Chapter 6

Policy Implications

Contents

Table

Chapter 6

Policy Implications

SUMMARY

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. In the United States, these needs are recognized in the Constitution and various public laws.

In 1974, Congress passed the Privacy Act to address the tension between the individual's interest in privacy and the government need to know. Since the act was passed, there have been dramatic changes in the scale and scope of technological innovations applied to records and record systems, primarily as a means to detect fraud, waste, and abuse, and to aid in law enforcement investigations. New technological applications—most notably the widespread use of microcomputers, computerized record searches, and computer networking—have multiplied within Federal agencies, and have expanded the opportunities for inappropriate, unauthorized, or illegal access to and use of personal information. Individual rights and remedies, as well as administrative responsibilities, are not clear under current policies. At the same time, there is stronger public concern for privacy and more support for legislative protections than there was in the past.

OTA'S analysis of Federal use of electronic record systems 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. Second, there is serious question as to the efficacy of the current institutional arrangements for oversight of Federal compliance with the Privacy Act and related Office of Management and Budget (OMB) guidelines. 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. Fourth, within the Federal Government, the broader social, economic, and political context of information policy, which includes privacy-related issues, is not being considered.

Overall, OTA has concluded that Federal agency use of new electronic technologies in processing personal information has eroded the protections of the Privacy Act of 1974. Many applications of electronic records being used by Federal agencies, e.g., computer profiling and front-end verification, are not explicitly covered either by the actor subsequent OMB guidelines. Moreover, the use of computerized databases, electronic record searches and matches, and computer networking is leading rapidly to the creation of a de *facto* national database 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. Absent a forum in which the conflicts generated by new applications of information technology can be debated and resolved, agencies have little incentive to consider privacy concerns when deciding to establish or expand the use of personal record systems.

Additionally, OTA'S analysis of electronic record systems and their effect on individual privacy has confirmed once again the complexity of Federal information policy. Its broad social, economic, and political implications need systematic policy study.

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 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;
   - 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 a new universal identification number; or
   - review policy with regard to access to the Internal Revenue Service's (IRS) information by Federal and State agencies, and policy with regard to the IRS'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 access is 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.

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 information practices and to protect the rights of individuals.

In the 1960s, Congress and the executive branch began the first modern reexamination of the effects of government information collection on individual privacy and agency accountability. This occurred in response to two factors: first, the explosion in information activities necessitated by the Great Society programs; and second, the introduction in Federal agencies of large mainframe computers for information storage and retrieval. This reexamination went on for a number of years, and included, most prominently, the 1966 and 1967

hearings on the reposal to establish a National Data Center. the 1971 Senate Committee on the Judiciary hearings on Federal databanks,' the 1973 Department of Health, Education, and Welfare's Advisory Committee on Automated Personal Data Systems,[3] and the 1972 project on databanks sponsored by the Russell Sage Foundation and the National Academy of Sciences.[4]

The reexamination of government information collection, computers, and privacy culminated in the 1974 joint hearings of the Senate Committee on Government Operations, Ad Hoc Subcommittee on Privacy-and Information Systems and the Senate Committee on the Judiciary, Subcommittee on Constitutional Rights; '-and hearings of the House Committee on Government Operations.[C] These hearings coincided with Watergate and its revelation of how those in power could use and abuse personal information, especially that held by the IRS and the Federal Bureau of Investigation, for their own personal advantage. The result of these hearings was the enactment of the Privacy Act of 1974, which established rights and remedies for individuals who are the subjects of agency recordkeeping and specified requirements that Federal agencies were to meet in handling personal information. In addition, OMB was assigned responsibility for overseeing agency implementation of the act.

Technology.—At the time the Privacy Act was debated and enacted, there were technological limitations on how agencies could use individual records. The vast majority of Federal record systems were manual. Computers were used only to store and retrieve, not 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 enactment of the Privacy Act, 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, as well as entire record systems, in electronic form. Specifically:

- Microcomputers were not used at all by Federal agencies in the 1970s. Agencies responding to the OTA survey reported a few thousand microcomputers in 1980, with a dramatic increase to over 100,000 in 1985.
- Computer matching was not used by Federal agencies until 1976, and from 1980 to 1984 there was almost a threefold increase in the number of computer matches. Computer matching has become routine in a number of programs, especially eligibility benefit programs.
- Use of computer-assisted front-end verification, especially with on-line computer searches, has intensified in the 1980s, particularly following the requirements of the 1984 Deficit Reduction Act.
- The widespread use of computerized data-

[1]U.S. Congress, House Committee on Government Operations, Special Subcommittee on Invasion of Privacy, *The Computer and Invasion of Privacy,* hearings, 89th Cong., 2d sess,, July 26, 27, and 28, 1966 (Washington, DC: U.S. Government Printing Office, 1966); U.S. Congress, Senate Committee on the Judiciary, Subcommittee on Administrative Practice and Procedure, *Invasions of Privacy (Government Agencies),* hearings, 89th Cong., 2d sess., part 5, Mar. 23-30 and June 7-9, 14, and 16, 1966 (Washington, DC: U.S. Government Printing Office, 1967); and *Computer Privacy Hearings,* 90th Cong., 1st sess., Mar. 14-15, 1967 (Washington, DC: U.S. Government Printing Office, 1967).

[2]U.S. Congress, Senate Committee on the Judiciary, Subcommittee on Constitutional Rights, *Federal Data Banks, Computers and the Bill of Rights,* hearings, 92d Cong., 1st sess., Feb. 24-25 and Mar. 2,3,4,9, 10, 11, 15, and 17, 1971, part 1 (Washington, DC: U.S. Government Printing Office, 197 1).

[3]U. S. Department of Health, Education, and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, *Records, Computers and the Rights of Citizens* (Washington, DC: U.S. Government Printing Office, 1973).

[4]Alan F. Westin and Michael A. Baker, *Databanks in a Free Society (New* York: Quadrangle/New York Times Book Co., 19'72).

[5]U.S. Congress, Senate Committee on Government Operations, Ad Hoc Subcommittee on Privacy and Information Systems, and Committee on the <Judiciary, Subcommittee on Constitutional Rights, *Privac,y—The Collection, Use and Computerization of Personal Data,* joint hearings, 93d Cong., 2d sess., June 18-20, 1974 (Washington, DC: U.S. Government Printing Office, 1974).

[6]U.S. Congress, House Committee on Government Operations, *Privacy Act of 1974* (Report 93-1416), 93d Cong., 2d sess. (Washington, DC: U.S. Government Printing Office, 1974).

bases, electronic record searches and matches, and computer networking is leading rapidly to the creation of a de *facto* national database 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.

- In the 1970s, manual profiling was used by a few agencies, especially for law enforcement purposes. In the 1980s, computers can be used to generate profiles, and software programs can search databases on the basis of these profiles. The use of computer profiling is expanding beyond law enforcement per se to include various management programs, such as those designed to detect fraud, waste, and abuse.

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 this expanded access to and use of personal information in decisions about individuals, the completeness, accuracy, and relevance of information becomes even more important. Additionally, it is 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.

Information Technology and Fair Information Principles.–The core of the Privacy Act of 1974 is the code of fair information principles. Twelve years later, it is important to review these principles in light of current information technology applications and administrative practices. Although there are a number of iterations of the code of fair information principles, the model for the Privacy Act was the one developed by the Department of Health, Education, and Welfare's Advisory Committee on Automated Personal Data Systems, and hence will serve as the basis for the analysis here.

The first principle is that there must be no personal data recordkeeping system whose very existence is secret. Ensuring that all record systems containing personally-identifiable information are cataloged for the public record depends on each agency carefully monitoring its record systems. In an age of electronic record systems, it is difficult for an agency to keep an accurate catalog of all record systems, both because of the number of systems and because of the continual electronic changes and manipulations. Additionally, the multiplication of personal data systems makes it difficult for an individual to be aware of all the systems whose existence is public.

There are two types of record systems whose status under the Privacy Act is unclear. The first is a personal information system maintained on a microcomputer. Privacy Act officers are unsure of their responsibilities in this area and are looking for either legislative or OMB clarification.[7] The question is whether records maintained on microcomputers are analogous to 'desk notes, which are not covered by the Privacy Act, or whether they are of a different character because they can be retrieved by others and easily disseminated.

