wide network of more than 1,500 mainframes and 200,000 terminals. Any user at any terminal can send a message or a file to any other user. A user at any of those more than 200,000 terminals can connect to any application in any of those 1,500 systems. Programs and even entire applications spread spontaneously through the network, usually without management direction or intent and often without management understanding or knowledge. Employees can access the network from their homes. Some vendors and contractors use it . . . [DP] management did not plan it. They bought it and built it but they were just as surprised as anyone else when they saw what 'God had wrought. '[11]

[11] W.H. Murray, "Security Programs, Functions, and Concepts for the New Computer Economics, " *Proceedings of the 11th Annual Computer Security Conference* (Northboro, MA: Computer Security Institute, 1984).

THE PERIOD 1960-78

EDP systems made it possible for client data to be:

- collected and recorded more easily;
- analyzed, compared, and collated more fully;
- distributed to or made accessible to more people within the organization;
- amalgamated with data on individuals obtained from other organizations having computerized record systems; and
- disseminated more widely, both in intra-organizational networks and in response to specific demands from other organizations.

These capabilities made it possible to provide more customized and personal services by business and government. They also raised the possibility of greater aggregation of data--computerized databases can break down the vital compartments and boundaries that helped keep client information confidential. This is what the privacy-and-data banks debate of the 1970s was about.[12]

There were also several aspects of internal organizational control in the 1960-78 era, before end-user computing, that provided the framework for carrying out new privacy rules that were developed:

- in the EDP era, small staffs of EDP professionals ran the data centers and controlled access to automated files; and
- centralized security procedures of access and audit were available to check (if necessary) that terminal users followed the legal and organizational rules.

[12] For an early discussion of the debate see, U.S. Senate, Committee on the Judiciary, Subcommittee on Constitutional Rights, *Federal Data Banks and Constitutional Rights, 1974.*

Computer-system security measures originally evolved from manual techniques for physical security carried over from the electronic accounting machines of the 1950s. Usually physical security (locking up sensitive card decks and tapes) was the prime technique. As first and second generation batch processing computer systems were introduced, followed by remote terminals and third generation systems, computer security techniques became more technological and sophisticated. Passwords were used to restrict access to information based on a user's or terminal's privileges or on the type of function being performed. A few systems, especially those involved in national defense, used cryptography or enciphering. Some systems provided other mechanisms to assist proper authorization, most notably the hardware rings provided by the GE/Honeywell machines of the late 1960s and early 1970s. During this period, it was hard enough to get a program to run at all on a given hardware system, and security took a back seat to other design criteria such as correctness, speed, cost, and utility.

As third generation computer systems became more common in industry and government, the use of data within organizations changed and networks were built up. Rather than use one computer center, one or more systems could be accessed via user terminals. Indeed, commercial time-sharing networks grew to service the needs of organizations without the resources or inclination to start their own networks. Minicomputers (minis) appeared, but in contrast to today's microcomputer systems, minis were generally still purchased and operated by data processing specialists within the organization.

At the same time, there was growing public awareness of potential loss of privacy and problems of fairness or due process. Thus, the security of computer systems took on added importance and led to additional safeguards such as logs, journaling, of important operations and more specific policies with respect to computer security, as a means to guarantee confidentiality and accountability. However, the most sensitive narrative information was still not computerized at this time; it remained on paper in manual files. Thus, most problems involving personal data in the 1970s still were associated with paper records. In the early 1980s, medical, banking, credit and employment information was placed in large databases, beginning the current rapid move to store personal, employee, and client data on-line.

The advent of commercial products to enhance computer security, such as the ACF2 access control package for IBM mainframes and various vendors' versions of the National Bureau of Standards Data Encryption Standard had not yet been introduced. Leading manufacturers were starting to take seriously the task of educating users about these issues. An advance guard of computer practitioners were becoming knowledgeable about computer security issues. "Second-generation" technological security issues (e.g., the idea of kernels in software engineering)[13] were just starting to be investigated.

[13] "A security kernel is a small nuclear piece of the operating system that controls access to other parts of the computer system—either information or data. This nucleus itself must be tamperproof so that its programs may not be modified, allowing system operators to verify whether it has implemented the systems security policy through the programs. See G.J. Popek and C.S. Kline, "Issues in Kernel Design," *Advances in Computer Security*, Rein Turn (cd.) (Dedham, MA: Artech House, Inc., 1981), pp. 139-144; and R.C. Summers, "An Overview of Computer Security," *IBM Systems Journal, vol. 23, No.* 4, pp. 309-325. This development has been primarily in the Department of Defense; there are no commercially available security kernels.

THE POLITICAL AND LEGISLATIVE CLIMATE

The response of American society to both the social change aspects of privacy protection and the computer-based handling of personal data by organizations has been well studied, [14] By the late 1970s, a detailed latticework

[14] See for example, W. H. Ware, "Information Systems Security and Privacy," *Communications of the ACM*, vol. 27, No. 4, 1984, pp. 31.5-321,

of laws, regulations, organizational policies, and social expectations regarding privacy protection in EDP systems had been put into place. Codes of "fair information practices" were embodied in law or organizational standards to govern the collection, use, and release of personal data on clients and customers, and to make this process visible and accountable to both data subjects and the public.

