Chapter 2

Electronic Record Systems and the Privacy Act: An Introduction

Contents

Tables

Figures

Chapter 2

Electronic Record Systems and the Privacy Act: An Introduction

SUMMARY

Although privacy is a value that has always been regarded as fundamental, its meaning is often unclear. Privacy includes concerns about autonomy, individuality, personal space, solitude, intimacy, anonymity, and a host of other related concerns. There have been many attempts to give meaning to the term for policy purposes. In 1890, Samuel Warren and Louis Brandeis defined it as "the right to be let alone." In 1967, Alan Westin defined it as "the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others." This latter definition served as the basis for the Privacy Act of 1974 (Public Law 93-579).

The Privacy Act was enacted by Congress to provide legal protection for and safeguards on the use of personally identifiable information maintained in Federal Government record systems. The Privacy Act established a framework of rights for individuals whose personal information is recorded, and the responsibilities of Federal agencies that collect and maintain such information in Privacy Act record systems.

When the Privacy Act was debated and enacted, Federal agency record systems were still based largely on paper documents. In 1986, many Federal agency record systems are based largely on electronic record-keeping. Computers and telecommunications are used to process detailed information on millions of citizens. No longer is personal information merely stored in and retrieved from file cabinets; now large volumes of such information are collected, retrieved, disclosed, disseminated, manipulated, and disposed of by computers. Moreover, direct on-line linkages now make it possible to compare individual information with a host of public and private agencies. Computer tapes, software, and networking also make it possible to compare personal information stored in different record systems.

The Privacy Act, with the goal of providing the means by which individuals could control information about themselves, balanced the interests of Federal agencies in collecting and using personal information against the interests of individuals in controlling access to and use of that information. Technology has now altered that balance in favor of the agencies. Computers and telecommunication capabilities have expanded the opportunities for Federal agencies to use and manipulate personal information. For example, there has been a substantial increase in the matching of information stored in different databases as a way of detecting fraud, waste, and abuse, as will be discussed in chapter 3. Likewise, computers are increasingly being used to certify the accuracy and completeness of individual information before an individual receives a benefit, service, or employment, as will be discussed in chapter 4 on front-end verification. These technological capabilities appear to have outpaced the ability of individuals to protect their interests by using the mechanisms available under the Privacy Act.

In addition to technological threats to Privacy Act protections, several studies of the act's effectiveness have been critical of both agency implementation and Office of Management and Budget (OMB) oversight, and have questioned the individual's ability to use the remedies in a meaningful way. The technological changes have aggravated these problems, and have created some new ones as well.

OTA reached four general conclusions about individual privacy and electronic record sys-

terns that cut across all areas of information technology application:

1. Advances in information technology are having two major, and somewhat opposing, effects on the electronic record-keeping activities of Federal agencies. They are facilitating electronic record-keeping by Federal agencies, enabling them to process and manipulate more information with great speed. At the same time, the growth in the scale of computerization, the increase in computer networking and other direct linkages, the electronic searches of computerized files, and the proliferation of microcomputers are threatening Privacy Act protections.
2. Federal agencies have invested only limited time and resources in Privacy Act matters. Few staff are assigned to Privacy Act implementation, few agencies have developed agency-specific guidelines or updated guidelines in response to technological changes, and few have conducted record quality audits.
3. Privacy continues to be a significant and enduring value held by the American public. General concern over personal privacy has increased among Americans over the last decade, as documented by several public opinion surveys over the past 6 years. About one-half of the American public believes that computers are a threat to privacy, and that adequate safeguards to protect information about people are lacking. There is increasing public support for additional government action to protect privacy.
4. The courts have not developed clear and consistent constitutional principles of information privacy, but have recognized some legitimate expectations of privacy in personal communications.

An OTA survey of the use of information technology by Federal agencies revealed that:

- components within 12 cabinet-level departments and 13 independent agencies reported 539 Privacy Act record systems with 3.5 billion records. Forty-two percent of the systems were fully computerized, 18 percent were partially computerized, and 40 percent were manual. Of the large Privacy Act record systems (i.e., over 500,000 persons), 57 percent were fully computerized, 21 percent were partially computerized, and 22 percent were manual; [1]
- agencies responding reported an increase from a few thousand microcomputers in 1980 to about 100,000 in 1985;
- only about 8 percent of Federal agencies that responded have revised or updated their Privacy Act guidelines with respect to microcomputers; and
- only about 12 percent of agencies reported that they have conducted record quality audits.

[1]Agencies were asked to report only their 10 largest Privacy Act record systems. Twelve of thirteen cabinet departments responded (only the Department of Housing and Urban Development did not), as did 20 selected independent agencies. However, some major personal information collectors within cabinet departments (e.g., the Internal Revenue Service within the Department of the Treasury and the Departments of the Army and Navy within the Department of Defense) did not respond.

INTRODUCTION

The Federal Privacy Act of 1974 was enacted by Congress to provide legal protection for and safeguards on the use of personally identifiable information maintained in Federal Government record systems. The Privacy Act established a framework of rights for individuals and responsibilities for Federal agencies that collect and maintain personally identifiable information. This framework incorporates a number of "fair information principles" including, primarily, that there should be no secret record systems, individuals should be able to see

and correct their records, and information collected for one purpose should not be used for another.

At the time the Privacy Act was debated, Federal agency record systems were still based largely on paper documents, with some agencies using large mainframe computers for the storage and retrieval of information in very large record systems. By 1986, Federal agencies have become electronic environments with computers and telecommunications being used to process detailed information on millions of citizens. Agencies now use computers, often microcomputers, to collect, disclose, disseminate, manipulate, and dispose of personal information. Direct on-line linkages between computerized databases make it possible to almost instantaneously compare information. Additionally, computer tapes and computer software make it possible to compare entire record systems.

The Privacy Act, with the goal of providing the means by which individuals could control personal information, balanced the interests of Federal agencies in collecting and using personal information against the interests of individuals in that information. Computer and telecommunication capabilities have expanded the interests of Federal agencies in personal information and enhanced their ability to process it. These capabilities have also overshadowed the ability of individuals to use the mechanisms available in the Privacy Act because, in general, it is more difficult for them to follow what occurs during the information-handling process.

The use of computers and telecommunications for processing personal information also offers opportunities for protecting that information. Techniques such as passwords, encryption, and audit trails are available to protect the confidentiality and security of information in an electronic environment. Although their use may provide more protection for the individual, these techniques do not necessarily give the individual control over the stages of information processing, as provided for in the Privacy Act.

BACKGROUND

Privacy

Privacy is a value that continues to be highly esteemed in American society, yet its meaning, especially for policy purposes, is often unclear. Privacy is a broad value, representing concerns about autonomy, individuality, personal space, solitude, intimacy, anonymity, and a host of other related concerns. There have been many attempts to define a "right to privacy." In a seminal article, Warren and Brandeis[2] defined it as "the right to be let alone." They found the primary source for a general right to privacy in the common law protection for intellectual and artistic property, and argued that:

> ,.. the principle which protects personal writings and all other personal productions, not against theft and physical appropriation, but against publication in any form, is in reality not the principle of private property, but that of an inviolate personality.

Subsequent legal debates have been structured by two points raised by Warren and Brandeis. The first is whether privacy is an independent value whose legal protection can be justified separately from other related interests, such as peace of mind, reputation, and intangible property. The second is controversy over their definition of the "right to privacy" as the "right to be let alone." Such a definition is so broad and vague that the qualifications necessary to make such a definition practical in society negate the right itself.

Second only to the Warren and Brandeis article in influence on the development of legal thinking regarding protection of privacy in the United States is Dean Presser's 1960 *Califor-*

[2] "(The Right to Privacy," *Harvard* Law Revriew, 1890.

nia Law Review article, "Privacy. " His primary finding is that:

> At the present time the right of privacy, in one form or another is declared to exist by the overwhelming majority of the American courts.[3]

Presser analyzed four distinct torts—intrusion, disclosure, false light, and appropriation—that could be isolated in State common law decisions and that represented four different types of privacy invasions. Each of these torts depends on physical invasion or requires publicity, and hence offers little protection for privacy of personal information. Although Presser's analysis has received wide acceptance as a way of categorizing tort law relating to privacy, most legal scholars doubt that these traditional privacy protections in common law can, or should, be extended to cover more general privacy concerns.

