Chapter 1
Summary

Chapter 1

Summary

INTRODUCTION

All governments collect and use personal information in order to govern. Democratic governments moderate this need with the requirements to be open to the people and accountable to the legislature, as well as to protect the privacy of individuals. Advances in information technology have greatly facilitated the collection and uses of personal information by the Federal Government, but also have made it more difficult to oversee agency practices and to protect the rights of individuals.

In 1974, Congress passed the Privacy Act to address the tension between the individual's interest in personal information and the Federal Government's collection and use of that information. The Privacy Act codified principles of fair information use that specified requirements agencies were to meet in handling personal information, as well as rights for individuals who were the subjects of that information. To ensure agency compliance with these principles, the act enabled individuals to bring civil and criminal suits if information was willfully and intentionally handled in violation of the act. In addition, the Office of Management and Budget (OMB) was assigned responsibility for overseeing agency implementation of the act.

At the time the Privacy Act was debated and enacted, there were technological limitations on the use of individual records by Federal agencies. The vast majority of record systems in Federal agencies were manual. Computers were used only to store and retrieve, not to manipulate or exchange information. It was theoretically possible to match personal information from different files, to manually verify information provided on government application forms, and to prepare a profile of a subset of individuals of interest to an agency. However, the number of records involved made such applications impractical.

In the 12 years since the Privacy Act was passed, at least two generations of information technology have become available to Federal agencies. Advances in computer and data communication technology enable agencies to collect, use, store, exchange, and manipulate individual records in electronic form. Microcomputers are now widely used in the Federal Government, vastly increasing the potential points of access to personal record systems and the creation of new systems. Computer matching and computer-assisted front-end verification are becoming routine for many Federal benefit programs, and use of computer profiling for Federal investigations is expanding. These technological advances enable agencies to manipulate and exchange entire record systems, as well as individual records, in a way not envisioned in 1974. Moreover, the widespread use of computerized databases, electronic record searches and matches, and computer networking is leading rapidly to the creation of a de *facto* national databasel containing personal information on most Americans. And use of the social security number as a de *facto* electronic national identifier facilitates the development of this database.

These technological advances have opened up many new possibilities for improving the efficiency of government recordkeeping; the detection and prevention of fraud, waste, and abuse; and law enforcement investigations. At the same time, the opportunities for inappropriate, unauthorized, or illegal access to and use of personal information have expanded. Be cause of the expanded access to and use of personal information in decisions about individuals, the completeness, accuracy, and relevance of information is even more important. Additionally, the expanded access and use make

'The term de *facto* national database is used to distinguish it from a national database that was created by' law, i.e. ! a de *jure* national database.

it nearly impossible for individuals to learn about, let alone seek redress for, misuse of their records. Even within agencies, it is often not known what applications of personal information are being used. Nor do OMB or relevant congressional committees know whether personal information is being used in conformity with the Privacy Act.

Overall, OTA has concluded that Federal use of new electronic technologies in processing personal information has eroded the protections of the Privacy Act of 1974. Many of the electronic record applications being used by Federal agencies, e.g., computer profiling and front-end verification, are not explicitly covered by the act or by subsequent OMB guidelines. The rights and remedies available to the individual, as well as agency responsibilities for handling personal information, are not clear. Even where applications are covered by the Privacy Act or related OMB guidelines, there is little oversight to ensure agency compliance. More importantly, neither Congress nor the executive branch is providing a forum in which the conflicts-between privacy interests and management or law enforcement interests—generated by Federal use of new applications of information technology can be debated and resolved. Absent such a forum, agencies have little incentive to consider privacy concerns when deciding to establish or expand the use of personal record systems.

POLICY PROBLEMS

OTA'S analysis of Federal agency use of electronic record systems, specifically for computer matching, front-end verification, and computer profiling, revealed a number of common policy problems.

First, new applications of personal information have undermined the goal of the Privacy Act that individuals be able to control information about themselves. As a general principle, the Privacy Act prohibits the use of information for a purpose other than that for which it was collected without the consent of the individual. New computer and telecommunication applications for processing personal information facilitate the use of information for secondary purposes, e.g., use of Federal employee personnel information to locate student loan defaulters, or use of Federal tax information to evaluate a Medicaid claim.

The expanded use and exchange of personal information have also made it more difficult for individuals to access and amend information about themselves, as provided for in the Privacy Act. In effect, the Privacy Act gave the individual a great deal of responsibility for ensuring that personal information was not misused or incorrect. Technological advances have increased the disparity between this responsibility and the ability of the individual to monitor Federal agency practices. For example, individuals may not be aware that information about them is being used in a computer match or computer profile, unless they monitor the *Federal Register* or questions about them arise as a result of the application. In computer-assisted front-end verification, individuals may be notified on an application form that information they provide will be verified from outside sources, but are unlikely to be told which sources will be contacted.