Laws and regulations were promulgated to deal with privacy in particular fields of organizational recordkeeping-Federal agencies, banking, insurance, health care, education, credit-reporting, employment, law-enforcement, etc. " The earliest statute was the Fair Credit Reporting Act of 1970 (15 U.S.C. 1681). This act requires all credit investigating and report - ing agencies such as banks and retail charge card firms to make the records they collect available to the subject. Furthermore, it provides procedures allowing the subject to correct the information. Finally, it only allows disclosure to authorized customers. Since thi:s statute, many more have been enacted providing protection policies for information privacy.

The Crime Control Act of 1973 requires that State criminal justice record keeping systems, developed with Federal funds, ensure the privacy and security of the information collected.

The Privacy Act of 1974 (5 U.S.C. 552a) restricts the collection, use, and disclosure of individually identifiable information by the Federal Government. It gives the individual rights to access the information and to correct it.

The Tax Reform Act of 1976 (26 U.S.C. 6103) protects the confidentiality of personal tax information. It restricts disclosure of tax information for nontax purposes.

In furtherance of such laws, and in manly areas where no legislation had yet been enacted, many private and public organizations developed "privacy codes" or "fair information practices standards" to govern their own handling of client or employee personal data. The motives for such action were a blend of concern to meet legitimate privacy concerns of clients and employees; the desire to avoid the necessity of detailed legal regulation; and the judgment that fair-information-practices rules had a generally positive effect on accuracy, completeness, and timeliness in the management of automated data systems, and could be initiated without heavy costs in money or efficiency. A few corporations such as IBM, Bank of America, and Control Data Corp. had also developed employee privacy codes in the early to middle 1970s, but most of the 10,000 large private employers in the United States had not.

By the time that end-user computing began to add new dimensions to the handling of personal data in office work in the early 1980s, there were still debates among privacy advocates as to whether the data collection and the confidentiality aspects of privacy had been ade quately dealt with, in what was coming to be called the "first-generation" of privacy protection measures. In spite of the emphasis on notice, challenge, and due process rights of data subjects, and workable procedures for strengthening confidentiality rules, critics argued that there had been too few limitations on what was appropriate information to collect about people's transactions and activities in many sectors of business and government life. They also argued that merging data from different organizations about the same individual (e.g., in computer matching programs) threatened to shatter basic confidentiality standards.

There was also debate among informed observers and the media about whether the necessary machinery with which to enforce privacy rights had been created, and about other questions—the implementation of the Federal Privacy Act of 1974, the desirability of a continuing Privacy Commission or Privacy Ombudsman (as Canada and many European countries have), and U.S. Supreme Court rulings

[15] Examples would be the Federal Privacy Act of 1974 (5 U.S.C. 552a); the Federal Freedom of Information Act Amendments of 1974, and similar "jurisdiction-wide" statutes in 12 States. At the statutory level, this is exemplified by the Family and Educational Privacy Amendments of 1974 (20 U. S. C'. 12239), and by State medical, banking, insurance, and employee-privacy legislation.

in matters of data collection by business and government organizations.[16]

The report of the U.S. Privacy Protection Study Commission in July 1977 urged new laws and voluntary codes in the private sector. What followed was a new series of statutes that affected information privacy.

The Right to Financial Privacy Act of 1978 (12 U.S.C. 3401) limits the access of Federal agencies to information about the customers of financial institutions, by describing the procedures necessary to obtain that information. It also provides bank customers other assurances of privacy about some aspects of the bank records.

The Privacy Protection Act of 1980 (42 U.S.C. 2000aa) prohibits government agents from conducting unannounced searches of press office and file records if no person in the office is suspected of having committed a crime.

The Electronic Funds Transfer Act of 1980 states that any institution providing EFT or other services must notify customers about third party access to customer accounts.

The Debt Collection Act of 1982 (Public Law 97-365) establishes due process procedures that Federal agencies must go through to release any information about bad debts to credit bureaus.

The Cable Communications Policy Act of 1984 requires any cable service to inform the subscriber of any personally identifiable information collected. They must inform the user about how the information is to be used and how long the information is maintained on record. If the information is disclosed, the individual must be informed and restrictions are placed on how and to whom information is disclosed.

Only after the passage of new privacy legislation in 1978-82 protecting bank depositors, and State laws on insurance, employment, and medical privacy did broad private sector institutionalization of privacy rules take place. The establishment of organizational procedures and regulatory or judicial enforcement of privacy was just becoming the norm when end-user computing began to spread in the early 1980s.

In the mid-1980s as office automation is spreading, an extensive set of confidentiality protections for manual and EDP systems has been put into place; but debate continues as to whether these protections are adequate in scope and are being vigorously administered.