In the mid-1960s, concern with the "privacy" of computerized personal information held by credit agencies and the government rekindled interest in defining a right to privacy. Edward Shils viewed privacy of personal information as:

> . . . a matter of the possession and flow of information, . . Privacy in one of its aspects may therefore be defined as the existence of a boundary through which information does not flow from the persons who possess it to others.[4]

Alan Westin conceived of privacy as "an instrument for achieving individual goals of self-realization, and defined it as "the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others.

The "right to privacy' as "the right to control information about oneself" has served as the definition for policy purposes in the United States. Various statutes have been designed to give individuals the means to control information about themselves. Such means include primarily the right to know and the right to challenge and correct. Organizations are also expected to follow "Principles of Fair Information Use, "[6] which establish standards and regulations for collection and use of personal information. See table 1 for a list of statutes providing protection for information privacy.

History of the Privacy Act

In the mid-1960s, Congress and certain executive agencies began to study the privacy implications of records maintained by Federal agencies. The congressional concern with privacy and individual records was precipitated by the 1965 Social Science Research Council proposal that the Bureau of the Budget establish a National Data Center to provide basic statistical information originating in all Federal agencies.

In 1966, the Senate Committee on the Judiciary, Subcommittee on Administrative Practice and Procedure[7] and the House Committee on Government Operations, Special Subcommittee on Invasion of Privacy,[a] held hearings on the proposals for a National Data Center. Both committees were unconvinced of the need for such a center or of its ability to keep data confidential. In 1967 and 1968, the House and Senate again held hearings on the proposal for a National Data Center, and remained unconvinced that such a center could adequately pro tect the privacy of individual records. The committees and various witnesses feared that once such a center was established, its limited role would not be maintained. There was also great

[3]William L. Presser, "Privacy," *California Law Review,* vol. *48, 1980, Pp. 383, 386.*

[4]Edward Shils, "Privacy: Its Constitution and Vicissitudes, " *Law and Contemporary Problems, vol. 31, 1966,* pp. 281, 282.

[5]Alan Westin, *Privacy and Freedom (New* York: Atheneum, 1967), p. 39.

[6]A "Code of Fair Information Practice" was first developed in: U.S. Department of Heath, Education, and Welfare, *Records, Computers and the Rights of Citizens* (Washington, DC: U.S. Government Printing Office, 1973).

[7]See U.S. Congress, Senate Committee on the Judiciary, Subcommittee on Administrative Practice and Procedure, *invasions of Privacy* (Government Agencies), Hearings, 89th Cong., February 1965, June 1966 (Washington, DC: U.S. Government Printing Office, 1965-67).

[a]See 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 25, 27, 28, 1966 (Washington, DC: U.S. Government Printing Office, 1966).

Table 2-1 .—Statutes Providing Protection for Information Privacy

Fair *Credit Reporting Act of* 1970 **(Public Law 91-508.15 U S.C 1681) requires credit Investigation and reporting agencies to make their records available to the subject, provides procedures for correcting Information, and permits disclosure only to authorized customers**

Crime *Control Act of* 1973 **(Public Law 93-83) requires that State criminal justice Information systems, developed with Federal funds, be protected by measures to insure the privacy and security of information**

Family Educational Rights and Privacy Act of 1974 **(Public Law 93-380 20 U.S.C. 1232(g)) requires schools and colleges to grant students or their parents access to student records and procedures to challenge and correct Information, and limits disclosure to third part [es**

Privacy *Act of* 1974 **(Public Law 93-579, 5 U S C 552(a)) places restrictions on Federal agencies' collection, use, and disclosure of per sonally identifiable Information, and gives individuals rights of access to and correction of such Information**

Tax *Reform Act of* **1976 (26 U S C 6103) protects confidentialty of tax Information by restricting disclosure of tax Information for nontax purposes The list of exceptions has grown since 1976**

Right to *Financial Privacy Act of* **1978 (Public** Law **95.630, 12 U S C 3401) provides bank customers with some privacy regarding their records held by banks and other financial Institutions, and provides procedures whereby Federal agencies can gain access to such records**

Privacy *Protection for Rape Victims Act of 1978* **(Public Law 95-540) amends the Federal Rules of Evidence to protect the privacy of rape victims**

Protection of Pupil Rights *of* **1978 (20 U S C 1232(h)) gives parents the right to Inspect educational materials used in research or ex perimentation projects, and restricts educators from requiring in - trusive psychiatric or psychological testing**

Privacy Protection Act of **1980 (Public Law 96.440, 42 U S C 2000(a)(a)) prohibits government agents from conducting unannounced searches of press offices and files if no one in the office ıs suspected of committing a crime**

Electronic Funds Transfer Act of **1978 (Public Law 95-630) provides that any Institution providing EFT or other bank services must notify its customers about third-party access to customer accounts**

Intelligence Identifies Protection Act of 1982 **(Public Law 97-200) prohibits the unauthorized disclosure of Information Identifying certain U S. Intelligence officers, agents, Informants, and sources**

Debt Collection *Act of* **1982 (Public Law 97-365) establishes due process steps (not Ice, reply. etc) that Federal agencies must follow before they can release bad debt information to credit bureaus.**

Cable *Communications Policy Act of* **1984 (Public Law 98-549) requires the cable service to inform the subscriber of the nature of per sonally identifiable Information collected and the nature of the use of such ınformation, the disclosures that may be made of such ınformation the period during which such ınformation Will be maintained, and the times during which an individual may access such information Also places restrictions on the cable services' collection and disclosures of such Information**

Confidentiality provisions **are Included in several statutes, including: the Census Act (13 U S C 9214), the Social Security Act (42 U S C 408(h)), and the Child Abuse Information Act (42 U.S.C. 5103(b(2)(e)))**

NOTE All statutes embody the same scheme of individual rights and fair infer mation practices

SOURCES Robert Aldrich Privacy Protection Law in the *United* **States** (NTIA **Re**port 82/98. May 1982 Sarah P Collins Citizens Control over Rec *orals Held by Third Parties (* CRS Report No 78 255, Dec 8 1978 and the Office of Technology Assessment

reluctance to condone the centralization of both personal information and responsibility for that information within an *executive agency.* Although the committees agreed that the existing situation was inefficient, they believed that such decentralized inefficiency was amenable to congressional oversight, whereas centralized efficiency would be more difficult to check. The proposal for a National Data Center was therefore rejected.

In 1970, the Senate Judiciary Committee, Subcommittee on Constitutional Rights, chaired by Senator Sam Ervin, Jr., began a 4-year study of Federal Government databanks containing personal information and held related oversight hearings.[8] These hearings and the survey of agencies conducted by the Ervin Subcommittee laid the groundwork for the Privacy Act of 1974.

In 1972, Alan Westin and Michael Baker, with the support of the Russell Sage Foundation and the National Academy of Sciences, released a report, *Databanks in a Free Society,* in which they concluded that computerization of records was not the villain it had often been portrayed to be. Their policy recommendations applied to both computerized and manual systems and included:

1. a "Citizen's Guide to Files";
2. rules for confidentiality y and data sharing;
3. limitations on unnecessary data collection;
4. technological safeguards;
5. restricted use of the social security number; and
6. the creation of information trust agencies to manage sensitive data.l"

[8] See 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, parts 1 and 11 (Washington. DC: U.S. Government Printing Office, 1971).

[9] Alan F, Westin and Michael A. Baker, *Databanks* in *a Free Society (New* York: Quadrangle The New York Times Book Co., 1972).

In 1973, the Secretary of Health, Education, and Welfare's Advisory Committee on Automated Personal Data Systems released its report, *Records, Computers and the Rights of Citizens,* in which it discussed three changes resulting from the use of computerized record-keeping:

1. an increase in organizational data processing capacity;
2. more access to personal data; and
3. the creation of a class of technical record-keepers.