The second type of record system whose status is unclear is one that is developed as a result of electronic record searches-primarily computer matches, computer profiles, or computer screens. All electronic record searches generate a new file of those who appear in both systems or who meet the criteria of a profile or screen. Agencies argue that the Privacy Act notice procedures would not apply to these because they are only temporary systems that are destroyed in the process of verification,

[7] Panel on "Privacy Problems Relating to Computer Security, Seventh Annual Symposium on the Freedom of Information and Privacy Acts, sponsored by the Office of Personnel Management Government Executive Institute, Washington, DC, August 1985,

and, therefore, are not record systems under the Privacy Act.

The second principle of fair information practice is that there must be a way for an individual to find out what information about him or her is in a record and how it is used. Technology makes the first requirement of this principle even more important for individuals because more information is being collected from third parties as a result of computerization and on-line searches. While technology could offer individuals more ways to learn what is in their records, OTA found that no agencies have yet offered individuals computer access to their personal information.

Technology has also affected the requirement that there must be a way for an individual to find out how personal information is used. With computerization, the matching of records, searching of files based on profiles, and verifying of information with numerous other record systems have become routine for many record systems. The fact that the uses of information in government databases are increasing does not necessarily mean that individuals will not find out about such uses; however, OTA'S research indicates that agencies have generally not informed individuals, at least not in a direct fashion.

The third principle, that there must be a way for an individual to prevent information about him or her that was obtained for one purpose from being used or made available for another purpose without his or her consent, is affected most dramatically by new applications of technology. The principle includes not just knowledge of the uses of information, but also a means to prevent uses. Given the scale of government recordkeeping and the number of administrative uses of information, it appears to be extremely difficult for an individual to take action.

In computer matching, front-end verification, and computer profiling, information that was collected for one purpose, such as personnel or tax, is being used for another purpose, e.g., detection of fraud, registration for selective service, or payment of child support. In some cases, this principle has been overriden by legislation that has authorized the exchanges. In these instances, the legislative history reveals little explicit consideration of the effect on the fair information principles of the Privacy Act. In the majority of cases, these new uses of information have not been authorized by legislation, but instead have been justified under the routine use exemption of the disclosure pr~ visions in the Privacy Act. This exemption has been used for such a large number of information exchanges and for so many types that it now appears to mean that all uses of Federal records are permitted except those that are expressly prohibited.

The fourth principle of fair information practice is that there must be a way for an individual to correct or amend a record of identifiable information about him or her. This principle has become even more important in an age of electronic recordkeeping because more information is collected from parties other than the individual and because information is added to files at indeterminate periods. The increased exchanges and uses of information by Federal agencies make it more difficult to determine what information is maintained and how it is used; therefore it is harder for an individual to corrector amend records. On the other hand, in an age of electronic recordkeeping, it is possible that corrections to individual files could be negotiated via a home computer or agency computer, and agreed upon changes made directly into the system. Based on OTA'S research, it appears that no agency is using computers and telecommunications to provide new ways for an individual to amend records.

The fifth principle is that any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data. It is from this principle that the maxim that information must be accurate, timely, relevant, and complete has been taken [Public Law, 93-579, Sec. 3(e)(5)]. With electronic record systems, data are collected, manipulated, and exchanged much more quickly than in paper systems. The speed of exchanges

and large number of users make it more difficult to determine who is responsible for data reliability and use. Once again, the technology offers at least a partial solution in that audit trails can be built into systems. In addition, systems can be programmed to automatically purge records or separate data elements after a specified period of time. OTA found that agencies were not, on the whole, making use of the technology to ensure record quality, and were conducting few reviews of record quality.

Public Opinion.—In general, Americans do not believe that there are adequate safeguards for protecting the privacy of information about people.[8] The percentage of the public believing that personal information about them is being kept in files not known to them has increased from 44 percent in 1974 to 67 percent in 1983. Most Americans, from two-thirds to three-fourths, believe that agencies that release information they gather to other agencies or individuals are seriously invading personal privacy. Yet, a significant percentage of the public believes that public and private organizations do share personal information. Most Americans, 84 percent, believe that master files of personal information could be compiled "fairly easily," and 78 percent would regard this as a violation of their privacy.

There is increasing public support for additional government action to protect privacy. In 1978, two-thirds of the public responded that laws could go a long way to help preserve privacy. Sixty-two percent thought it was very important that there bean independent agency to handle complaints about violations of personal privacy by organizations. In 1982, over 80 percent of the public supported the major principles of the code of fair information principles. In 1983, large majorities of the public supported the enactment of new Federal laws to deal with information abuse, including laws that would require that any information from a computer that might be damaging to people or organizations must be double-checked thoroughly before being used, and laws that would regulate what kind of information about an individual could be combined with other information about the same individual.

[8]For a more complete discussion of public opinion and privacy, see ch. 2.

POLICY PROBLEMS

OTA's analysis of Federal agency use of electronic record systems, specifically for computer matching, computer-assisted 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 for locating student loan defaulters, or use of Federal tax information for evaluation of 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 for notices of such uses or unless questions about their personal information 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), 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 catch-all exemption permitting a variety of Federal agency information exchanges.

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 implementation of the Privacy Act. OTA also found that neither OMB nor any other agency or office in the Federal Government is, on a regular basis, collecting or maintaining information on Privacy Act implementation. Given the almost total lack of information on Federal agency personal information activities, 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, 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 government-wide information on or OMB oversight of: 1) the scope and magnitude of computer matching, computerized front-end verification, and computer profiling activities; z) the quality and appropriateness of the per-

sonal 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 a myriad of 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 these developments. 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; yet these factors are not systematically considered in the existing policy arenas.

POLICY ACTIONS

Overall, OTA has concluded that Federal agency use of new information technologies in processing personal information has eroded the protections of the 1974 Privacy Act. Many of the electronic record applications being used by Federal agencies, e.g., computer profiling and front-end verification, are not explicitly covered by either the act or subsequent OMB guidelines. Even where applications are covered by statute or executive 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 competing interests, such as management efficiency and law enforcement—generated by 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.

OTA has identified a range of policy actions for congressional consideration, including maintaining the status quo, problem-specific actions, institutional changes, and consideration of a national information policy. These policy actions are discussed below.

Action 1: Maintaining the Status Quo

> Congress could do nothing at this time, monitor Federal use of information technology, and leave policymaking to case law and administrative discretion.

The implication of maintaining the status quo is that the present policy problems and confusion will continue. It is likely that the policy emphasis on management efficiency; on detection and prevention of fraud, waste, and abuse; and on effective law enforcement will continue to take precedence over privacy-related concerns. This emphasis will most likely result in an increased use of current applications of information technology in Federal agencies for record searches such as computer matching, computer-assisted front-end verification, and computer profiling. In addition, it is likely that new applications will be developed.

Without congressional action, individuals will continue to be unaware of the majority of uses and disclosures of personal information by Federal agencies because there will be no notice other than that which appears in the *Federal Register*. If an individual has a question about agency practices and procedures, it is difficult for him or her to find the appropriate person to contact in a Federal agency. If an individual wishes to challenge an agency use of personal information, he or she will not have clearly defined or effective recourse because of the problems with the damage remedies of the Privacy Act.

Additionally, absent congressional action, there will be a lack of information available to Congress and the American people, as well as within agencies, concerning the scale and scope of technological applications applied to records and record systems in Federal agencies. This will make it even more difficult for Congress to be aware of current or proposed agency practices in order to exercise effective oversight. Moreover, the lack of information will aggravate the existing difficulties in monitoring the quality, e.g., accuracy and completeness, of personal information that is used and exchanged by Federal agencies.

If Congress does not address the problems resulting from Federal agency applications of

new information technology in processing personal information, then Federal agency staff will be left to interpret the meaning of the fair information principles in an electronic age. This would undermine a primary goal of the Privacy Act because it would increase the discretion of administrative agencies in handling personal information. Additionally, this would not meet the need expressed by some agency staff for more specific guidance from either OMB or Congress.

Most importantly, lack of congressional action will, in effect, represent an endorsement of the creation of a *de facto* national database containing personal information on most Americans, and an endorsement of the use of the social security number as a *de facto* national identifier. Current legislation, such as the Deficit Reduction Act of 1984, has accelerated what had been the gradual development of a national database because of the increased data searches and creation of computerized databases authorized by this legislation. Individual authorizations such as these have been largely unnoticed by the public. However, without consideration of the overall societal and political implications, these authorizations taken together could lead to personal information practices that most of the American public would find unacceptable.