The laws above basically deal with rights to confidentiality. Until recently, no Federal law dealt specifically with sanctions against the use of computers by individuals to commit a crime, or with trespassing by reading private computer files.]' In October 1984, Congress passed the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, which makes it a felony to access confidential or restricted information related to national security without authorization, and makes it a misdemeanor for unauthorized persons to access the data banks of financial institutions, or to use, modify, destroy, or disclose information in a *government* computer.

There are of course many criminal laws that can be used in prosecuting computer-related crime, but there are problems in applying many of the laws defining theft to cases where only "virtual property" (nonphysical property) is concerned. Thirty-three States now have computer crime laws, but some do not cover hackers who penetrate systems for fun rather than profit. "

'There were debates over whether new systems or applications were covered by "first generation' privacy measures; for example, electronic funds transfer (EFT) systems, two-way cable systems, and Postal Service electronic-mail projects. There was also concern that plans for large sophisticated computer systems as replacements for older systems in the Federal Government might go forward without sufficient attention to privacy risks, for example, the proposed FBI "Triple 1" system for processing criminal history records, and the planned IRS, Social Security, Secret Service, and Veterans Administration systems.

'The Privacy Act of 1974 (Public Law 93-579) and the Crime Control Act of 1973 (Public Law 93-83, sec. 524(b)) are, however, designed to prevent misuse of Federal *records* of all kinds in ways that would violate the privacy of citizens.

"List provided by the National Center for Computer Crime Data (Los Angeles) includes Alaska, Arizona, California, Colorado, Connecticut, Delaware, Florida, Georgia, Hawaii, Idaho, Illinois, Iowa, Maryland, Massachusetts, Michigan, Minnesota. Missouri, Montana. Nevada. New Mexico, North Carolina, North Dakota, Ohio, Oklahoma, Pennsylvania, Rhode Island, South Dakota, Tennessee, Utah, Virginia, Washington, Wisconsin, and Wyoming.

THE THIRD PHASE OF OFFICE AUTOMATION

The Handling of Client Data

Confidentiality in an organization with new decentralized or networked office technologies requires consideration of a number of new factors:

Low-security or no-security physical environments in offices. Except for military, diplomatic, and a few private-sector settings that operate in "highly sensitive data" modes, most organizations have put microcomputers onto desks in working areas that are open to passing fellow workers, service personnel, invited visitors, or even the general public. Storage of diskettes, location of printers, and other peripheral equipment is also usually in unsecured environments.

More finished and relined information in office automation systems. In most organizations, word processors contain finished correspondence, memoranda, documents, charts, and reports. These stored materials may contain sensitive personal information on clients, proprietary data of the organization, information confidential to particular employees or units, and data about terms of contracts and other legal responsibilities. While much raw data and some reports of this kind are in mainframe storage, the information in word processors or professional/executive microcomputers is generally more complete, revealing, and easily found, because it includes explanatory text.

More readily accessible information in office computer systems. An interloper, whether an employee or someone from outside, who seeks to extract sensitive data from the mainframe database generally has to know specialized mainframe software codes, as well as how to deal with special security protections that most organizations have built into mainframe databases. With microcomputers, unskilled interlopers are more able to call up data on screens, print out documents, or copy diskettes than they would be in EDP systems.

The mobility of microcomputers and their data-storage media. Dumb terminals connected to mainframes are known to the system, and their uses are usually logged or monitored. Microcomputers can be moved around within organizational offices without central control or notice, and portable versions can be taken home or on trips. Information is archived on floppy discs rather than magnetic tapes.

Less sophisticated office automation users. While 10 percent of organizational personnel may have been using terminals in the middle 1970s, either in EDP units or as EDP-trained operators in users' departments, at least 25 to 35 percent of personnel in large organizations are probably using microcomputers today, and eventually this may approach 100 percent. Typically, new users have not been educated about confidentiality issues or security protections.

Uncontrolled channels of data communications. Electronic message systems, bulletin boards, and microcomputer networks encourage users to send messages to everyone using these systems or to create their own distribution lists. As a result, messages with confidential data can move around either anonymously, or without control for their confidentiality. Fraudulent memos can be circulated for political purposes without an easily traceable origin. Reproducing machines, and before them, mimoegraph machines had the same effect, of course; computers merely allow this communication to be done in the privacy and safety of one's own office or home. [19]

Wide ability to add information to or copy or extract information from corporate databases. Controls over alteration of data or unauthorized access become critical.[20] Microcomputers can be used to attack the security of mainframe and mini data, and obtain confidential client data improperly. This can in fact be done from any terminal, including those developed for mainframe use, but more understandable

[19] "This situation may seem trite, but a recent State supreme court ruling stated that an employee's privacy had been violated by an interoffice memorandum. "SJC Outlines Rules on Employer Rule in Workers' Privacy," *Boston Globe,* July 7, 1984; as cited in Philip Adler, et al., "Employee Privacy: Legal and Research Developments and Implications for Personnel Administration," *Sloan Management Review,* winter 1985, pp. 13-22), In this case upheld by the U.S. Court of Appeals, First Circuit on Aug. 6, 1984; the memorandum was on paper.