It recommended the enactment of a Federal "Code of Fair Information Practice" that would apply to both computerized and manual systems. This code served as the model for the Privacy Act, as well as for the Council of Europe's 1974 "Resolution on the Protection of the Privacy of Individuals vis~a-vis Electronic Data Banks in the Private Sector. '[11] The major principles of the code include:

- There must be no personal data record-keeping system whose very existence is secret.
- 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.
- 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 other purposes without his or her consent.
- There must be a way for an individual to correct or amend a record of identifiable information about him or her.
- 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.[12]

In 1974, in the wake of Watergate, hearings on numerous privacy bills were held in both the Senate and the House.[13] In the subcommittee hearings, there was little disagreement on the need for individual rights with respect to personal information held by Federal agencies. Discussions centered instead on the logistics of enabling individuals to use these rights, and the specific fair information practices that agencies were to follow. The Senate version also provided for a permanent Federal Privacy Board with regulatory powers, while the House version provided no such oversight mechanism. As a compromise, the Privacy Protection Study Commission was created, and oversight responsibilities were given to the Office of Management and Budget.

In 1977, the Privacy Protection Study Commission released its comprehensive report, *Personal Privacy in an Information Society,* which analyzed the policy implications of personal record-keeping in a number of areas including credit, insurance, employment, medical care, investigative reporting, education, and State and local government.[14] The report made numerous policy recommendations, very few of which have been realized in statutory law.

Implementation of the Privacy Act

A number of studies have evaluated the implementation and effectiveness of the Privacy Act. Most notable are analyses done by the House Committee on Government Operations, the Privacy Protection Study Commission, and the General Accounting Office. All conclude

[11] Reprinted in *Privacy and Protection of Personal Information in Europe,* Staff Report of the Senate Committee on Government Operations (Washington, DC: U.S. Government Printing Office, March 1975).

[12] U.S. Department of Health, Education, and Welfare, *Records, Computers and the Rights of Citizens* (Washington, DC: U.S. Government Printing Office, 1973).

[13] See 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, *Privacy–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).

[14] Privacy Protection Study Commission, *Personal Privacy in an Information Society* (Washington DC: U.S. Government Printing Office, 1977) with five appendices: *Privacy Law in the State; The Citizen* as *Taxpayer; Employment Records; The Privacy Act of 1974: An Assessment; and Technology and Privacy.*

[15] *See* U.S. Congress, House Committee on Government Operations, Government Information and Individual Rights Subcommittee, *Implementation of the Privacy Act of 1974: Databanks (1975);* Privacy Protection Study Commission, *The*

that the act has been disappointing in providing protection for individuals from misuse of personal information by Federal agencies. For example, the Privacy Protection Study Commission reached three general conclusions:

1. the Privacy Act represents a large step forward, but it has not resulted in the general benefits to the public that either its legislative history or the prevailing opinion as to its accomplishments would lead one to expect;
2. agency compliance with the act is difficult to assess because of the ambiguity of some of the act requirements, but, on balance, it appears to be neither deplorable nor exemplary; and
3. the act ignores or only marginally addresses some personal-data record-keeping policy issues of major importance now and for the future. 'G

in his opening statement before hearings on oversight of the Privacy Act, Representative Glenn English, Chairman of the Subcommittee on Government Information, Justice, and Agriculture of the Committee on Government Operations, remarked that:

> One of my chief concerns is that the bureaucracy, with the approval of OMB, has drained much of the substance out of the Act. As a result, the Privacy Act tends to be viewed as strictly a procedural statute, For example, agencies feel free to disclose personal information to anyone as long as the proper notices have been published in the Federal Register. No one seems to consider any more whether the Privacy Act prohibits a particular use of information. 17

All of the studies evaluating the implementation and effectiveness of the Privacy Act cite its major weaknesses to be its reliance on individual initiative; the ambiguity of some of the act's requirements; the casual manner in which OMB has implemented and enforced the act; and OMB guidelines issued subsequent to the act that seem to contradict the purpose of the act. These studies report that the act has been used less than anticipated. This *is* attributed to the investment of time and money an individual must make, and to the finding that agencies have not made it easy to use the Privacy Act.

The purpose of the Privacy Act is "to provide certain safeguards for an individual against an invasion of privacy" [Public Law 93-579, sec. 2(b)]. To this end, the act stipulates that Federal agencies meet six major requirements. Each of these requirements, and agency experience to date in meeting each requirement, is discussed below.

Requirement 1

Permit an individual to determine what records pertaining to him are collected, maintained, used, or disseminated by such agencies.

To this end, agencies are to publish in the *Federal Register an* annual notice of the existence and character of all systems of records containing personal information, and a notice of any new systems of records or new uses of the information in an existing system. The purpose of this was to ensure that there were no secret systems of records by giving the individual notice of agency record-keeping practices. However, most agree that the *Federal Register* is not the ideal vehicle for such notice as it is not easily accessible to most people. In "The President's Annual Report on the Agencies' Implementation of the Privacy Act of 1974" for calendar years 1982 and 1983, OMB identified the effectiveness of the public notice process as one area for further study, noting that:

> The problem may lie in the method used to disseminate this kind of information. While the *Federal Register* stands as the official organ of the government, it is a publication with limited circulation read by few ordinary citizens.'*

Privacy Act of 1974: An Assessment (1977); General Accounting Office, *Agencies Implementation of and Compliance With the Privacy Act Can Be Improved (1978);* and House Committee on Government Operations, Government Information, Justice, and Agriculture Subcommittee, *Oversight of the Privacy Act of 1974 (1983).*

"Privacy Protection Study Commission, app. 4, op. cit., p. 77.

"House Committee on Government Operations, 1983, op. cit., p. 5.

[R]" The President's Annual Report on the Agencies' Implementation of the Privacy Act of 1974, " CY 1982-1983 (issued Dec. 4, 1985), p. 118.

In 1983, OMB, on the basis of the Congressional Reports Elimination Act of 1982 (Public Law 97-375), eliminated the requirement that agencies republish all of their system notices each year in the *Federal Register*. The reason offered for this decision was lack of public and congressional interest. OMB viewed agency republication as a duplication of the *Federal Register's* annual compilation of Privacy Act notices. OMB recently estimated that the elimination of this requirement, including its administrative expenses, had saved the government over $1 million.[19]

Additionally, the Privacy Act requires agencies to inform individuals, on an application form or on a separate form that individuals can retain, of the following information: 1) the authority that authorizes the solicitation of the information and whether disclosure of such information is mandatory or voluntary; 2) the principal purpose or purposes for which the information is intended to be used; 3) the routine uses that may be made of the information; and 4) the effects of not providing all or any part of the requested information [see Public Law 93-579, sec. 3(e)(3)]. See box A for an example of a Privacy Act notice.

Requirement 2

Permit an individual to prevent records pertaining to him obtained by such agencies for a particular purpose from being used or made available for another purpose without his consent.

To this end, agencies are to acquire the prior written consent of the individual to whom the record pertains before disclosing a record *unless* one of *twelve* exceptions is met [see Public Law 93-579, sec. 3(b)]. Included in this list are the releases of information to: 1) those officers and employees of the agency that maintains the record who have a need for the record in the performance of their duties; 2) the Bureau of the Census for census-related activities; 3) the National Archives of the United States for historical preservation; 4) a government agency for a civil or criminal law enforcement activity; 5) either House of Congress; and 6) the Comptroller General. The Debt Collection Act of 1982 added an exception for agency disclosure of bad debt information to credit bureaus.

Additionally, an agency may disclose a record without the consent of the individual if the disclosure would be for a "routine use, " defined as "the use of such record for a purpose which is compatible with the purpose for which it was collected" [Public Law 93-579, sec. 3(a)(7)]. If an agency intends to disclose personal information for a "routine use, " then it must publish a notice in the *Federal Register*. This exemption has proved to be quite controversial. In the 1983 Oversight of the Privacy Act Hearings, James Davidson, former counsel to the Senate Subcommittee on Intergovernmental Relations of the Committee on Government Operations, stated that the "routine use" exemption was:

> . . . designed to require that the agencies examine the data, see if the use that the other agency was going to put it to was compatible with the reason for which it was collected, then issue notice so the public and other agencies and OMB could comment on the propriety of the exchange.[20]

Davidson went on to note that this has not been the way that agencies have used the routine use exemption; rather, if agencies had been routinely exchanging information over the years, they have assumed that the routine use exemption allows them to continue.

There have been a number of legislative proposals to amend the "routine use' definition. The Privacy Protection Study Commission recommended that, in addition to the requirement that the use of a record be "compatible with the purposes for which it was collected, " the use also be "consistent with the conditions or reasonable expectations of use and disclosure under which the information in the record was provided, collected, or obtained. "[21] In the 1982

[19] 1 bid., p. 10.