Action 2: Problem-Specific Actions

Congress could also consider a number of problem-specific actions, dealing with computerized record searches, specific categories of information (social security number, tax information, and medical or other sensitive information), microcomputers, and record/data quality.

There are a number of procedural and substantive changes that Congress could legislate. In fashioning such changes, it would be easiest for Congress to deal with specific problem areas. Each of these will be discussed below. These changes are not mutually exclusive. Indeed, to provide the most comprehensive protection for personal information, it maybe necessary to legislate in all of these areas.

A. 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 information, and the rights of individuals.

In order to do this Congress could, in effect, require congressional approval for every record search involving personal information. This would entail amending the "routine use" provision of the Privacy Act to eliminate matching and other record searches from this exemption. As a result, agencies would need to obtain congressional authorization each time they wished to search records containing personal information. Although this approach would enable Congress to monitor record searches and to limit agency discretion in deciding to search records, it may involve a prohibitive time investment for Congress or be a de *facto* prohibition on such searches. Federal agencies likely would be opposed to such an approval process, as they might perceive it as unnecessary interference in internal agency affairs.

Alternatively, Congress could authorize general record searches, but establish explicit standards and procedures. This would require amending the Privacy Act in at least three possible ways:

1. Amend the "routine use" provision to allow record searches under specific circumstances and with specific types of records. In this way, Congress would establish the criteria under which matches and other searches could be done, and the types of records that could not be used in these searches (e.g., medical files or tax and security clearance records).
2. Specify the due process protections (e.g., notice, right to a hearing, right to confidentiality of results, or right to counsel) for persons whose records are to be searched, and the time when due process protections come into effect (e.g., before the match, after the match but before verification, and after verification).
3. Require a cost/benefit analysis before and after every match.

Although establishing standards and procedures may be more workable and realistic than requiring congressional approval for every record search, it does not provide any mechanism to ensure that agencies have complied with the general standards. Based on the experience of agency record searches to date, it appears that oversight and enforcement are essential.

In addition to any of the above amendments, or as an alternative, Congress could require agencies to adopt a 5-year plan for detecting fraud, waste, and abuse. In this way, agency proposals to search record systems would be placed within a context. Agencies would then need to justify record searches as a technique according to criteria such as purpose, cost, and alternatives considered. Such plans could be subject to congressional approval. Again, this would likely be ineffective without critical review, oversight, and enforcement.

Also, in addition to the above, Congress could amend the Privacy Act to require the social security number on all Federal, State, and local government forms. This might improve the accuracy of information used in matching, and might reduce the costs of verifying hits. However, it seems unwise to adopt this action without considering the problems with using the social security number as an authenticator and identifier, and the problem of endorsing a national identifier.

B. Implement more controls and protections for sensitive categories of personal information, such as medical and insurance.

Statutes provide specific protection in many areas where personal information is collected and used—e.g., banks, credit agencies, educational institutions, and criminal history repositories. Based on *United States v. Miller, 425* U.S. 435 (1976), if there is no specific statutory basis for an individual's right with respect to a particular type of personal information held by another party, the individual may not be able to assert a claim about how that information is used.

The Privacy Protection Study Commission (PPSC) analyzed the privacy implications of the recordkeeping practices in a number of areas, including insurance, employment, and medical care, and made recommendations for policy. Very few of these recommendations resulted in legislation, although some were embodied in voluntary codes by organizations such as insurance companies and employers.

Medical information is still an area in which an individual's interests are not protected by statute. In 1977, PPSC recommended that "now is the proper time to establish privacy protection safeguards for medical records. "g The Commission was led to this conclusion by the changing conceptions of the medical record and increased automation. Although many bills to protect medical information have been introduced, none has yet passed. The Federal Government collects, maintains, and discloses a great deal of sensitive medical information. Agencies involved include, for example, the Department of Health and Human Services (HHS), the Occupational Safety and Health Administration, the Environmental Protection Agency, and the Veterans Administration. Agencies collect medical information for purposes such as delivering services, providing cost reimbursements, and conducting research. Legislation could address these and other needs.

Legislating for a specific type of information or specific organizational entity on a piecemeal basis is not without its problems. OTA'S research indicates that it is difficult to isolate collection of personal information in this way. Instead, the information infrastructure is complex and constantly overlapping. Needs, interests, and programs converge at many points.

C. *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.*

[g]Privacy Protection Study Commission, *Personal Privacy in an Information Society* (Washington, DC: U.S. Government Printing Office, 1977), p. 290.

Agencies appear to be dealing with microcomputer policy on an ad hoc basis. This approach results in variation in the protection afforded personal information by Federal agencies. In establishing policy for the use of microcomputers withing Federal agencies, it is necessary to address the management, data integrity, security, confidentiality, and privacy aspects.

OTA'S companion report, Management, Security, and Congressional Oversight,[10] analyzes in detail the management, data integrity, and security aspects of information systems policy, including for microcomputers. Briefly, there are four general kinds of measures to protect information systems. First are administrative security measures, such as requiring that employees change passwords every few months; removing the passwords of terminated employees quickly; providing security training programs; storing copies of critical data off-site; developing criteria for sensitivity of data; and providing visible upper management support for security. Second are physical security measures, such as locking up diskettes and/or the room in which microcomputers are located, and key locks for microcomputers, especially those with hard disk drives.

There are also numerous technical measures to assure security, including audit programs that log activity on computer systems; security control systems that allow different layers of access for different sensitivities of data; encrypting data when they are stored or transmitted, or using an encryption code to authenticate electronic transactions; techniques for user identification; and shielding that prevents eavesdroppers from picking up and deciphering the signals given off by electronic equipment.

Lastly, there are legal remedies to discourage information system abuse, generally known as computer crime, and to prosecute perpetrators. Because computerized information is intangible, its abuses do not fit neatly into existing legal categories, such as fraud, theft, embezzlement, and trespass. This makes computer crime a different kind of criminal act needing special legislative attention. Concern with protecting the privacy of personal information is related to computer crime in that such crimes may involve unauthorized access to personal information.[11]

However, there are important aspects of privacy protection that are not addressed by the security measures discussed above. The Privacy Act establishes individual rights of knowledge, access, and correction, and places requirements on agencies to maintain records in a certain fashion, and to use and disclose records for certain purposes. These procedural and substantive protections are limited to records containing personal information that are "contained in a system of records." A system of records is defined as "a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual" [See.3(a)(5)]. It is unclear which records maintained on microcomputers come under this definition. Once this has been determined, it will be necessary to provide a means of monitoring these records to ensure that the individual rights of knowledge, access, and correction are provided.

D. 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.

A central aspect of Federal records policy, as embodied in the Privacy Act and Paperwork Reduction Act, is that records should be complete and accurate. Through the provisions in these acts, Congress has recognized the importance of record quality both to management efficiency and to the protection of individual

[10] U.S. Congress, Office of Technology Assessment, *Federal Government Information Technology: Management, Security, and Congressional Oversight,* OTA-CIT-297 (Washington, DC: U.S. Government Printing Office, February 1986).

[11] For further discussion of computer crime issues and policy options, see ibid., especially ch. 5. Also see U.S. Congress, Office of Technology Assessment, *Federal Government Information Technology: Electronic Surveillance and Civil Liberties,* OTA-CIT-293 (Washington, DC: U.S. Government Printing Office, October 1985).

rights. Agency decisions based on inaccurate or incomplete information can lead to wasteful or even harmful results. Many Federal record systems are now computerized. While computerized systems offer the potential to improve record quality, undetected or uncorrected errors can be disseminated more quickly and widely—with potentially serious consequences.

Based on available evidence, including the results of the OTA survey, OTA has concluded that most Federal agencies do not maintain statistics on record quality or conduct audits of record quality. While many agencies have policies and procedures intended to ensure record quality, they do not measure actual quality levels (by comparing record contents with primary information sources), and thus do not have a complete basis for knowing whether or not problems exist.

OTA asked Federal agencies (major components of all 13 cabinet departments plus 20 independent agencies) for the results of any record quality audits conducted on Privacy Act record systems and for record quality statistics on all computerized record systems maintained for law enforcement, investigative, and/or intelligence purposes. Only one agency provided any statistics, and very few of the other agencies indicated that such statistics may exist.