Additionally, new computer and telecommunication capabilities enable agencies to exchange and manipulate not only discrete records, but entire record systems. At the time the Privacy Act was debated, this capability did not exist. The individual rights and remedies of the act are based on the assumption that agencies were using discrete records. Exchanges and manipulations of entire record systems make it more difficult for an individual to be aware of uses of his or her record, as those uses are generally not of immediate interest to the individual.

Second, there is serious question as to the efficacy of the current institutional arrangements for oversight of Federal agency compliance with

the Privacy Act and related OMB guidelines. Under the Privacy Act, Federal agencies are required to comply with certain standards and procedures in handling personal information—e.g., that the collection, maintenance, use, or dissemination of any record of identifiable personal information should be for a necessary and lawful purpose; that the information should be current, relevant, and accurate; and that adequate safeguards should be taken to prevent misuse of information.

OMB is assigned responsibility for oversight of agency implementation of the Privacy Act. Prior studies by the Privacy Protection Study Commission (1977), the U.S. General Accounting Office (1978), and the House Committee on Government Operations (1975 and 1983) have all found significant deficiencies in OMB'S oversight of Privacy Act implementation. For example, under the Privacy Act, information collected for one purpose should not be used for another purpose without the permission of the individual; however, a major exemption to this requirement is if the information is for a "routine use' '—one that is compatible with the purpose for which it was collected. Neither Congress nor OMB has offered guidance on what is an appropriate routine use; hence this has become a catchall exemption permitting a variety of exchanges of Federal agency information.

Looking more specifically, OTA found that OMB is not effectively monitoring such basic areas as: the quality of Privacy Act records; the protection of Privacy Act records in systems currently or potentially accessible by microcomputers; the cost-effectiveness of computer matching and other record applications; and the level of agency resources devoted to Privacy Act implementation. OTA also found that neither OMB nor any other agency or office in the Federal Government is currently collecting or maintaining this information on a regular basis. Given the almost total lack of information concerning the activities of Federal agencies with respect to personal information, OTA conducted its own one-time survey of major Federal agencies and found that:

- the quality (completeness and accuracy) of most Privacy Act record systems is unknown even to the agencies themselves; few (about 13 percent) of the record systems are audited for record quality, and the limited evidence available suggests that quality varies widely;
- even though the Federal inventory of microcomputers has increased from a few thousand in 1980 to over 100,000 in 1985, very few agencies (about 8 percent) have revised privacy guidelines with respect to microcomputers;
- few agencies reported doing cost-benefit analyses either before (3 out of 37) or after (4 out of 37) computer matches; authoritative, credible evidence of the cost-effectiveness of computer matching is still lacking; and
- in most Federal agencies, the number of staff assigned to Privacy Act implementation is limited; of 100 agency components responding to this question, *33* reported less than 1 person per agency assigned to privacy and 34 reported 1 person.

Additionally, OTA found that there is little or no governmentwide information on, or OMB oversight of: 1) the scope and magnitude of computer matching, front-end verification, and computer profiling activities; 2) the quality and appropriateness of the personal information that is being used in these applications; and 3) the results and cost-effectiveness of these applications.

Third, neither Congress nor the executive branch is providing a forum in which the privacy, management efficiency, and law enforcement implications of Federal electronic record system applications can be fully debated and resolved. The efficiency of government programs and investigations is improved by more complete and accurate information about individuals. The societal interest in protecting individual privacy is benefited by standards and protections for the use of personal information. Public policy needs to recognize and address the tension between these two interests.

Since 1974, the primary policy attention with respect to Federal agency administration has shifted away from privacy-related concerns. Interests in management, efficiency, and budget have dominated the executive and legislative agenda in the late 1970s and early 1980s. Congress has authorized information exchanges among agencies in a number of laws, e.g., the Debt Collection Act of 1982 and the Deficit Reduction Act of 1984. In these instances, congressional debates included only minimal consideration of the privacy implications of these exchanges.

A number of executive bodies have been established to make recommendations for improving the management of the Federal Government, e.g., the President's Council on Integrity and Efficiency, the President Council on Management Improvement, and the Grace Commission. All have endorsed the increased use of applications such as computer matching, front-end verification, and computer profiling in order to detect fraud, waste, and abuse in government programs. However, these bodies have given little explicit consideration to privacy interests. Some executive guidelines remind agencies to consider privacy interests in implementing new programs, but these are not followed up to ensure agency compliance.