[20] "House Committee on Government Operations, 1983, op. cit., p. 51.

[21] Privacy Protection Study Commission, app. 4, op. cit., p. 120.

Box A.—U.S. Department of Education Application for Federal Student Aid, 1986=87 School Year

INFORMATION ON THE PRIVACY ACT AND USE OF YOUR SOCIAL SECURITY NUMBER

The Privacy Act of 1974 says that each Federal agency that asks for your social security number or other information must tell you the following:

1. **Its legal right to ask for the information and wheiher [he law says you must give it;**
2. **what purpose the agency has in asking for it and how it will be used; and**
3. **what could happen if you do not give it.**

Our legal right to require that you provide us with your social security number for the Pell Grant and Guaranteed Student Loan programs is based on Section 7 (a) (2) of the Privacy Act Of 1974.

You must give us your social security number to apply for a Pen Grant or a Guaranteed Student Loan. We need the number on this form to be sure we know who you are, to process your application, and to keep track of your record. We also use your social security number in the Pen Grant Program in recording information about your college attendance and progress, in making payments to you directly in case your college does not, and in making sure that you have received your money. If you do not give us your social security number, you will not get a Pen Grant or a Guaranteed Student Loan.

We also ask you to voluntarily give us your social security number if you are using this form only to apply for financial aid under the College Work-study, National Direct Student Loan, and Supplemental Educational Opportunity Grant programs. We use your social security number in processing your application. If you do not give us your social security number, you may still receive financial aid under these three programs.

our legal right to ask for all information except your social security number is based on sections of the law that authorizes the Pell Grant, Supplemental Educational Opportunity Grant, College Work-Study, National Direct Student Loan, and Guaranteed Student Loan programs. These sections include sections 411, 4138, *443, 4&,* 425, 428, and 482 of the Higher Education Act of 1965, as amended.

If you are applying for Federal student aid under all five programs, you must fill in everything except questions 4-3 and *4-4* on either form, Step 12 on Form 1, and question 1-7 on Form 2. But if you are not applying for a pen Grant or a Sup plemental Educational Opportunity Grant. YOU can also skiP question 4-2 on either form. If you are using Form 1 and *you* are not applying for a Pen Grant or a Guaranteed Student Loan, you can skip questions 5-1 through 5-3 (as well as questions 4-3 and 4-4 and Step 12). Finally, if you are only applying for a Pen Grant and you are using Form 1, you can skip 7-2, 7-3, and 6-3 as well as questions 4-3 and 4-4 and Step 12. if you skip question *4-4,* we will count your answer as .. No" for that question.

We ask for the information on the form so that we can figure your '"student aid index" and "expected family contribution." The student aid index is used to help figure out how much of a Pen Grant you will get, if any. The student aid index or the expected family contribution may also be used to figure out how much other Federal financial aid you will get. if any, While you are not required to respond, no Pell Grant may be awarded unless this information is provided and filed as required under 20 U.S.C. 1070a; 34 CFR 690.11.

We will send your name, address, social security number, date of birth, student aid indices, student status, year in college, and State of legal residence to the college that you list in question 4-3 (or its representative), even if you check '"No" in question 44. This Information will also go to the State scholarship agency in your State of legal residence to help them coordinate State financial aid programs with Federal student aid programs. Also, we may send information to members of Congress if you or your parents ask them to help you with Federal student aid questions. We may also use the information for any purpose which is a ""routine use" listed in Appendix B of 34 CFR 5b.

and 1983 "President's Annual Report on the Agencies' Implementation of the Privacy Act of 1974, " problems with the interpretation and implementation of the "routine use" disclosure were identified as Privacy Act issues for further study. The "Annual Report" stated that it would 'be useful for the Congress to reconsider this problem and provide clearer guidance on routine use disclosures. "2[2]

[22]'' The President's Annual Report, " 1982-1983, op. cit., p. 121.

Requirement 3

Permit an individual to gain access to information pertaining to him in Federal agency records, to have a copy made of all or any portion thereof, and to correct or amend such records.

These individual rights are a cornerstone of the act; however, they have not been used as much as anticipated. Reasons offered include:

1. the time an individual must spend in communicating with an agency;

2. the possible difficulty in adequately identifying personal records for which access is requested; and
3. the lack of public awareness of these rights.

The Privacy Protection Study Commission concluded that:

> Agency rules on individual access, and on the exercise of the other rights the Act establishes, appear, in most instances, to be in compliance with the Act's rule-making requirements. Yet, they too are often difficult to comprehend, and because the principal places to find them are in the *Federal Register* and the *Code of Federal Regulations,* it is doubtful that many people know they exist, let alone how to locate and interpret them.[23]

An additional reason that this goal has not been realized is that there are seven exemptions to this requirement that are authorized by the Privacy Act itself. In general, these exemptions include those systems of records that include investigatory material compiled for law enforcement purposes or for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment or promotion, military service, Federal contracts, or access to classified material. Also exempt are those systems of records that are maintained in connection with providing protective services to the President or other individuals, and those that are required by statute to be maintained and used solely as statistical records [Public Law 93-579, sec. 3(k)].

In the 1979 "Annual Report of the President on the Implementation of the Privacy Act of 1974, " the individual access provisions were described as the "most apparently successful provision of the Act. "[24] It was reported that since 1977, agencies had recorded over 2 million requests for access and had complied with over 96 percent of the requests. But, the 1979 Annual Report noted that it was not clear whether the access requests were the "direct result of the Act" because of prior procedures by which employees and clients were given access to their records.[26] In the 1982-83 Annual Report, OMB reported that access requests and requests to amend records had declined for most of the agencies with major record holdings. OMB attributed this to the existence of other agency access policies (for example, for personnel records) that are used rather than filing a Privacy Act request.[2G]

Requirement 4

Collect, maintain, use, or disseminate any record of identifiable personal information in a manner that assures that such action is for a necessary and lawful purpose, that the information is current and accurate for its intended use, and that adequate safeguards are provided to prevent misuse of such information.

These "Fair Information Principles" are another cornerstone of the act. Yet, the agencies have loosely construed these requirements and have at times ignored them altogether. The Privacy Protection Study Commission concluded that:

> None of these several collection requirements and prohibitions appears to have had a profound impact on agency record-keeping practice, mainly because they are either too broadly worded or have been perceived as nothing more than restatements of longstanding agency policy .27

In testimony before the House Subcommittee on Government Information, Justice, and Agriculture, John Shattuck, then legislative director for the American Civil Liberties Union, reached a similar conclusion, stating that:

> The Code of Fair Information Practices which constitutes the core of the statute is so general and abstract that it has become little more than precatory in practice, and has proved easy to evade.[28]

The vagueness of the principles contributes to agencies' practices. T-he act does not define,

[23] Priva;y Protection Study Commission, app. 4, op. cit., p. 84.

[24] "Fifth Annual Report of the President on the Implementation of the Privacy Act of 1974, " Calendar Year 1979 (released August 1980), p. 11.

[25] Ibid.

[26] Ibid., p. 20.

[27] Privacy Protection Study Commission, app. 4, op. cit., p. 44.

[28] House Committee on Government Operations, 1983, op. cit., p. 273.

nor does it require agencies to set standards for, such terms as "current" or "necessary." The act also does not develop, nor does it require agencies to develop, procedures to ensure "accurate" information or "adequate safeguards . . . to prevent misuse. "

Requirement 5

Permit exemptions from the requirements with respect to records provided in this Act only in those cases where there is an important public policy need for such exemption as has been determined by specific statutory authority.

As discussed above, the exemptions for permission to disclose, and for access and correction, are broadly defined. However, overall, agencies exempt only a small percentage of their systems of records. In order to ensure that agencies only exempted systems of records where necessary, the Privacy Act requires that the President report annually on the operation of the exemption provision. In the 1979 Annual Report, OMB concluded that agencies have "implemented this provision in a thoughtful and sparing manner" and that:

- Only 14 percent of total systems have been exempted.
- Agencies have invoked exemptions to completely deny access in only 0.2 percent of cases.
- Agencies routinely screen records in exempt systems and release material not deemed to need protection."

In the 1982-83 Annual Report, OMB reported that, from 1975 to 1983, the number of exempt systems declined by over 16 percent.[30]

Requirement 6

Be subject to civil suit for any damages which occur as a result of willful or intentional action which violates any individual's rights under this Act.