[20] "'This does not address. the problem of unauthorized users external to the organization accessing the databases. One commonly suggested procedure is the use of tiered passwords for accessing the computer and then the particular volume or file the information is stored in.

software instructions are expanding the number of persons able to probe password security, attempt unauthorized entry, or alter confidential data.

Little or no hardware or software security protections. Because of the ways that word processors and microcomputers entered office work, there was neither a perceived necessity or an assumed "market demand' for built-in terminal hardware protections such as locks on the machines. Similarly, in buying or designing software for office systems, organizations have generally not specified audit trails, cryptographic protections, and other measures that could have been installed–though at added costs.

Unpredictable individual and group behavior. There is no way to predict with any assurance how office employees and managers will use these powerful new capacities. There will be some conduct by insiders and outsiders arising out of the new opportunities in microcomputer use that pose risks, and this has to be the perspective from which managers assess risks to confidentiality and security.

Security and Confidentiality Issues

The potential vulnerabilities to client data emerging in office automation can involve either new situations created by microcomputer use, or can be extensions of familiar risks in manual and EDP recordkeeping. The types of potential end-user conduct that could violate existing privacy standards are discussed below. "

Data Collection

Microcomputers permit the creation of any files or databases that the end user wishes to maintain. Either without awareness of or in deliberate disregard of privacy, end users may put personal client information into "their" files that violate laws, regulations, organizations rules, or ethical guidelines. If there is no auditing or physical inspection of end-user files, then management may be unaware of such conduct, and suffer legal sanctions or have the companies reputation compromised.

Confidentiality

End users may take client information from central files and merge it or match it with other client data in ways that violate privacy standards. Through electronic mail and message systems, end users may send confidential client information inadvertently to those not entitled to have it, especially if "automatic" distribution lists are used.

Subject Notice and Access

Where end users create files improperly or record confidential data they should not have accessed, failure to inform clients that such files have been created and might be used in making decisions about clients could be a violation of several basic privacy laws (the Federal Privacy Act, State fair information practices acts, Fair Credit Reporting Act, State insurance privacy acts, etc.), as well as the organizational rules of many banks, insurance firms, brokerage houses, medical facilities, educational institutions, and other private organizations. Failure to provide opportunities for individual clients or potential clients to examine and challenge these files would be a violation of such laws or rules.

It is critical to distinguish the privacy issues generated by the transition from manual record systems to EDP systems, from those of the current progression from centralized to decentralized computing. The arrival of EDP brought about revolutionary increases in two areas: 1) data-collection capacities (reducing costs and time constraints, magnifying data-analysis capabilities, etc.); and 2) data-sharing capacities (circulating personal data within and between organizations). The response in terms of privacy laws and organizational codes was: 1) to increase the visibility of organizational activities affecting sensitive personal data

I+; xamining such potential vulnerabilities in office automation follows the studies of EDP systems impact done by the National Academy of Sciences in 1969-72; the HEW Advisory Committee in 1972-73; and the U.S. Privacy Protection Study Commission in 1975-77. Hopefully, the examination of potential office automation vulnerabilities can benefit from the experiences with risk-assessment and reality-testing that were developed in 1969-77 EDP studies, as well as the practical experiences gained over the past decade in administering the standards promulgated (for client data) as the '*first generation' of privacy and security rules.

(changing these from private "kitchen work' to public notices and descriptions, with specific rights of data-subject inspection challenge); 2) to stipulate broad relevancy and social acceptability standards for data collection; and 3) to provide rules and procedures for confidentiality or data sharing.

The use of microcomputers in the office has the foIlowing characteristics:

- They do *not* significantly increase the scope of data-collection capacities over existing EDP systems. However, because of their ease of use or cost, data not entered into the mainframe system can now be entered, potentially increasing the quantity of data collected. This requires managers to provide greater education and oversight of users to see that they know the limitations on data collection set by law or code, and do not violate these in "personalistic" data recording.
- They *do* increase the risks of improper circulation of personal client (or personnel) data within the organization and to outside organizations, threatening confidentiality, because they provide many more employees with a tool for accessing the records or information.
- They do increase due process problems. To the extent that stand-alone-diskettes and off-line storage of personal client data would not be known to data subjects, the use of that data for decisionmaking could not be challenged under privacy rules for subject access.