With respect to audits of the quality of Privacy Act records, only 16 of 127 (or 13 percent) agencies responding indicated that they conduct such audits; none provided the results.[12] Only one agency provided record quality statistics (for three systems under its jurisdiction) for law enforcement, investigative, and intelligence record systems. No statistics were provided for any of the other 82 systems reported.[13] Subsequent to the data request, the FBI was asked for and did provide the results of partial audits of the National Crime Information Center (see app. A for further discussion).

Should Congress wish to address the record quality problem directly, the appropriate congressional committees could conduct oversight on Federal electronic record quality, and, if satisfied that a significant problem exists, consider amendments to the Privacy Act and/or Paperwork Reduction Act to provide stronger guidance to the executive branch on this topic. Congress could also ask for General Accounting Office and/or Inspector General audits of record quality of selected Federal agency record systems in order to provide additional independent confirmation of Federal record quality. Finally, Congress could direct one or more of the central agencies responsible for information technology management (Office of Information and Regulatory Affairs, OMB; National Bureau of Standards; or Office of Information Resources Management, General Services Administration) to develop audit packages and techniques that could be used by Federal agencies to measure and monitor record quality.

E. Review issues concerning use of the social security number as a de facto *national identifier and, if necessary, restrict its use or legislate a new universal identification number.*

The Privacy Act makes it "unlawful for any Federal, State, or local government agency to deny to any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his social security account number' unless disclosure is required by law or unless the system of records was in existence prior to January 1, 1975 (the grandfather clause). Although the General Accounting Office, HHS, and numerous task forces all agree that "the social security number is, at best, an imperfect identifier and authenticator, 14 its use has expanded since 1974. The social security number is an impor-

[12] A total of 142 agencies were surveyed; 5 did not respond at all, and 10 others responded that the question was not applicable or that the information was not available, for a net total response of 127 agencies.

[13] Again, 142 agencies were surveyed; a total of 85 computerized law enforcement, investigative, or intelligence record systems were identified. Agencies responded as follows: record quality statistics maintained (3 systems); no record quality statistics (63 systems); no response (17 systems); not applicable or information not available (1 system); and classified (1 system).

[14] Privacy Protection Study Commission, *Personal Privacy in an Information Society*, op. cit., p. 609.

tant component in the matching process, and HHS has developed a software program, which will detect erroneous social security numbers, that is to be used in conjunction with a match.

Contrary to the stated intent of the Privacy Act, the trend in the use of the social security number appears to be towards its adoption as a de *facto* national identifier. Federal, State, and local agencies, as well as the private sector, have increased their requests, as well as their requirements, for disclosing one's social security number (or Taxpayer Identification Number). In hearings on the Privacy Act, concern with the possibility of the adoption of a universal identifier was voiced. Much of the concern focused on the record searches that a universal identifier would allow. Congress considered setting severe restrictions on the use of the social security number, but was dissuaded by testimony that the costs and implications of such restrictions were unknown. Since enactment of the Privacy Act, Congress has passed numerous laws authorizing Federal agencies to collect the social security number and requiring State agencies to collect it in administering Federal programs.

PPSC was asked to study restrictions on the use of the social security number and to make recommendations. The major finding of PPSC was "that restrictions on the collection and use of the social security number to inhibit exchange beyond those already contained in the law would be costly and cumbersome in the short run, ineffectual in the long run, and would also distract public attention from the need to formulate general policies on record exchanges. "[15] PPSC went on to recommend that "the Federal Government not consider taking any action that would foster the development of a standard, universal label for individuals, or a central population register, until such time as significant steps have been taken to implement safeguards and policies regarding permissible uses and disclosures of records about individuals. " Such a comprehensive study has not yet been conducted.

[15]Ibid., p. 614.

If the social security number is being used as a de *facto* standard universal identifier in the United States, both the benefits and hazards of having a national identifier need to be evaluated. The General Accounting Office, PPSC, congressional committees, and the Social Security Administration itself have all discussed parts of these issues. Congress could make a comprehensive review of issues concerning use of the social security number as a *de facto* national identifier and establish a clear policy for the electronic age, with appropriate enforcement mechanisms.

F. 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 access is permitted.

IRS files are valuable sources of information for many record searches because of the variety of information on file (e.g., address, earned income, unearned income, social security number, number of dependents) and because the information is relatively up to date. As a general rule, returns and return information are to remain confidential, as provided for in Section 6103 of the Tax Reform Act of 1976. Under this section, information may be disclosed for tax and audit purposes and proceedings, and for use in criminal investigations if certain procedural safeguards are met.

Additionally, Section 6103(1) allows for the disclosure of tax return information for purposes other than tax administration. The list has grown considerably since 1976, and includes: the Social Security Administration and Railroad Retirement Board (Public Law 94-455, 1976); Federal loan agencies regarding tax delinquent accounts (Public Law 97-365, 1982); the Department of Treasury for use in personnel or claimant representative matters (Public Law 98-369, 1984); Federal, State, and local child support enforcement agencies (Public

Law 94-455, 1976); and Federal, State, and local agencies administering certain programs under the Social Security Act or Food Stamp Act of 1977 (Public Law 98-369, 1984). Section 2651 of the Deficit Reduction Act also amends Section 6103(1) of the Tax Reform Act and allows information from W-2 forms and unearned income reported on 1099 forms to be divulged to any Federal, State, or local agency administering one of the following programs: Aid to Families With Dependent Children; medical assistance; supplemental security income; unemployment compensation; food stamps; State-administered supplementary payments; and any benefit provided under a State plan approved under Titles I, X, XIV, or XVI of the Social Security Act. Section 6103(m) of the Tax Reform Act also provides for disclosure of taxpayer identity information to a number of agencies, including the National Institute for Occupational Safety and Health and the Secretary of Education.

In all instances, Sections 6103(1) and (m) specify procedures that other parties are to follow in order to gain access to IRS information. Moreover, Federal, State, and local employees outside of IRS who handle IRS information are subject to the same criminal liabilities as IRS employees for misuse or disclosure of the information. The IRS also puts out a publication, *Tax Information Security Guidelines for Federal, State and Local Agencies* (Publication 1075; Rev. 7-83), that describes the procedures agencies must follow to ensure adequate protection against unauthorized disclosure.

Pressure to extend the list of agencies that can access IRS information has intensified with interest in record searches to detect fraud, waste, and abuse; to register men for the Selective Service; and for any program that requires a current address for an individual. The IRS's position is that its goal is to maintain a voluntary tax system and that the public's perception that tax information should remain confidential is important to maintaining a voluntary system. Thus, the IRS is, in principle, opposed to disclosing tax information.

Technological advances, however, may make voluntary disclosure of tax information by the affected individual less important and thus reduce the IRS's concern for confidentiality. For example, the IRS is moving towards a system where information provided by the individual would be phased out of the tax return process and replaced with information disclosed directly to the IRS by the sources, e.g., employers, banks, credit agencies, investment companies, mortgage companies, etc. If this becomes the case, the IRS will not need to be concerned with maintaining a voluntary tax system or with protecting the confidentiality of tax information.

Congress may wish to legislate a general, but enforceable, policy regarding the circumstances under which tax information may be disclosed and procedures for such disclosure. The ad hoc process of amending Sections 6103(1) and (m) when the political situation allows, as reflected in the long list of congressionally authorized disclosures, may not be the most effective approach to maintaining the confidentiality of tax information.

Congress may also wish to examine IRS access to other agency and private sector databases, and legislate a more clearly delineated policy for such access. This becomes more important as the IRS relies increasingly on sources of information other than the taxpayer. Additionally, IRS access to other databases may result in inaccurate or irrelevant information being included in IRS records.

Action 3: Institutional Changes

Congress could initiate a number of institutional adjustments, e.g., strengthening the oversight role of OMB, increasing the Privacy Act staff in agencies, or improving 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 estab**lishing a Data Protection or Privacy Board or Commission.**

Strengthening the institutional framework for information privacy policy could achieve

three purposes, either singly or in combination. First, an institution could play the role of an ombudsman in assisting individuals to resolve individual or class grievances with a Federal agency about personal information practices. Second, it could oversee Federal agency compliance with the Privacy Act and related OMB guidelines. Third, an institution could provide a forum in which proposals to alter personal information practices and systems (e.g., to conduct a computer match or to set up a new computerized database) could be discussed in the context of the implications for personal privacy and consistency with the principles of the Privacy Act.