This requirement is intended to provide individuals the means to enforce agencies to comply with the provisions of the act, if they were not satisfied with the outcome of an administrative appeal. The time and cost involved to bring a suit under the Privacy Act is often prohibitive. In addition, some individuals have used the Freedom of Information Act, rather than the Privacy Act, to gain access to their records, and thus cannot bring suit under the Privacy Act. Where individuals have used the Privacy Act, their civil suits have rarely been successful because of the need to find" willful or intentional" activity, because injunctive relief under the act is unclear, and because the courts have narrowly construed the circumstances under which an individual can recover damages.[31] Richard Ehlke of the Congressional Research Service summarized the situation as follows:

> Despite over seven years of operation, the case law under the Privacy Act is relatively undeveloped. The greater visibility of the Freedom of Information Act, the breadth of many of the Privacy Act exceptions, and the limited remedial scheme of the Act are undoubtedly factors in this development. Much of the litigation has focused on these aspects of the Act–the limitations inherent in the "record" and "system of records" triggers to the Act; the expansive law enforcement exemptions; the exceptions to the consensual disclosure requirement; and the limited remedies available to redress many violations of the Act.[32]

[30] "'President's Annual Report, 1979, " op. cit., p. **14.**
[30] "'President's Annual Report, 1982 -83," op. cit., p. 19.

[31] See Richard Ehlke, "Litigation Trends Under The Privacy Act, ' June 1983, *Congressional Research Service,* in *Oversight of the Privacy Act of 1974*, op. cit., pp. 437-469.
[32] Ibid., pp. 468-469.

FINDINGS

OTA has reached four general conclusions about individual privacy and electronic record systems that cut across all areas of application of information technology. Each finding is discussed below.

Finding 1

Advances in information technology are having two major, and somewhat opposing, effects on the electronic record-keeping activities of Federal agencies.

They are facilitating electronic recordkeeping by Federal agencies, enabling them to process and manipulate more information with great speed. At the same time, the growth in the scale of computerization, the increase in computer networking and other direct linkages, electronic searches of computerized files, and the proliferation of microcomputers are threatening Privacy Act protections.

In the early 1960s, the use of computers to process personal information in Federal agencies was in its beginning stages and Federal agencies were still largely paper environments.[33] At this time, most computing was done on large mainframes by central processing, and only record systems containing a large number of records were stored on computers. In 1975, the First Annual Report of the President on Implementation of the Privacy Act reported that 73 percent of the personal data systems subject to the act were totally manual, but the remaining 27 percent that were fully or partially computerized contained over 80 percent of the total individual records.[34]

In 1985, the increase in the number of computerized records is significant. In the OTA survey, agencies were asked to report their 10 largest Privacy Act record systems. Components within 12 cabinet-level departments[35] and 13 independent agencies[3G] reported a total of 539 Privacy Act record systems containing 3.5 billion records. Of these systems, 42 percent were totally computerized, 18 percent were partially computerized, and 40 percent were wholly manual (see table 2). More importantly, of the large systems of records (i.e., over 500,000 persons), 57 percent were totally computerized, 21 percent were partially computerized, and 22 percent were wholly manual (see table 3).

The qualitative changes that have occurred in the various stages of the information process as a result of computerization are also significant. No longer is information merely stored and retrieved by computer. Now information is routinely collected on computer tapes, used within an agency in computer form, exchanged with and disclosed to regional offices or other agencies in computer form, manipulated and analyzed with sophisticated computer software, and archived on computer tapes.

"Before the Privacy Act was passed, two surveys of the degree of computerization of Federal agency record systems were conducted. In 1966, the Senate Judiciary Subcommittee on Administrative Practice and Procedure conducted a survey of "government dossiers" to determine the extent and nature of Federal agencies' collection of personal information. The subcommittee determined that Federal files contained more than 3 billion records on individuals, and that over one-half of these records were retrievable by computers. [See: U.S. Congress, Senate Committee on the Judiciary, Subcommittee on Administrative Practice and Procedure, *Government Dossier* (Committee Print) (Washington, DC: U.S. Government Printing Office, 1967), pp. 7-9.] The Subcommittee on Constitutional Rights, chaired by Senator Sam Ervin, surveyed agencies and found that 86 percent of the 858 databanks with 1.25 billion records on individuals were, at least in part, computerized. The large percentage of computerization found by the Ervin study may be attributed in part to the fact that the study used the phrase "databank cent aining personal information about individuals." To many, "databank" may imply a computerized system; thus, it is likely that manual systems were underreported in the Ervin survey. (See U.S. Congress, Senate Committee on the Judiciary, Subcommittee on Constitutional Rights, *Federal Data Banks and Constitutional Rights,* 93d Cong., 2d sess., 1974.)

[34] *Federal Personal Data Systems Subject to the Privacy Act of 1974, First Annual Report of the President, Calendar Year 1975, Pp. 4-6.*

[35] Only the Department of Housing and Urban Development did not respond to this question at all. However, some major personal information collectors within cabinet departments (e.g., Internal Revenue Service within the Department of the Treasury and the Departments of the Army and Navy within DOD) did not respond.

[3G] Consumer Product Safety Commission, Federal Trade Commission, National Aeronautics and Space Administration, Nuclear Regulatory Commission, Securities and Exchange Commission, Selective Service System, Agency for International Development, Federal Election Commission, Federal Reserve System, Small Business Administration, National Archives and Records Administration, Commission on Civil Rights, and Arms Control and Disarmament Agency.

Table 2.—Privacy Act Record Systems Reported by Federal Agencies[a]

Agency	Fully computerized		Partially computerized		Subtotals		'Manual		Totals	
	Number of systems	Number of records	Number of systems	Number of records	Number of systems	Number of records	Number of systems	Number of records	Number of systems	Number of records
Agriculture	22	27.0	6	1.5	28	28.5	14	05	42	290
Commerce	13	8821	3	04	16	882.5	5	14	21	883.9
DOD	15	500	4	17	19	51. 7	32	36	51	553
Education	3	17	1	00	4	17	0	00	4	17
Energy	3	04	7	04	10	08	4	03	14	15
DHHS	26	1,3046	16	90	42	1,3136	20	901	62	1,4037
Interior	32	45	11	52	43	9.7	17	04	60	10.1
Justice	28	101 2	9	2244	37	325.6	31	22	68	3278
Labor	8	16	9	09	17	25	1	00	18	25
DOT	36	100	8	30	44	130	17	02	61	132
Treasury	16	488	6	36.1	22	849	20	4603	42	5452
State	0	00	1	200	1	20.0	9	902	10	1102
Independent agencies	27	224	15	10	42	23.4	44	51 4	86	748
Totals	229	2,454.3	96	3036	325	2,7579	214	700.6	539	3,4589

[a]Agencies were asked to report only their 10 largest privacy Act record systems Twelve of thirteen Cabinet departments responded (only the Department of Housing and Urban Development did not as did 13 out of 20 independent agencies (see appB al the end of this report for a list) and some major privacy record holders did not respond (e g the Internal Revenue Service n the Department of the Treasury and the Departments of Army and Navy in the Department of Defense)

[b]Millions of records

SOURCE Office Of Technology Assessment

Table 3.—Computerized and Manual Privacy Record Systems

	Large systems[a]		Medium systems[b]		Small systems[c]		Totals	
	Number	Number of persons	Number	Number of persons	Number	Number of persons	Number	Number of persons
100% computerized	43	1,653,336,199	105	11,277,938	81	237,240	229	1,664,851,377
Parilally computerized	16	285,880,382	41	3,912,622	39	213,790	96	290,006,794
100% manual	17	695,419,523	50	5,015.434	147	327,666	214	700,762,623

[a]Over 500. 000 person:
[b]o 001 10 500 000 persons
[c]Under 10 000 persons

SOURCE Office of Technology Assessment

Another significant change is the direct linkage of computer records via telecommunication systems. This allows for easy disclosure and exchange of information. On-line access can occur, for example, via private or public telephone lines or through local networks within an agency. One factor supporting the transition of Federal information systems to direct linkages is cost–the cost of a typical network interface was $500 in 1982, but is expected to drop to about $50 by 1987.[37] Another factor is the ease and efficiency to an agency official of communicating directly with the computer as information is collected or needed, rather than compiling transactions, batch= processing them on a tape at the end of the day or week, and waiting for a reply.