Security

How to protect records from accidental or deliberate destruction, loss, or theft is a security question. There are also differences between EDP and decentralized office automation. Surveys of private organizations show general agreement that by the end of 1984 there were significant security issues in use of microcomputers, not just for sensitive client and personnel data but also for general proprietary business information, financial data, national security information, and legally sensitive information. These problems have not been taken up yet by most top managements, and thus the policy directives and budget authorizations necessary to address this problem adequately have not existed in most private-sector organizations. The major problems developing with decentralized office automation are:

Lack of clear identification of sensitive information. The basic requirement for sound security is to identify information that is sensitive and needs special protection. Any effort to protect all personal information in ordinary business or government organizations would be too costly and would virtually paralyze organizational programs. 'z

Failure to provide adequate physical security for machines and storage media. Many microcomputers are not kept in locked rooms and diskettes are often not kept in locked cabinets or desks. Easy physical access to such microcomputer equipment poses real security risks; for exampIe, diskettes can be copied on another machine on or off the premises.

Failure to have key locks on terminals. Most microcomputers do not have key locks that control on-off functions, enabling third parties to activate them.

Weaknesses in password systems governing access to central databases. Microcomputers connected to mainframes in many organizations suffer from the same security problems as dumb terminals; users are casual about writing down or telling their passwords to others. But microcomputer users are probably less disciplined in handling password regulations than EDP-trained personnel.

No logs *or journals.* Though central databases of confidential client data are often provided with audit trails, transaction logs, or journaling capabilities, these techniques are often not used when groups of microcomputers are connected to minicomputers or, through them, to mainframe files.

Not recording efforts to penetrate security. Unlike mainframe systems, microcomputer-based office systems generally do not record efforts to enter restricted files without proper identification or passwords, or warn security officers that such efforts have taken place or are under way.

[2]Many European countries do attempt to protect a large amount of the personal data collected.

Absence of either security education for users or auditing of their practices. Even if sensitive information was identified, security measures were adopted, and records were kept of efforts to access databases improperly from microcomputers, most experts would agree that security of sensitive client data also requires that users be educated about security policies and procedures. Second, it requires that inspections or auditing be carried out to learn whether security policies are being followed.

When it comes to security measures needed to safeguard sensitive client data in microcomputers and end-user office automation, current evidence shows that: 1) the techniques for installing security protections are well known; 2) the process of risk-assessment and vulnerability analysis to determine cost-beneficial policies is well known; but 3) these techniques and processes have just begun to be undertaken in the private sector, and are only somewhat further advanced in the Federal establishment. The first task in dealing with security is not to identify wholly new security approaches or methodologies, but to stimulate organizations to provide directives and resources with which to modify and apply known techniques and processes.

There are some situations in which new forms of office automation may require special measures. For example, if combined voice/data terminals are widely used, manufacturers may have to provide means of preventing the undetected turning on of the microphone capabilities of terminals, to ensure that neither officials within the organization nor outside hackers, or more serious intruders, used these terminals for organizational espionage.

Local area networks present particular problems. Three different types of network configurations exist and present different security problems. In a star network, several terminals are connected to a central controlling device; the central computing power can be used to control data and software, maintaining a high degree of security. In a ring configuration (or a loop) the workstations are arranged in a circular network. Each station is linked by a repeater mechanism that monitors all passing information to see if any are addressed to that workstation. This configuration has gained more acceptance in Europe than in the United States. Because information travels around the ring, any workstation has the capability of accessing it. The tree or bus network, the most easily expandable of the three, does not require a central controller and, security is therefore contingent on the security capabilities of individual workstations.

PRIVACY ISSUES IN WORK MONITORING

The monitoring of office work by computers was discussed in chapter 5; but it is sometimes discussed as a privacy issue rather than as a quality of worklife issue. The privacy issue raised by computer-mediated work monitoring is whether the collection of operator performance data through “machine capacities” and its use to evaluate employees constitutes an intrusive form of “employer surveillance’ that violates reasonable expectations of personal privacv by the employee. Whatever the pros and cons of computerized-work monitoring, it is probably not best posed in terms of privacy. The work is done on the employer’s premises; the activities are usually group settings open to view rather than individual activities taking place in closed or private rooms; supervision is a normal condition of the employer-employee relationship; and collecting quantitative data as to employee output has long been used in evaluating and compensating work performance in factories and offices.

Unlike the use of TV-monitors to watch assembly lines, or of hidden microphones to overhear workers in cafeterias or restrooms, the collection of operator-production statistics generated by system software does not represent an intrusive act per se, provided that employees know that monitoring systems are used, employees have access to their individual records; and a procedure is provided for contesting the accuracy or fairness of applying records for evaluative purposes.

SECURITY AND CONFIDENTIALITY IN AUTOMATED PUBLIC OFFICES

The protection of data is a major concern in public-sector offices, especially in regard to matters of national security, diplomacy and foreign relations; the Federal role in monetary transactions; government funds transfers; and foreign trade. Most of the sensitive information about such subjects, however, is usually in large computer and communication systems, and is usually protected by encryption and a variety of other mechanisms. However, shared databases and the downloading of data to microcomputers for end-user computing is raising new concerns, especially since data that are not per se identified as sensitive can, when aggregated, reveal information that is highly sensitive.