In the increasingly complex, technological, and bureaucratic environment of the late 1980s, the fair information principles of the Privacy Act are even more important, but the Privacy Act scheme of enforcement and oversight appears to be increasingly anachronistic. For instance, it may not be realistic to ask individuals to control information about themselves in view of the cost and time burdens entailed. Also, the number of organizations that retain personal information is large, and the intricacies of their uses and disclosures of information are such that it appears almost impossible for most individuals to monitor how information is being used.

Moreover, the implicit assumption that each individual has a discrete interest in protecting his or her privacy, and that there is no larger societal interest, can be challenged. Many researchers and practitioners believe that there is also a social interest in maintaining certain boundaries of personal information collection and use. As discussed in chapter 2, the results of public opinion polls implicitly support this view.

There are three weaknesses in a personal information policy that provides for enforcement primarily through individual grievances and requires little direct oversight of agency practices.

First, *the policy relies on individuals to protect their interests.* The Privacy Act requires that individuals be aware of their rights, understand the potential threats posed by Federal agency collection and use of personal information, and be willing to invest the time and money necessary to protect their interests. These requirements place a burden on the individual. Every time one comes in contact with an agency seeking personal information, he or she would need to question the purposes for which information is sought and the necessity of each piece of information.

To ensure that information is not misused, the individual would need to follow up to make sure that no new information was added to the file, and that the uses and disclosures of information were in keeping with the agency's stated purposes. If individuals find that files contain inaccurate or irrelevant information, or that information was used for improper purposes, then they would need to know what legal remedies are available and take action against the Federal agency. Such a procedure means that individuals would need to be conscious of their rights at every stage of the information-handling process. Most people are so accustomed to disclosing information that they rarely think through all of the possible consequences. As Michael Baker suggests:

> What we can expect in the way of self-protective action on the part of individual citizens is severely limited by the fact that record-keeping practices are of relatively low visibility to and salience for the individual.[16]

The second weakness in the enforcement scheme of the Privacy Act is that *it only provides remedies once misuses have been identified.* If an individual has the right to correct inaccurate information or make a case for deleting or amending information in his or her record, the right only "rights" a wrong already committed against the individual. It does not protect the record from further errors or misuses, nor does it prevent similar wrongs from being committed against other individuals. It provides no preventive protection unless the granting of new rights to individuals can be

[16] Michael A. Baker, "Record Privacy as a Marginal Problem: The Limits of Consciousness and Concern, *Columbia Human Rights Law Review,* vol. 4, 1972, p. 89,

viewed as a means of deterring agencies from engaging in questionable information practices. But the time and money necessary to take action against a Federal agency make it unlikely that many individuals will take advantage of these rights. Thus, the deterrent effect of such rights on agency information practices is likely to be minimal.

The third weakness is that the personal information policy *is not sensitive to the existing imbalance of power between the individual and Federal agencies.* Under the Privacy Act, the interests of individuals are placed in opposition to the needs of the government for information. In most situations, the individual is dependent on the government for employment, credit, insurance, or some other benefit or service. Therefore, the individual is not likely to "afford" the risk of questioning an agency's information practices. Some view this as the most significant policy weakness and argue that:

> [the] enormous imbalance of power between the isolated individual and the great data collection organizations is perfectly obvious: under these conditions, it is a pure illusion to speak of "control." Indeed, the fact of insisting exclusively on means of individual control can in fact be an alibi on the part of a public power wishing to avoid the new problems brought about by the development of enormous personal data files, seeking refuge in an illusory exaltation of the powers of the individual, who will thus find himself alone to run a game in which he can only be the loser.[17]

Strengthening an existing institution or establishing a new one would bring more visibility to the issue of personal information collection and use; provide a central place for individuals to bring complaints and for agencies to seek advice; and enable Congress, the agencies, and the public to get more complete, accurate, and timely information on agencies' practices. The institution could also place limitations on the initial collection of information; review, and possibly approve, proposals to link record systems; and set standards for and oversee data quality in all systems.

A number of institutional changes available to Congress are discussed below:

A. Strengthen the role of the Office of Management and Budget in the enforcement and oversight of the Privacy Act.

Under the Privacy Act, OMB is responsible for providing guidelines and regulations, providing assistance to the agencies, overseeing the procedural mechanisms, and preparing the President Annual Report on Implementation of the Privacy Act. OMB has issued a number of guidelines, most significantly with respect to computer matching and the Debt Collection Act. However, in at least one instance–the guidelines released under the Debt Collection Act–OMB issued its guidelines without time for public comment.[18] In another instance, OMB did not issue guidelines as promised in a judicial action.[19] In addition, OMB has not yet acted on a requirement in the Paperwork Reduction Act to "submit to the President and the Congress legislative proposals to remove inconsistencies in laws and practices involving privacy, confidentiality, and disclosure of information."[20]

From the enactment of the Privacy Act in 1974 until 1980, OMB provided assistance through a separate office with a few staff members within its Information Policy Division. At this time, as the Privacy Protection Study Commission found, "neither OMB nor any of the other agencies with guidance responsibilities have subsequently played an aggressive role in making sure that the agencies are equipped to comply with the act and are, in fact, doing so."[21]

---

[17] S. Rodota, "Privacy and Data Surveillance: Growing Public Concern," *OECD Information Studies #10–Policy Issues in Data Protection and Privacy* (Paris: OECD, 1976), pp. 139-140.

[18] See comments of Christopher DeMuth, Administrator, Office of Information and Regulatory Affairs (OIRA), Office of Management and Budget (OMB), and Robert Bedell, Deputy Administrator, 01 RA, OMB, in *Oversight of the Privacy Act,* House Committee on Government Operations, Subcommittee on Government Information, Justice, and Agriculture, 1983, pp. 123-124.

[19] See *Bruce v. United States,* 621 F.2d 915 (8th Cir. 1980).

[20] See House Report No. 98-455.

[21] Privacy Protection Study Commission, *Personal Privacy in an Information Society,* op. cit., p. 21.

The Paperwork Reduction Act created the Office of Information and Regulatory Affairs with desk officers to oversee the implementation of information-related policies (including the Privacy Act) within an agency. Although this style of oversight does not necessarily mean that Privacy Act concerns receive less attention, it appears that this has been the practice. Testimony from Christopher DeMuth of OMB at the 1983 hearings on oversight of the Privacy Act[22] indicates (and interviews with OMB confirm) that the desk officers spend little time on Privacy Act matters.

OMB has focused its attention on the review of systems of records, as provided for in the Privacy Act. The act does not offer OMB any other specific guidance and OMB has not taken the initiative—e.g., by reviewing agencies' mechanisms for providing individual access and correction or for maintaining the accuracy of records.

OMB prepares the President's Annual Report on Implementation of the Privacy Act. Annual reports for the years 1975 through 1978 were well-documented studies of agency practices under the Privacy Act, and included descriptions of Federal personal information systems and agency administration, as well as data on use of the access and correction provisions of the act. The information contained in 1980 and 1981 reports was not as complete and focused mainly on systems that agencies designated as exempt from the Privacy Act. In 1982 debates on the Congressional Reports Elimination Act, OMB recommended that the Privacy Act Annual Report be eliminated. Congress rejected this suggestion.[23] The 1982-83 Annual Report on Implementation of the Privacy Act was not delivered to Congress until December 1985. This report synthesized Federal agencies' administration of the act over the past 10 years, and suggested areas for congressional action.

The goal of the Paperwork Reduction Act of 1980 was to reduce paperwork and improve information technology management. The act was designed to coordinate information-related activities of Federal agencies—specifically, automated data processing, telecommunications, office automation, information systems development, data and records management, and, possibly, printing and libraries. The act also acknowledged the importance of information as a resource and made a commitment to the management concept of information resources management, popularly known as IRM.[24]

Concern with protecting the confidentiality and security of personal information and providing individuals access to that information is part of the IRM concept. However, privacy has not been centrally integrated into IRM as presently implemented in Federal agencies. In part, this can be attributed to the fact that the Privacy Act and Paperwork Reduction Act are distinct pieces of legislation, with different public, congressional, and agency constituencies.

Another reason for the lack of integration and coordination is that OMB was somewhat slow to take a lead role in formulating IRM policy. In December 1985, OMB issued Circular A-130, "Management of Federal Information Resources, " which sets basic guidelines for the collection, processing, and dissemination of information by Federal agencies, and for the management of information systems and technology. The circular also revised and coordinated existing directives on privacy and computer security. Although the circular succeeds in centralizing information policy in one document, it does not contain any significant changes from previous congressional and OMB policies, and, in general, does not provide detailed guidance to agencies.