With such computer networking, the exchanges of information occur rapidly, often leaving no audit trail of who had access to the data or what changes were made. Monitoring the use of agency information becomes much more difficult in this environment. But, at the same time, the environment supports a vast increase in the exchange and manipulation of information, as well as an increase in the number of people having access to the *information.* In 1977, the Privacy Protection Study Commission warned that:

> The real danger is the gradual erosion of individual liberties through the automation, integration, and interconnection of *many small,* separate recordkeeping systems, each of which alone may seem innocuous, even benevolent, and wholly justifiable.[38]

[37]See Michael Killen, "The Microcomputer Connection to Local Networks," *Data* Communications, December 1982.

[38]Privacy Protection Study Commission, app. 4, op. cit., p. 108.

Another technological development that has implications for Privacy Act protections is efficient electronic searching through computer records. The two most common types of searches are computer matching and computer profiling (or computer screening). In a computer match, two sets of computer files are compared record by record to look for any individuals who appear in both files. In a computer profile or computer screen, a single computer file is searched for selected factors about a specific type of individual. Because of the importance of these electronic searches, each will be discussed in depth in the following chapters.

Another critical factor in the Federal agency technology environment in the mid-1980s is the microcomputer. The microcomputer puts the power of information collection, storage, retrieval, exchange, manipulation, and printing into the hands of discrete individuals. In doing so, it raises privacy, security, productivity, and management issues that had been irrelevant or dormant in other eras of information processing.[39]

Because of the control over information processing that microcomputers give users and because of their relatively low cost, the use of microcomputers has grown dramatically across all sectors of society. The Federal Government has not been immune to this trend. All agencies are experiencing an influx of microcomputers. The OTA survey revealed that the agencies surveyed had a few thousand microcomputers in 1980 and over 100,000 in 1985.

A major impetus in this demand for microcomputers within the Federal Government is the perceived need to increase productivity and efficiency. The broad range of information processing features that a microcomputer offers and the variety of software programs available make microcomputers attractive throughout an agency. For clerical work, microcomputers are used most often for document preparation and data entry .40 At the administrative level, microcomputers are used for accounting, budgeting, and planning. Microcomputers can be used by professionals for data analysis as well as document preparation. For technical users, microcomputers offer control over system design and programming.[41]

Microcomputers complicate the monitoring of the uses of personal information for two reasons. First, they make it easier for individual users to create their own systems of records. This complicates Privacy Act oversight because files created on microcomputers were not considered when the Privacy Act was enacted, and it may be impractical to subject them to the act. The Privacy Act applies to a "record" that is retrieved from a "system of records." The Privacy Act defines "record" to mean:

> . . . any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.

The act defines "system of records" to mean:

> . . . 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.[42]

If a file created and maintained on a microcomputer meets the criteria for a system of records, i.e., is retrieved by name, identifier, or other identifying particular, then individuals should have the right to access and amend their records. To do so, all microcomputer files containing records that are retrievable by name

[39]The KBL Group, Inc.,"Agency Profiles of Civil Liberties Practices," OTA contractor report, December 1984, p. 153.

[40]See U.S. Congress, Office of Technology Assessment, *Automation of America's Offices, OTA-CIT-287* (Washington, DC: U.S. Government Printing Office, December 1985) for an in-depth analysis of the effects of microcomputers in the workplace.

[41]"National Bureau of Standards, *Microcomputers: Introduction to Features and Uses,* Special Publication 500-110, March 1984, pp. viii-ix.

[42]"Privacy Act of 1974 (Public Law 93-579), sec. 3(a)(4)(5).

or other identifier would need to be reported to the Privacy Act Officer and noted in the Federal Register.

The second feature of the microcomputer that makes it difficult to monitor the uses of personal information is that a microcomputer serves as a remote terminal to access centralized systems of records. Such shifting of data from mainframes to microcomputers raises critical questions of data integrity and security. For example, when a record is being used by one user, there may be no other access to that information. More importantly, there may be no audit trail of additions and deletions." Additionally, there may be no indication of how current the records are, thus increasing the likelihood that inaccurate data will be disseminated.[44]

At the present time, most microcomputers in Federal agencies are desk-top models. The trend to portable computers—also known as briefcase, lap, or notebook computers—and transportable computers will aggravate the problems of data integrity and security, especially since information will be transported out of government offices into areas that are neither controlled nor secured. Another technological development that will have implications for the processing of personal information is the multiuser microcomputers, or "super microcomputers, which are used primarily for group work situations.

Finding 2

Federal agencies have invested only limited time and resources in Privacy Act matters. Few staff are assigned to Privacy Act matters, few agencies have developed agency-specific guidelines or updated guidelines in response to technological changes, and few have conducted record quality audits.

The Privacy Act allows agencies much latitude to develop their own arrangements for supervising implementation and compliance with the act. The only requirement the act places on agencies is to:

> . . . establish rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records, or in maintaining any record, and instruct each such person with respect to such rules and the requirements of this section, including any other rules and procedures adopted pursuant to this section and the penalties for noncompliance [Public Law 93-579, sec. 3(e)(9)].

In 1977, the Privacy Protection Study Commission reviewed agency experience and concluded that:

> . . . the 97 Federal agencies that maintain systems of records subject to the Privacy Act of 1974 have all taken different approaches to administration, training, and compliance monitoring. . . agencies or components of agencies that have carefully structured programs for administering the Act appear to be the ones in which the Act's objectives are being best achieved.[45]

Based on responses to the OTA survey of Federal agencies, 67 percent of agencies responding reported one (34 agencies) or less than one (33 agencies) full-time equivalent (FTE) staff assigned to Privacy Act matters. Only seven agencies reported ten or more FTEs assigned to Privacy Act matters, and six of these were located in the Department of Justice. The FBI reported the largest number of FTEs–65—assigned to Privacy Act issues.

The Privacy Act requires agencies to:

> . . . maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination [Public Law 93-579, sec.3(e)(5)].

OTA asked agencies to specify the procedures they follow to ensure Privacy Act record quality (for example, complete and accurate records). In response, most agencies submitted a copy of their policy directives con-

[44] National Bureau of Standards, op. cit., p. 96.
[44] The KBL Group, Inc., op. cit., p. 162.

[45] Privacy Protection Study Commission, app. 4, op. cit., p. 108.

taining general information and procedures for administering the Privacy Act. Only about 24 percent (30 agencies) have developed agency-specific guidelines or procedures for determining what is "relevant' and 'timely' information within their agency.

The results of the OTA survey also indicated that few agencies had conducted audits of record quality. Of 127 agency respondents, only about 13 percent (16 agencies) indicated that they conducted record quality audits. Of these 16 agencies, none provided copies of the results.[4a] With respect to record quality statistics for law enforcement, investigative, and intelligence record systems, only one agency provided statistics (for three systems under its jurisdiction). No statistics were provided for any of the other 82 systems reported.[47]

The OTA survey also asked whether agencies had revised or updated Privacy Act guide lines with respect to microcomputers. Of 119 agency respondents, only 8.4 percent (10 agencies) had done so. One agency noted that microcomputers were not used in connection with the maintenance of Privacy Act information; however, as was noted above, files on microcomputers or accessible through microcomputers may well fall under the Privacy Act "system of records" criteria.

Finding 3

Privacy continues to be a significant and enduring value held by the American public, as documented by several public opinion surveys over the past 6 years.

About one-half of the American public believes that computers are a threat to society, and that adequate safeguards do not exist to protect information about people. There is increasing public support for additional government action to protect privacy.

This finding is based on a comprehensive review of public opinion surveys that covered issues of technology and civil liberties, with special attention to the question of privacy and information practices.[48] Most studies, although privately sponsored, were designed and conducted by major public opinion research organizations such as Louis Harris & Associates, the Gallup Organization, the Roper Organization, the National Opinion Research Center, and the major news organizations.

A major difficulty in interpreting existing survey research is that most questions have emphasized general concerns about privacy and civil liberties, rather than specific concerns about the implications of particular uses of computing and information technologies, such as computer matching or computer profiling. As a result, much is known about abstract concerns for privacy, but little about levels of support or opposition to emerging technologies and their use by government agencies. An additional problem of survey research is that the meaning of responses is clouded by definitional differences in what constitutes an invasion of privacy, including definitions ranging from personal freedoms, solitude, and freedom from gossipy neighbors to freedom from governmental or employer surveillance. With these caveats in mind, a number of conclusions and trends about public opinion can be made.