In general, decisions to use applications such as computer matching, front-end verification, and computer profiling are being made by program officials as part of their effort to detect fraud, waste, and abuse. Given the emphasis being placed on Federal management and efficiency, agencies have little incentive to consider privacy concerns when deciding to establish or expand the use of personal record systems. As a result, ethical decisions about the appropriateness of using certain categories of personal information, such as financial, health, or lifestyle, are often made without the knowledge of or oversight by appropriate agency officials (e.g., Privacy Act officers or inspectors general), OMB, Congress, or the affected individuals.

Fourth, within the Federal Government, the broader social, economic, and political context of information policy, which includes privacy-related issues, is not being considered. The complexity of Federal Government relations—within executive agencies, between the executive and legislature, between the Federal Government and State governments, and between the Federal Government and the private sector—is mirrored in interconnecting webs of information exchanges. This complexity and interconnectedness is reflected in myriad laws and regulations, most of which have been enacted in a piecemeal fashion without consideration of other information policies.

Some of these policies may be perceived as being somewhat inconsistent with others, e.g., the privacy of personal information and public access to government information. Some laws and regulations may only partially address a problem, e.g., Federal privacy legislation does not include policy for the private sector or for the flow of information across national borders. In other instances, issues that are inherently related and interdependent, such as privacy and security, are debated and legislated in separate forums with only passing attention to their relationship.

Additionally, the Federal Government information systems, as well as its information policy, are dependent on technological and economic developments. Federal funding for research and development and Federal financial and market regulations will have significant implications for information technologies and markets. Yet, under the present policymaking system, there is no assurance that these implications will be considered. Likewise, the international information policy environment, as well as international technological and economic developments, affects domestic information policy; again, these factors are not systematically considered in the existing policy arenas.

POLICY ACTIONS

OTA identified a range of policy actions for congressional consideration:

1. Congress could do nothing at this time, monitor Federal use of information technology, and leave policymaking to case law and administrative discretion. This would lead to continued uncertainty regarding individual rights and remedies, as well as agency responsibilities. Additionally, lack of congressional action will, in effect, represent an endorsement of the creation of a de *facto* national database and an endorsement of the use of the social security number as a *de facto* national identifier.
2. Congress could consider a number of problem-specific actions. For example:
   - establish control over Federal agency use of computer matching, front-end verification, and computer profiling, including agency decisions to use these applications, the process for use and verification of personal information, and the rights of individuals;
   - implement more controls and protections for sensitive categories of personal information, such as medical and insurance;
   - establish controls to protect the privacy, confidentiality, and security of personal information within the microcomputer environment of the Federal Government, and provide for appropriate enforcement mechanisms;
   - c review agency compliance with existing policy on the quality of data/records containing personal information, and, if necessary, legislate more specific guidelines and controls for accuracy and completeness;
   - review issues concerning use of the social security number as a de *facto* national identifier and, if necessary, restrict its use or legislate anew universal identification number; or
   - review policy with regard to access to the Internal Revenue Service's information by Federal and State agencies, and policy with regard to the Internal Revenue Service's access to databases maintained by Federal and State agencies, as well as the private sector. If necessary, legislate a policy that more clearly delineates the circumstances under which such accesses are permitted.
3. Congress could initiate a number of institutional adjustments, e.g., strengthen the oversight role of OMB, increase the Privacy Act staff in agencies, or improve congressional organization and procedures for consideration of information privacy issues. These institutional adjustments could be made individually or in concert. Additionally or separately, Congress could initiate a major institutional change, such as establishing a Data Protection or Privacy Board or Commission.
4. Congress could provide for systematic study of the broader social, economic, and political context of information policy, of which information privacy is a part.

ABOUT THE REPORT

Chapters 2 through 6 of this report provide technical and policy analyses relevant to electronic record systems privacy, and to proposed legislation such as: the "Data Protection Act of 1985" that would establish a Data Protection Board as an independent agency of the executive branch; possible amendments to the Privacy Act and Paperwork Reduction Act; and management improvement legislation.

Appendix A to this report updates trends and issues relevant to the privacy of information in computerized criminal history record systems, the subject of a prior OTA study. Ap-

pendix B describes the methodology of and respondents to the OTA survey (known officially as the OTA Federal Agency Data Request). Appendix C lists the OTA contractor papers relevant to this report. Appendix D lists the outside reviewers and contributors. Appendix E summarizes the Deficit Reduction Act regulations on front-end verification. Appendix F describes the privacy and data protection policies in selected countries.

Other components of this OTA assessment include the October 1985 OTA report on *Electronic Surveillance and Civil Liberties* that discusses issues and options relevant to electronic communications privacy, and the February 1986 OTA report on *Management, Security, and Congressional Oversight* that discusses, among other things, management, technical, and legal issues and options relevant to protecting the security (and, hence, privacy) of computer systems.