In terms of strengthening OMB'S role, Congress could to do three things. First, it could amend the Privacy Act, giving OMB the authority to issue regulations-not merely guide lines-and the authority to enforce them. Such

[22] "Oversight of the Privacy Act, ibid., pp. 123-124.
[23] See House Report No. 98 455.
[24] For a more complete discussion of IRM, see U.S. Congress, Office of Technology Assessment, *Federal Government Information Technology: Management, Security, and Congressional Oversight,* op. cit.

additional authority would put OMB in the role of policing agency personal information practices. The advantage of strengthening OMB authority is that it could be achieved with minor institutional change and minimal overhead. The major disadvantages are that agencies may resist this expansion in OMB'S authority, and that continued congressional oversight would be required to ensure that OMB was fulfilling its new responsibilities. Given OMB'S prior attention to this area and its other responsibilities, some of which may conflict with data protection/privacy, it may be questionable whether OMB could improve its oversight role even with additional authority.

Second, Congress could enhance OMB'S institutional base for dealing with the Privacy Act. This could be done by setting up a separate office with responsibility for data protection/privacy. In order for this office to be effective, Congress would need to ensure that adequate staff and budget are provided. Alternatively, Congress could increase the staff in the Office of Information and Regulatory Affairs and provide a separate staff person per agency who would be responsible for the privacy issues of that agency. Although the institutional framework is in place to achieve these changes quickly, the problem of ensuring OMB commitment to ensure compliance with the Privacy Act remains.

Third, Congress could upgrade the Office of Information and Regulatory Affairs, possibly by taking it out of OMB and establishing it as anew Office of Federal Management, as provided for in S. 2230, the "Federal Management and Reorganization and Cost Control Act of 1986. " This would have the advantage of removing the conflict that exists within OMB between budgetary constraints and management interests. However, it would be important to ensure that privacy be accorded equal importance with other management interests. The principal disadvantage of such a change is that it would be controversial, as it represents a major institutional reorganization.

B. *Increase the size, stature, and authority of privacy staff in agencies.*

Under the Privacy Act, each agency has designated an official who is responsible for Privacy Act matters. In many agencies, this official is also responsible for the Freedom of Information Act. In most agencies, there is little or no staff support for Privacy Act matters. The OTA survey revealed that 67 percent of agency components responding (67 out of 100) reported one FTE (full-time equivalent) staff person or less assigned to Privacy Act matters. Only 7 percent of agency components (7 out of 100) responding reported having 10 or more FTEs assigned to Privacy Act matters. Five of these components were located in the Department of Justice and included the Drug Enforcement Agency, Immigration and Naturalization Service, Federal Bureau of Investigation, and Criminal Division. The other agencies with more than 10 FTEs assigned to the Privacy Act were the Social Security Administration and the Office of the Secretary in the Department of Commerce.

Congress could amend the Privacy Act to require agencies to provide a certain level of professional and staff support for Privacy Act matters. Such an amendment could provide for adequate training conducted by both related agency staff (e.g., Freedom of Information Act officers, General Counsel staff, staff in the Inspector General's Office, and IRM personnel) and external groups (e.g., OPM'S Government Executive Institute and the American Society of Access Professionals).

In amending the Privacy Act, Congress could also specify the responsibilities and authorities of the Privacy Act officers, e.g., to serve as liaison between individuals and agencies in resolution of problems or grievances; to approve, or be consulted about, new record applications; and to maintain information on agency practices. If Privacy Act staff are to be effective in protecting privacy interests from within the agency, their authority must be stated in the legislation; otherwise it is possible that upper management will thwart their efforts.

The primary problem with this action is that enforcement and oversight responsibilities are

left within the agencies. Therefore, in addition to statutory changes, intensified congressional oversight of each agency may be required.

C. *Improve congressional organization and procedures for consideration of information privacy issues.*

At present, Congress does not have a mechanism for coordinated oversight of public laws and bills having privacy implications. Indeed, almost every committee has responsibility for some aspect of the personal information practices of Federal agencies. For example, issues related to the Privacy Act and privacy in general are of interest to the House Committees on Government Operations and on the Judiciary and the Senate Committees on Governmental Affairs and on the Judiciary; privacy issues involving school records are sent to the House Committee on Education and Labor and the Senate Committee on Labor and Human Resources; issues involving privacy of credit records are sent to the Committees on Banking in each House; privacy issues arising under the Freedom of Information Act are considered by the House Committee on Government Operations and the Senate Committee on the Judiciary; issues involving cable subscriber privacy are sent to the House Committee on Energy and Commerce and the Senate Committee on Commerce, Science, and Transportation; in the House, medical records confidentiality has been discussed by the Committees on Government Operations, Energy and Commerce, and Ways and Means, as well as by the Senate Committee on Energy and Commerce; and tax record confidentiality comes under the purview of the House Committee on Ways and Means and the Senate Committee on Finance.

Because of the fragmentation of the committee system and the primacy of substantive concerns in individual committees, privacy interests are often not given thorough consideration. Moreover, it is difficult for interest groups who define their roles as protecting privacy to keep track of relevant legislation and to monitor all pertinent congressional hearings.

If Committees with crosscutting privacy jurisdiction were established in both Houses, either as permanent committees, new subcommittees, or select committees, and all bills having privacy implications were referred jointly or sequentially to those committees, privacy issues could be debated and resolved in a more deliberate and focused manner. It is theoretically easy for Congress to make a change of this nature, but politically it is likely to be difficult as reform efforts of the past decade indicate.[25]

An easier alternative would be for Congress to retain the existing committee structure, but provide for better monitoring of bills having information privacy implications, and joint referral of such bills to committees with privacy jurisdiction.

D. *Establish a Privacy or Data Protection Board.*[26]

The proposal to establish an entity to oversee the personal information practices of Federal agencies is not new. The original Privacy Act that passed the Senate provided for the establishment of a Privacy Protection Commission with powers to:

- monitor and inspect Federal systems and databanks containing information about individuals;
- compile and publish an annual U.S. Information Directory so that citizens and Members of Congress will have an accurate source of up-to-date information about the personal data-handling practices of Federal agencies and the rights, if any, of citizens to challenge the contents of Federal databanks;
- develop model guidelines for implementation of the Privacy Act and assist agencies and industries in the voluntary development of fair information practices;
- investigate and hold hearings on violations of the act, and recommend corrective action to the agencies, Congress, the

[25] See, for instance, Steven S. Smith and Christopher J. Deering, *Committees in Congress* (Washington, DC: Congressional Quarterly Inc., 1984).

[26] The term "data protection" is a more precise term for the issues that arise from the collection and use of personal information. It is the term adopted by many European countries. However, privacy is the more easily understood term in the United States.

President, the General Accounting Office, and the Office of Management and Budget;
- investigate and hold hearings on proposals by Federal agencies to create new personal information systems or modify existing systems for the purpose of assisting the agencies, Congress, and the President in their effort to assure that the values of privacy, confidentiality, and due process are adequately safeguarded; and
- make a study of the state of the law governing privacy-invading practices in private databanks and in State, local, and multistate data systems. [27]

The Senate's Privacy Protection Commission was to be composed of five persons who were expert in law, social science, computer technology, civil liberties, business, and State and local government.

A professional staff would have been provided for the commission. The Senate Committee on Government Operations concluded:

> There is an urgent need for a permanent staff of experts within the Federal Government to inform Congress and the public of the data-handling practices of major governmental and private personal information systems. [28]

The Senate considered three alternative institutional placements for the commission—in the U.S. General Accounting Office, in OMB, or in an independent commission–and concluded that an independent commission was, on balance, the best solution. The House did not approve the establishment of a Privacy Protection Commission as it did not see the need for outside oversight of agency practices. As a compromise, both Houses approved the establishment of a Privacy Protection Study Commission to study further the personal information systems and practices of government and private organizations, to make recommendations as to whether the principles of the Privacy Act should be extended beyond Federal agencies, and to make other recommendations as the commission deemed necessary.