The Federal Government collects large volumes of detailed personal data about citizens and in particular about Federal employees. As early as 1967, a study of computerized Federal records revealed that the files contained more than 3 billion records and that over half of them could be accessed via computer terminals.[23] Several years later in 1974, another congressional committee found that 86 percent of the 858 known government databanks were computerized.[24] Successive waves of office automation have continued to provide greater access to these expanding data files. This information can be integrated through computer matching and other techniques and through the exchange of data between agencies and with State governments, in ways that cause deep concern about confidentiality. For example, when one applies for Food Stamps, the Department of Health and Human Services, which administers the program, matches one's name with those in the Internal Revenue Service (IRS) earnings file (which is in fact maintained and used by the Social Security Administration (SSA) to verify eligibility. SSA checks the data in the IRS earnings file to verify income reported by recipients of SSA retirement benefits.[25]

In general, information-handling associated with end-user office automation is not classified information, but it is often sensitive information, especially when aggregated in certain ways.[26] Routine records, forms, and correspondence often contain information that would allow individuals to put together and profit from advance knowledge of government actions. For example, plans for siting highways and government facilities, impending regulations, actions that affect interest rates, sales of minerals and timber rights, etc., are very tempting. Personal data about Federal employees can be used to discourage whistleblowing. Less often voiced, but still important, is the concern about unauthorized access to

Government Dossier, op. cit.
'Federal Data Banks and Constitutional Rights, op. cit

According to briefings and interviews provided for OTA by SSA.
This has chiefly been of concern to the Department of Defense; for example, the problem was exhaustively discussed in a planning conference held for the U.S. Army Information Systems Command by SRI in Tucson, AZ, in December 1984. Hypothetical examples given in an informal talk concerned the possibility of aggregating routine travel orders or schedules for key individuals to reveal the (undisclosed, sensitive) location and timing of small meetings; or the possibility of aggregating data on materials delivery to a site to reveal information about development of weapons systems, However, some civil liberties specialists have long been concerned about the ability to aggregate information from many sources about one individual to produce a profile of his or her marital, financial, social, business, professional, and political activities.

information that is simply embarrassing or politically fatal to officials or to their nominees for official positions. In congressional members' offices, there are grounds for concern about protection of information in computers, which is chiefly protected by ID's and passwords. (The privacy and security issues related to large Federal computer systems and databases will be covered in a forthcoming OTA report. [27]

Even when nonclassified Federal data is normally stored in large databases or processed in central EDP centers, it is increasingly hable to be at some point accessed, handled, analyzed, or even generated using personal computers or terminals scattered throughout agency headquarters and field offices. Most of the concern about government security has focused on large information systems. There has been much less attention to the protection of data in day-to-day agency operations in which decentralized office automation is used. Violations of security and confidentiality need not be intentional or malicious; they are often the result of ignorance or carelessness. Office workers have not yet been acculturated to think routinely about computer security; there are stories of government workers routinely locking away sensitive papers but leaving the disks from which the copy was made lying next to their personal computer or word processor.

Government computers are thus subject to the same risks that plague banks, corporate payroll and financial management operations, and other private-sector computer systems, plus some risks that are particularly political in nature. As extreme examples, records could be destroyed to cripple a government program or project; or calendars and trip schedules could be used to plan the assassination of a political leader or a foreign dignitary."

Government Guidelines

Security and confidentiality for nonclassified government information is covered by the Privacy Act of 1974 and:

- OMB Circular A-71 Transmittal Memo No. 1, July 17, 1978, which provides general guidance to agencies, on administrative, technical, and physical measures to increase security; and
- OMB Circular A-123, which sets standards for internal controls implementing the Federal Managers Financial Integrity Act and directs each agency to review and update its security provisions.

The General Services Agency (GSA) and the National Bureau of Standards (NBS) in 1983 began development of guidelines for security in end-use computing and small office systems. The Office of Personnel Management (O PM) recommends personnel security policies for computer-related jobs. However, the General Accounting Office (GAO) has repeatedly criticized the lack of compliance with guidelines established in the circulars by Federal agencies. [29] In 1982, GAO said that:

> . . . increasing Federal investments in automated systems . . . have resulted in growing vulnerability to fraudulent, wasteful, abusive, and illegal practices because greater concentrations of information are accessible from remote terminals.

The Office of Management and Budget (OMB) is now updating A-71, A-123, and other circulars related to computer security. It is expected that they will be combined into one broad policy statement.[30]

The Special Concern About Employee Privacy

An aspect of Federal computer security that deserves–but has not received–special atten-

---

Implications of Federal Government Information Technology for Civil Liberties and Congressional O\ ersight, op. cit.

'According to the *Washington Post*, an air traffic controller, angry about the Soviet invasion of Afghanistan, deliberately endangered an Aeroflot jet carrying Soviet Ambassador Dobrynin, by manipulating a signal so that a computer read the jet as a small craft and did not properly monitor and control its landing at a busy airport. (Mary Thornton, "Age of Electronic Convenience Spawning Inventive Thieves," *The Washington Post*, vol. 107, May 20, 1 984).