General concern over personal privacy has increased among Americans over the last decade. When asked directly whether they are concerned about threats to personal privacy, most Americans will answer in the affirmative. In several Harris surveys[49] the following question was posed:

---

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

[47] 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).

[48] William H. Dutton and Robert G. Meadow, "Public Perspectives on Government Information Technology: A Review of Survey Research on Privacy, Civil Liberties and the Democratic Process," OTA contractor report, January 1985.

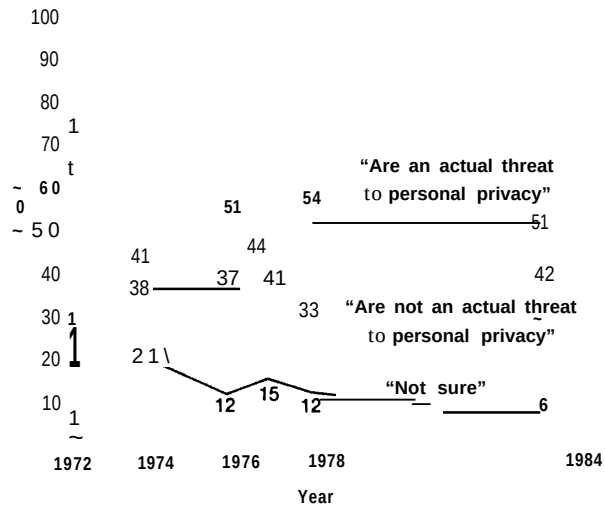
[49] Louis Harris & Associates, Inc., and Dr. Alan F. Westin, *The Dimensions of Privacy: A National Opinion Research Survey of Attitudes Toward Privacy* (conducted for Sentry Insurance), December 1979; and Louis Harris & Associates, Inc., *The Road After 1984: A Nationwide Survey of the Public and Its*

Now let me ask you about technology and privacy. How concerned are you about threats to your personal privacy in America today? Would you say you are very concerned, somewhat concerned, only a little concerned, or not concerned at all?

In 1983, 48 percent of the public described themselves as "very concerned. " This was double the 25 percent reported in January 1978 and a marked increase from 31 percent in December 1978. In 1983, an additional 29 percent described themselves as "somewhat concerned, " and only 7 percent said they were "not concerned at all, " a significant change from the 28 percent who so described themselves in January 1978. In addition, Americans overwhelmingly disagree (64 percent, compared with 27 percent who agree) with the statement that: "Most people who complain about their privacy are engaged in immoral or illegal conduct. " In other words, privacy is not merely an instrument for avoiding punishment or detection–it is seen as a legitimate value itself.

Most recently, about one-half of the American public believed that computers were a threat to privacy. As figure 1 indicates, the percentage perceiving computers as a threat has increased since 1974. In 1974, 38 percent of the respondents said computers were a threat and 41 percent said they were not. In 1977, 41 percent said computers were a threat and 44 percent said they were not a threat. In December 1978, 54 percent said they were a threat and only 33 percent indicated they were not. However in 1983, the percentage perceiving computers as a threat to privacy decreased slightly, while the percentage believing that computers are not a threat increased by approximately 10 percent. In 1982, Roper reported that 44 percent were very concerned with reports of abuse of personal information that is stored in computers, and 39 percent were very concerned about "reports of embezzlements and rip-offs through the use of a computer. "

Figure I.— Beliefs That Computers are an Actual Threat to Personal Privacy in This Country[a]



[a]Response 10 Do you feel that the present use of computers are an actual threat [o personal privacy in this country or not?

SOURCE. Lou Is Harris & Associates Inc *The Road After 1984 A Nationwide Survey of the Public and Its Leaders on the New Technology and Its Consequences for American Life* (conducted for the Southern New England Telephone for **presentation at the Eighth International** Smithsonian **Symposium, December 19S3)**

An increasing percentage of the public does not believe that the privacy of personal information in computers is adequately safeguarded –from 52 percent in 1978 to 60 percent in 1983. Although a majority of the public (60 percent) believes that computers have improved the quality of life,[50] a larger and increasing (68 percent in 1983) percentage of the public believes that the use of computers must be sharply restricted in the future if privacy is to be preserved .51

In general, citizens are concerned with the protections organizations provide for personal information. In 1979, 41 percent agreed and 41 percent disagreed with the statement: "Most organizations that use information about people have enough checks and safeguards against the misuse of personal information. " Government agencies were perceived as intrusive by about one-third of the public, with the Central Intelligence Agency, the Federal Bureau of Investigation, and government welfare agencies

Leaders on the New Technology and Its Consequences for American Life (conducted for the Southern New England Telephone for presentation at The Eighth International Smithsonian Symposium, December 1983.)

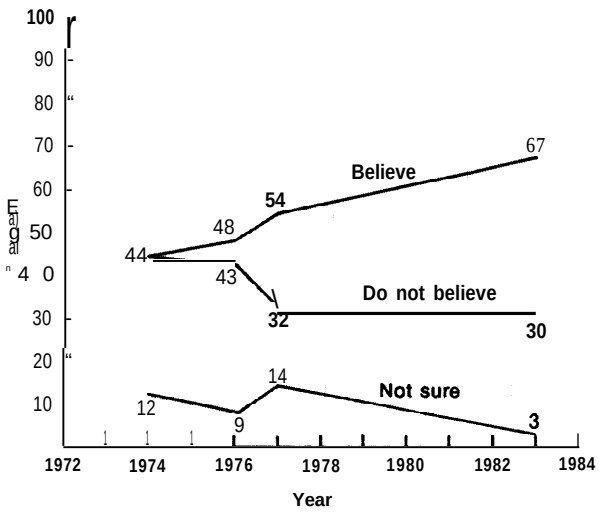
[50] Harris, op. cit., 1979, table 9.2.
[51] Harris, op. cit., 1983, table 3-3.

being mentioned most often as asking for too much personal information. About one-third of the public believe that government agencies should be doing more to maintain the confidentiality of personal information.[52] Most Americans believe that personal information about them is being kept in "some files somewhere for purposes not known" to them. As figure 2 indicates, the percentage of the public believing this to be the case has increased over time, with a high of 67 percent in 1983.

Most Americans, from two-thirds to three-fourths, believe that agencies that release the information they gather to other agencies or individuals are seriously invading personal privacy[53] (see table 4). But, as figure 3 indicates, significant percentages of the public believe that public and private organizations do share information about individuals with others.

[52]*Harris, op. cit., 1979, tables 2.2, 2.5, 2.6, 2.8, 2.9, 8.1.
[53]Harris, op. cit., 1983, table 1-6.

Figure 2.—Change in Percent of Public Believing That Files"Are Kept on Themselves[a]



[a]Response to "'Do you believe that personal (n formation about yourself is being kept In some files somewhere for purposes not known to you, or don't you believe this IS so?''

SOURCE' Louis Harris & Associates, Inc., *The Road After 1984: A Nationwide Survey of the Public and Its Leaders on the New Technology and Its Consequences for American Life* (conducted for the Southern New England Telephone for presentation at the Eighth International Smithsonian Symposium, December 1983).

The American public does not look favorably upon central files and databanks. Most Americans, 84 percent, believe that master files containing personal information, such as credit and employment histories, organizational affiliations, medical history, voting record, phone calls, buying habits, and travel, could be compiled "fairly easily. " Only 1 percent of the Harris respondents expressed uncertainty over this possibility. Seventy-eight percent believed that if such a master file were put together, it would violate their privacy .54

There is increasing support for additional government action to protect privacy. In 1978, the public was not sure who should be responsible for maintaining privacy. Nearly one-half (49 percent) said it should rest with the people themselves, while 30 percent said the courts, 26 percent Congress, 25 percent the States, 14 percent the President, and 12 percent said employers." Despite confusion over the source of responsibility, two-thirds of the public responded that laws could go a long way to help preserve our privacy.[55] Sixty-two percent "The public thought it was very important that there bean independent agency to handle complaints about violations of personal privacy by organizations .57 However, 46 percent were opposed to the creation of a National Privacy Protection Agency to protect privacy .68

In surveys conducted by the Roper Center in 1982,[59] large majorities believed that laws were needed to govern how information on individuals can be used by organizations that have computer files, and supported the major principles of the "Code of Fair Information Practices. " In 1982, 85 percent wanted laws to ensure that corrections of information were included in files, 82 percent said that individ-

[54]Ibid., table 1-2.
[55]Harris, op. cit.,1979, table 10.11.
[56]Ibid., table 10.3.
[57]Ibid., table 10.5.
[58]Ibid., table 10.4.
[59]The Roper Center, Institute of Social Research, University of Michigan, contains surveys by the major private polling organizations, including Gallup, Harris, Yankelovich, CBS/New York Times, and Roper. OTA commissioned a keyword search at the Roper Center to locate all previous public opinion research studies on any aspect of attitudes toward government information technology.