The Privacy Protection Study Commission released its report in 1977, and also recommended the establishment of a Federal Privacy Board or some other independent entity with responsibilities similar to those approved by the Senate in 1974. These include the responsibility to: monitor and evaluate the implementation of statutes and regulations; participate in agency proceedings; issue interpretative rules; continue to research, study, and investigate areas of privacy concern; and advise the President, Congress, government agencies, and the States on privacy implications of proposed statutes or regulations.[29]

Since 1977, there have been a number of bills creating a Privacy Commission or Data Protection Board, including H.R. 1721, the "Data Protection Act of 1985, " introduced in the 99th Congress. None has received serious congressional attention.

Many Western European countries and Canada have established boards or commissions with responsibilities for the protection of personal information. Because these may serve as a model for such an agency in the United States, descriptions of several countries are found in appendix F.

The advantages and disadvantages of a new privacy authority in the United States would be determined by the design of the agency and the powers with which it is vested. In this respect, a number of policy choices are important.

1. **Whether such an agency should have regulatory authority or advisory authority.** The data protection agencies in Sweden and France are regulatory agencies, with power to determine the personal information systems that government and private sector agencies can create, the information that can be retained, and the parties that can have access to the informa-

[27] U.S. Congress, Senate Committee on Government Operations, "Protecting Individual Privacy in Federal Gathering, Use and Disclosure of Information, " Report No. 93-1183, 93d Cong., 2d sess., 1974, pp. 23-24.

[28] Ibid, p. 24.

[29] Privacy Protection Study Commission, *Personal Privacy in an Information Society*, op cit, p. 37.

tion. The data protection agencies in West Germany and Canada have advisory authority and act as ombudsmen, serving as intermediaries between individuals and agencies, rendering advisory opinions, and lobbying for protection of personal information across a range of policy areas.

In the United States, it is likely that a regulatory agency would be resisted by existing Federal agencies because it would be perceived as having too much control over internal and day-today agency affairs. A regulatory agency may also become unwieldy and obstructive. An advisory/ombudsman authority may be more compatible with American philosophical and institutional traditions. It also has a precedent at the State level, e.g., New York. Based on the European and Canadian experience, the advisory/ombudsman model appears to have provided effective oversight of agency practices. Another possibility would be to establish an agency that is primarily advisory, but give it some veto power overparticular agency practices.

2. The institutional placement of such an authority. The major choice here is whether to make it independent of the executive branch and responsible to the legislature, or to make it part of the executive branch. If it were to be a new office or domestic council within the Executive Office of the President, it could have a great deal of visibility and stature if the President decided to make protection of personal information a priority. However, the stature of such a new office might well change with changes in administrations. Also, it could be politicized, especially if budgetary interests were given higher priority or if senior White House officials were interested in using personal information for political purposes—e.g., getting access to IRS information on political opponents or political activists.

Another possibility would be to have the authority established as a bureau within an existing executive department. The advantages of this option would be that it probably would be easier to establish and the overhead costs would be minimal. But, there are significant disadvantages. Inevitably, the power of the new authority would be dependent in part on that of the department, and its character shaped by the department. Additionally, any staff or line department, e.g., the Office of Personnel Management or the Department of Health and Human Services, collects and uses personal information, and, therefore, may have a conflict of interest in the resolution of information collection and disclosure policies.

A third possibility would be to have the authority established as an independent agency of the executive branch. While the agency head presumably would still report to the President, top officials could be made subject to Senate confirmation and even given statutory terms of office. These measures would help protect the authority from inappropriate political pressures and strengthen its institutional independence, as discussed later.

Alternatively, the new authority could report to Congress, either directly or through a special joint committee. The advantage of this approach is that an independent, nonoperating authority would have no stake in the existing personal information exchanges of executive agencies and might be more objective in resolving future conflicts. Moreover, an authority reporting to the legislature would increase the means Congress has to directly oversee the activities of executive agencies. Theoretically, a data protection/privacy authority reporting to the legislature, rather than to the executive, would have independence from the day-to-day operating constraints, as well as the political constraints, of executive agencies.

The disadvantage of having the new agency report to the legislature is that it might be subject to competing political interests, especially if there were different partisan majorities in the two Houses or if the executive and legislature were controlled by different parties. But, even if the authority became politicized, the political maneuverings might be more visible to Congress and the public if the authority re-

ported to Congress than if it were part of the executive. This would seem to ensure a certain degree of accountability.

In determining the placement and powers of a new agency, it will be important to consider the Supreme Court's recent decision in *Immigration and Naturalization Service v. Chadha, 103 S.* Ct. 2764 (1983), as well as its pending decision on the constitutionality of the Gramm-Rudman deficit reduction proposal.

3. The scope of issues for which the agency would be responsible. Some have proposed that such an authority should be responsible for all privacy issues, e.g., information privacy, surveillance, autonomy/life choices, and "chilling effects" on first amendment rights. If this were the case, information privacy would receive less sustained attention. Also, the size of the authority would, by necessity, be larger. Others have proposed that such an authority should be responsible for all information technology issues, for example, research and development, security, technology transfer, and industrial competitiveness. The same difficulties of focus and size would also apply to an authority with these responsibilities.

The uniqueness and complexity of problems presented by personal information collection and use argue that if an authority is established, it should be solely responsible for personal information issues—not all privacy issues or all information technology issues. However, the growing interrelationships between Federal and State personal information systems, and between public and private systems, argue that, to be effective, an authority would need the power to address all aspects of personal information exchanges. Limiting its purview to Federal agencies could narrow its effectiveness.

4. Outlining the agency's specific authority and responsibilities. Generally, such an agency is given some authority to require other agencies to register, or list, their personal information systems, with details on the information held, the sources of information, the uses, the period for which information is retained, and the exchanges and disclosures of information. This process of registration is supposed to ensure that there are no secret systems of personal records. Alternatively, the agency could be given the authority not only to register the systems, but also to approve their existence through a process of licensing. Additional responsibilities that could be considered include:

- some role in settling disputes over issues, such as access and accuracy, that develop between individuals and agencies;
- some role in formally making recommendations on proposed systems or new legislation that have implications for personal information;
- establishing guidelines and standards for specific personal information issues, e.g., what is an acceptable "routine use" or what is "accurate, timely, and complete' information;
- compilation and submission of an annual report on present and anticipated trends in personal information practices; and
- monitoring technological developments and assessing their implications for personal information practices.

5. Staffing a new authority. Two models exist for the organization of government agencies. One is to follow the independent regulatory agency model and have multiple commissioners appointed for staggered terms. Another is to have a single head for a fixed term of office. The advantage of the former is that partisan influences are minimized, while the advantage of the latter is that responsibility is clear and visible.

An additional issue is the size of the staff. The maximum number of staff reported for Western European and Canadian counterparts of such an authority is 30. Given the greater population and complexity of Federal/State relations, a somewhat larger staff may be necessary in the United States; however, there are advantages to keeping it small and well organized.

Congress might anticipate two arguments against a proposal to establish a new entity. The first is that it might entail another layer of bureaucracy. However, the purpose of a new

entity is to serve as a check on Federal agencies, not to become a part of the bureaucratic establishment. Additionally, the agency could be kept small and its style and organization nonbureaucratic. The second anticipated argument against a new entity would be that the costs associated with privacy protection may increase. This argument may be somewhat spe cious because, at present, there is no accounting of the costs associated with privacy protection. In calculating these costs, one would need to include agency administrative costs (e.g., the time of Privacy Act Officers, General Counsels, Inspectors General, program managers, and administrative judges); judicial costs (e.g., Department of Justice time and court costs); and the time of individuals.

Action 4: Consideration of a National Information Policy

Congress could provide for systematic study of the broader social, economic, and political context of information policy, of which privacy is a part.

OTA'S analysis of Federal agency electronic record systems and individual privacy has confirmed once again the complexity and interrelationships of Federal information policy. The broader social, economic, and political context of information policy is in need of systematic policy study. This discussion could occur in existing executive offices or congressional committees. Alternatively, or in concert, a national study commission could also provide a forum for discussion and examination of a national information policy.

A 1981 OTA study[30] found that there were numerous laws and regulations, some overlapping and some potentially or actually conflicting, that directly and indirectly affect the operators and users of information systems, the consumers of information services, and the subjects of personal information databanks. OTA concluded that continuation of this situation could inhibit many socially desirable applications of information systems or could create even more intractable policy problems in the future. At that time, OTA found that few policymakers were interested in a uniform Federal information policy that would encompass the problems that could arise from the many possible uses of data systems.