-'U.S. General Accounting Office, *Central Agencies' Compliance With OMB Circular ,4-71,* Transmittal Memorandum No. 1, I, CD-80-56- 1, Apr. 30. 1980: and *Federal Information Systems Remain Highly Vulnerable to Fraudulent, Wasteful, .4 busive, and Illegal Practices*, MASAD-82-18, Apr. 21, 1982.

Susan M. Menke, "Survey of Agencies Finds Many Are Implementing Standards," Special Section: Security, *Government Computer News*, November 1984.

tion is the question of the ability to protect, the privacy of Federal employees. Agencies collect and keep much personal data about em". ployees and even applicants for Federal jobs, Much more data is likely to be collected than would be sought by corporation personnel offices." These files may be, and usually are. widely dispersed and only superficially protected. As files are computerized, they can, more easily be aggregated and accessed, or tampered with. If files are stored in personal computers or can be accessed or downloaded, more and more people will have access to them. and may use them for satisfying curiosity, for mischief, for exerting political pressure, or for sheer malevolence. This raises significant questions about protection of privacy in Federal computer systems and databases.

Federal employees are the subject of much computer matching, which was described earlier; that is, the comparison of two or more computerized lists of individuals. For example, Federal employee lists were checked against lists of people earlier defaulting on student loans. A very early example of computer matching occurred during the Carter Administration; this was Project Match, through which names of Federal employees were matched with names on the roll of the Aid to Families with Dependent Children, in an effort to discover ineligible recipients.[32]

Accidental Losses

Telecommunications and computers are vulnerable to crime, mischief, and terrorism, but they are also vulnerable to unintended disruption, a point that is sometimes overlooked. This includes error or accident, and the simple breakdown or failure of equipment; it also includes destruction by fire, flood, earthquake, and other natural and technological disasters.

Data can also be lost permanently, or made temporarily inaccessible, by electrical outages. As government activities become more and more dependent on microelectronics there is the strong possibility-and given enough time the virtual inevitability—of electrical failures that affect critical activities or whole regions of the country, bringing all computer-mediated activity temporarily to a halt. Emergency response systems may be unable to respond adequately because some step or link depends on office automation that is down because of the same emergency. Routine recovery procedures may be hampered by loss of data in the same incident. GAO called attention to this danger in a strong report in 1981, identifying the need for further emergency planning by the Department of Energy and the Federal Emergency Management Administration.[33]

Some government operations are highly time sensitive (e.g., transfer of funds, transmittal of orders to the armed services, air traffic control, response to natural disasters, law enforcement actions). Others are dependent on ready access to individual and case records (tax collection, processing of welfare payments, payrolls, etc.). As the government becomes more and more dependent on office automation for orderly performance of necessary activities, the result of any disruption-whether irreparable or of brief duration and narrow scope– becomes more severe.

Federal agencies have not adequately prepared for natural or technological disasters that might wipe out electronic information, according to GA0.[34] Many still have no contingency plans or rely on letters of agreement from other agencies to supply equipment in emergencies. This course assumes that the other agency will: 1) be able and willing to live up to its agreement even at the cost of prejudicing some of its own activities, and 2) will not

---

"See Alan Westin, "Personnel Practices in the U.S. Civil Service, " *Information Age,* July 1982, pp. 149-169.

'According to information supplied by Federal officials to OTA.

[33] U.S. General Accounting Office, *Federal Electric Emergency Preparedness Is Inadequate,* EMD-81-50, *1981.*

[34] U.S. General Accounting Office, *Most Federal Agencies Have Done Little Planning for ADP Disasters,* AFMD-81-16, *1980;* and *Federal Electrical Emergency Preparedness Is Inadequate,* EMD-81-50, *1981.*

A contingency plan should have most or all of the following features: backup files at external storage sites, standby arrangements for renting processing time or services, a recovery operation center, a multilateral aid agreement involving five or more agencies, or a plan for reverting to manual (nonelectronic) operation if necessary.

have been disrupted at the same time by the same events. Nonelectronic equipment is often not available, and reversion to manual systems not possible; data may exist only in electronic, machine-readable form.

The cost of downtime or time lost because the computer is malfunctioning, is seldom calculated in justifications or cost-benefit analyses of office automation. In most cases, the downtime is merely an annoyance and a temporary problem. In some cases, it significantly aggravates the workload peaks and degrades the quality and timeliness of important services. In time-sensitive situations, such as response to local emergencies, it can mean catastrophe.

Comparisons With the Private Sector

In spite of these problems and concerns, the Federal Government is probably well ahead of the corporate sector in attention to the need for safeguarding privacy and security in the use of microelectronic office automation.[35] This reflects the implementation of provisions of the Privacy Act over the last 10 years, including annual reporting requirements; OMB guidelines; agency implementation procedures; and continuing attention from congressional committees, media, interest groups, and scholars.