OTA identified the need for consideration of an "information policy" that would address the confusing array of laws and regulations—and their strengths, overlaps, contradictions, and deficiencies—within some overall policy framework. This need has not yet been met.

There have been numerous proposals for the establishment of new organizations to study information-related policy problems (see table 15 for a summary) .3' Over the last several years, a growing number of Members of Congress and industry leaders, while not necessarily endorsing specific policies, have expressed concern about the lack of coordinated focus on national information policy issues and the absence of adequate institutional mechanisms. For example:

- Representative George Brown (with Representatives Don Fuqua and Doug Walgren) has introduced legislation to establish an Institute for Information Policy and Research and a Special Assistant to the President for Information Technology and Science Information;[32]
- Senator Sam Nunn (with Senator Frank Lautenberg) has introduced legislation to establish an Information Age Commission;[33]
- Representative Cardiss Collins has introduced legislation to establish a new Office of Telecommunications Policy in the Executive Office of the President;[34]

[30]U.S. Congress, Office of Technology Assessment, *Computer-Based National Information Systems,* OTA-CIT-146 (Washington, DC: U.S. Government Printing Office, September 1981)

[31]For a more complete discussion of information policy, see U.S. Congress, Office of Technology Assessment, " Institutional Options For Addressing Information Policy Issues: A Preliminary Framework for Analyzing the Choices, staff memorandum prepared by the Communication and Information Technologies Program, Nov. 29, 1983.

[32]H.R. 744, "Information Science and Technology Act of 1985", 99th Cong., 1st sess.

[33]S. 786, "Information Age Commission Act of 1985", 99th Cong., 1st sess.

[34]H.R. 642, "Telecommunications Policy Coordination Act of 1985", 99th Cong., 1st sess.

Table 15.—Selected Institutional Changes for Information Policy Proposed in the 99th Congress

Proposed instiutional change	Problem or issues to which change directed	Organizational form	Functions	Membership	Location	Resources and authority	Duration
Information Age Commission, S 786 (Nunn and Lauten berg)	Impact of computer and communication systems on society	Commission	Research, policy formulation and information dissemination	23 members–6 from Congress 6 from executive branch and 11 from private sector	Independent–reporting to President and Congress	Hold hearings, negotiate and enter into contracts, and secure cooperation and assistance from other executive agencies	2 years
Off Ice of Federal Management, S 2230 (Roth)	Management of the Federal Government	Off Ice	Strengthen overall Federal management and, in particular financial management and Information resources management, and reduce the costs of administration	From OMB Will be transferred to the Off Ice of Federal Procurement Policy, Off Ice of information and Regulatory Affairs, and other appropriate functions of OMB A new Off Ice of Financial Systems Will also be established	Executive Off Ice of the President	Provide central policy direction and leadership in general management maintain oversight of managerial systems and processes, advise President and Congress	Permanent
Off Ice of Critical Trends Analysis, S 1031 (Gore) H R 2690 (Gingrich)	Identification and analysis of critical trends and alternate futures	Off Ice	Publish reports, advise President establish advisory commission, and promote public discussion	–	Within Executive Off Ice of the President	Legislation requires President to submit report to Congress and requires Joint Economic Committee to prepare report on similar topic	On-going–prepare report every 4 years beginning in 1990
Institute for information Policy and Research, H R 744 (Brown)	Broad range of information policy concerns	Institute	Research policy formulation Information dissemination and promotion of innovation	15 member board representing government industry and commerce, and academic and professional organizations	An Independent structure within the executive branch Director to coordinate with other agencies	–	10 years unless extended by Congress
National Technology Foundation, H R 745 (Brown)	High-technology small business. technology transfers, and international activties	Foundation	Analyze and make grants and contracts for development of high-technology small businesses, conduct technology assessments, promote technology transfer and international cooperation	Transfers to the Foundation the following agencies Patent and Trademark Off Ice, NBS, NTIS, parts of NSF, and other specified agency sections	Independent govern mental agency	Award grants, loans, and other assistance, conduct assessments, promote technology transfers	Authorizes appropriations for FY 1986 through FY 1988
Data Protection Board, H R 1721 (English)	Personal records held by Federal agencies	Board	Develop guidelines, provide assistance, publish guides Investigate compliance, Issue advisory opinions, intervene in agency proceedings	Three members appointed by President with advice and consent of Senate for 7-year terms	Independent executive agency	Conduct inspections, hold hearings issue subpoenas	Permanent
Department of International Trade and Industry, H R 1928 (Watkins)	International trade and Industry	Department	Full range including advising, negotiating, and regulating	Travel and Tourism Administration Patent and Trademark Off Ice, NBS, NTIS, Off Ice of Telecommunications and Information, Off Ice of Small Business Trade Assistance, and Off Ice of Competitive Analysis	Independent department	Legislation requires President under certain conditions to submit statement on impact on International economic competitiveness of significant domestic product and Service Industries	Permanent
Advanced Technology Foundation H R 2374 (LaFalce)	Technology inbusiness, commerce, and Industry	Foundation	Promote the commercial application and diffusion of advanced technology within Industrial sectors		Within executive branch	Create referral service coordinate programs provide grants, and develop Information management system	Authorizes appropriations through FY 1989

SOURCE Off Ice of Technology Assessment

- Representative Glenn English has introduced legislation to establish a Data Protection Board;[35]
- The American Federation of Information Processing Societies has formed a panel of experts on National Information Issues, and the Association of Data Processing Service Organizations has proposed a Temporary National Information Committee.[36]

Most of these proposals view information policy within the context of an information society, i.e., one in which the creation, use, and communication of information will play a central role. There are numerous, interconnected issues arising from the following factors:

- the need to have a greater understanding of the changing role of information and its impact on society;
- the economic and political transition to an information society;
- the effect that the information revolution may have on the governmental process;
- dealing with information as an economic resource, a commodity, and a property;
- the importance of managing information and in trying to assure its accuracy and high quality, especially insofar as it is generated, used, and disseminated by the Federal Government;
- the need to protect individual civil liberties and rights to privacy;
- ensuring access to information and equity that may arise when information is treated more and more as a commodity and less and less as a public good; and
- the enhanced ability of information to travel across nation-al boundaries.

In most discussions of information policy, the relative importance of these issues has not been noted. Indeed, numerous Federal agencies have a role in aspects of information policy, but there is no office or agency providing integration across multiple information policy issue areas. Agencies that might provide such integration, such as the National Telecommunications and Information Administration (in the Department of Commerce) and the Office of Science and Technology Policy (in the Executive Office of the President), have not been provided the necessary mandate and resources, nor do they appear, at least at present, to have the desire to carry out such activities.

Proponents of a national information policy argue that it is just as important as national economic or environmental or defense policy, and deserves a clear focus at the highest levels of government. Beyond this, proponents point to the need for a mechanism to encourage high-level identification and understanding of and leadership on issues arising from the transition to an information society-including issues of protecting individual civil liberties and social equity and the development of information as a valuable economic as well as public good.

Opponents in the past have expressed concern about the dangers of centralizing too much authority over information policy in one place, and have favored continuation of a decentralized policy apparatus with coordination provided through interagency and White House working groups. Some of this concern reflects the experience with the old Office of Telecommunications Policy (created in 1970 in the Executive Office of the President and terminated in 1977). OTP was perceived in part as attempting to influence the content of broadcast news. This raised the specter of a high-level government censorship office.

Realistically, it maybe necessary to divide the information problem into more manageable pieces. Because of the urgency of the emerging privacy-related information problems and because there is no inherent group constituency for privacy rights, it may be timely to establish a study commission with responsibility for examination of these interrelated issues.

Two recent proposals for new study commissions in the information policy area include a "National Commission on Communications Security and Privacy" proposed in 1984 by

[35] H.R. 1721, "Data Protection Act of 1985", 99th Cong., 1st sess.

[36] AFIPS, *Washington Report,* July 1985, p. 5.

Representative Dan Glickman, of the House Committee on Science and Technology Subcommittee, and the "Information Age Commission" noted earlier. Any national commission on information policy would most likely be broad in scope and encompass many of the issue areas previously identified. A commission established along the lines of these proposals would have a finite lifetime, modest budget, and broad composition (e.g., with representatives from industry, labor, academia, State/local government, and Federal Government). Establishing a new commission need not be a substitute for other congressional policy actions. Indeed, a commission could be viewed as complementing related activities by Federal agencies and could help to improve public understanding of and focus on current and emerging information policy issues.