However, if the government is ahead of the private sector, this says more about the lack of systematic attention to these issues within corporations, than about the effectiveness of government attention. It does not mean that the problems have been taken care of. The particular vulnerabilities of office automation systems to casual misuse, and even serious abuse and fraud, are still not realized by most of the users.

But the openness of these small office automation systems, which makes them especially vulnerable, is probably also their best protection. The many users and the open office environment means that abuses are likely to be observed and reported, if they are recognized as abuses. They will be recognized only if office workers understand the ethical, legal, and policy issues involved and are sensitive to their importance. A thorough attempt to educate Federal office workers about this problem is in order.

Individual workers, however, can do relatively little about protecting their data in the case of power outages, system malfunctions, and technological or natural disasters. The primary responsibility for backup and fall-back systems, and other kinds of contingency planning must rest with top-level agency managers.

[35] This is the conclusion from an OTA contracted study, *Privacy and Security Issues in Office Automation*, Alan F. Westin and Lance J. Hoffman, 1985. Their study used documentary material from 44 Federal agencies and interviews at 7 agencies, Federal policies and practices were compared with findings from site visits and interviews in approximately 100 corporations and nonprofit organizations in 1982-84. The researchers did not do on-site studies of the implementation and efficacy of security measures in Federal agencies, but relied on reports of the manager and staff.

POLICY CONSIDERATIONS

Nearly a decade ago, the Senate Government Operations Committee investigated computer abuse in both the public and private sector; [36] as a result there have been proposals in the last three Congresses related to computer security in general and in particular to the security of computerized government information.[37] In April 1984, the House Committee on Science and Technology issued a special report on *Computer and Communications Se-*

[36] U. S. Congress, Senate Committee on Government operations, *Problems Associated With Computer Technology in Federal Programs and Private Industry: Computer Abuses*, Committee Print, 94th Cong., 2d sess., 1976; and *Computer Security in Federal Programs*, Committee Print, 95th Cong., 1st sess., 1977.

[37] Federal Computer Systems Act of 1977, S. 1766 and H. R. H421: S. 40 and H. R, 6196, 1979; Federal Computer Systems Protection Act of 1981, H. R. 3790.

curity and Privacy[38] that recommended that Congress charter a national commission to study the issues and outline a framework for policy. While recognizing the threat from "hackers and other outside intruders, " the report said that the greatest threat is from personnel who are authorized users of the computer resources that they attack. The report was highly critical of recent policy and programs related to computer security.

OTA concurs that violations of data confidentiality are most likely to occur within the organization by authorized users. External threats, whether from hackers, ordinary thieves, political opportunists, disgruntled former employees, terrorists, or others, nevertheless deserve greater attention. But these threats chiefly concern large systems. With small computers violations by insiders are most likely, and there are fewer safeguards against them. Both large systems and small computers are at risk from accidental disruption because of natural events, human error, and technological failure.

Because decentralized end-user computing is raising new uncertainties about how well data is protected, Congress may wish to reexamine the structure of privacy laws and thek application to these technologies, perhaps through a special commission or task force.

Stringent actions have been suggested. One possibility is to establish a new authority to implement, oversee, or enforce current and future statutes. This organization would have no responsibility for collection and distribution of data. There are precedents for this: Sweden for example has a Data Commission to oversee all records and their linkage. Another possible strategy is to have an ombudsman within each data-collecting organization. This is the approach used, for example, in Germany.

However, current laws may be adequate to address the problems of decentralized automation. Whether organizations treat "office automation" and centralized EDP as one or separate and distinct components of office activity, the critical element is to adapt existing rules to apply to predictable oversights, carelessness, or misuse by some persons in the large end-user population, and to assign organizational responsibility and continuing oversight duties to effective units at various levels of the organization. If organizations are not willing or able to create and enforce policies to ensure that existing safeguards and guarantees are applied in end-use computing to protect their clients and their employees, Congress may wish to clarif y and strengthen through legislation the liabilities that such organizations incur by their failure.

Current laws chiefly strengthen the right and the ability of an individual to control information about himself or herself. Thus, the individual is the final enforcer of principles of fair information use. Given the ubiquitous nature of the new information technologies and their linkages and systems integration, more specific *data* collection and *data* protection policies may become necessary as opposed to traditional policy approaches strengthening individual rights.

For Federal agencies, strong oversight attention is merited to make sure that reasonable security provisions are enforced. Special attention should be given to the questions of: 1) the ability of essential day-to-day government operations to continue when computers cannot operate, 2) the need for protecting employee data, and 3) the adequacy of procedures for protecting correspondence and records with congressional offices.

[38] U.S. Congress, House Committee on Science and Technology, *Computer and Communications Security and Privacy*, report prepared by the Subcommittee on Transportation, Aviation and Materials, Committee Print, 98th Cong., 2d sess., April 1984.