Table 4.—Seriousness of Breaches of Confidentiality

Q.: I'm going to read a few things which might be considered an invasion of privacy, all of which deal with computerized information. Do you feel that (READ EACH ITEM) would be a serious invasion of privacy, or not?

		Leaders			
	Total public	Congressmen and top aides	Corporate executives	Media: science editors	Superintendents of schools
Base	**1,256**	**'100**	100	100	100
The Internal Revenue Service not keeping individual Federal tax returns confidential:					
Serious	840/o	980/o	930/0	95 0/0	890/'0
Not serious	15	2	7	5	11
The FBI not keeping information about individuals confidential:					
Serious	82	95	93	91	86
Not serious	15	4	6	8	14
Banks sharing information about an individual's banking habits and size of bank accounts:					
Serious	78	66	60	66	78
Not serious	20	30	38	33	22
A credit business selling information about an individual credit standing:					
Serious	77	64	46	73	75
Not serious	22	34	54	25	25
The Census Bureau not keeping information about individuals confidential:					
Serious	73	88	73	82	75
Not serious	25	11	27	18	25
Insurance companies sharing information gathered about an individual:					
Serious	72	64	63	66	72
Not serious	26	31	35	32	28

SOURCE Lou Is Harris & Associates, Inc , The *Road After* 1984 *A Nationwide Survey of the Public and its Leaders* on the New Technology *and its Consequences for American Life* (conducted for the Southern New England Telephone for presentation at the Eighth International Smith son Ian Symposium. December 1983)

uals should be notified of the existence and contents of files containing information about them, 82 percent thought there should be laws to permit people to get copies of any information in files on themselves, and 71 percent thought there should be laws prohibiting most private parties from asking for social security numbers.'" In addition, 72 percent said businesses should have the right to get information only from the person directly, while only 14 percent said databanks were appropriate."

In the 1983 Harris survey (see table 5), strong majorities of the public and majorities of all four leadership groups 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. The authors of the Harris analysis observed that:

> Particularly striking is the pervasiveness of support for tough new ground rules governing computers and other information technology. Americans are not willing to endure abuse or misuse of information, and they overwhelmingly support action to do something about it. This support permeates all subgroups in society and represents a mandate for initiatives in public policy.[G2]

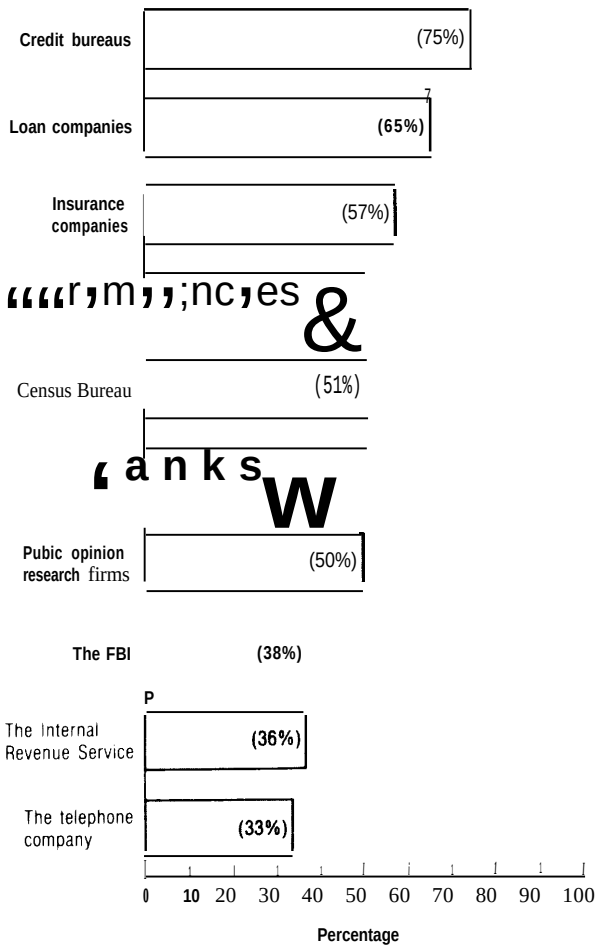
Finding 4

The Courts have not developed clear and consistent constitutional principles of information privacy, but have recognized some legitimate

"'Roper 82.6, June 5-12, 1982.
"Roper 82.8, August 14-21, 1982.

[G2] Harris, op. cit., 1983, P. 41"

Figure 3.— Percent of Public That Believes Each Agency "Shares" Information About Individuals With Others[a]



[a]Response to "Now I'd like to read you a list of organizations which might have a lot of information about individuals. For each, tell me if you think they do have a lot of information but treat it as strictly confidential, have information and probably share it with others, or don't really have information that people ought to be concerned about whether they share it or not. "

SOURCE Louis Harris & Associates, Inc , The *Road After 1984: A Nationwide Survey of the Public and Its Leaders on the New Technology and Its Consequences for American L{fe* (conducted for the Southern New Eng. land Telephone for presentation at the Eighth International Smithso. nian Symposium, December 1983).

expectations of privacy in personal communications.

Although a "right to privacy" is not mentioned in the Bill of Rights, the Supreme Court has protected various privacy interests. The Court has found sources for a right of privacy in the first, third, fourth, fifth, and ninth amendments. Since the late 1950s, the Supreme Court has upheld a series of privacy interests under the first amendment and due process clause, for example, "associational privacy, "[63] "political privacy, "[64] and the "right to anonymity in public expression. "[65] The fourth amendment protection against "unreasonable searches and seizures" also has a privacy component. In Katz v. *United States,* the Court recognized the privacy interests that protected an individual against electronic surveillance. But the Court cautioned that:

> the Fourth Amendment cannot be translated into a general constitutional "right to privacy. " That Amendment protects individual privacy against certain kinds of governmental intrusion, but its protections go further and often have nothing to do with privacy at all. Other provisions of the constitution protect personal privacy from other forms of governmental invasion.[66]

The fifth amendment protection against self-incrimination involves a right to privacy against unreasonable surveillance or compulsory disclosure.[67]

Until *Griswold v. Connecticut,* 381 U.S. 479 (1965), any protection of privacy was simply viewed as essential to the protection of other more well-established rights. In *Griswold,* the Court struck down a Connecticut statute that prohibited the prescription or use of contraceptives as an infringement on marital privacy. Justice Douglas, in writing the majority opinion, viewed the case as concerning "a relationship lying within the zone of privacy created by several fundamental constitutional guarantees," i.e., the first, third, fourth, fifth and ninth amendments, each of which creates "zones" or 'penumbras' of privacy. The majority supported the notion of an independent right of privacy inhering in the marriage relationship. Not all agreed with Justice Douglas as to its source; Justices Goldberg, Warren, and Brennan preferred to lodge the right under the ninth amendment.

---

[63] *NAACP v. Alabama, 357* U.S. 449 (1958).

[64] *Watkins v. United States,* 354 U.S. 178 (1957), and *Sweezy* v. New *Hampshire, 354* U.S. 234 (1957).

[65] *Talley* v. *Cab-form-a,* 362 U.S. 60 (1960).

[66] *Katz v. United States,* 389 U.S. 347, 350 (1967).

[67] See *Escobedo* v. *Illinois,* 378 U.S. 478 (1964), *Miranda v. Arizona, 384* U.S. 436 (1966); and *Schmerber v. California, 384* U.S. 757 (1966).

Table 5.—Support for Potential Federal Laws on Information Abuse[a]

	Total public	Leaders: Congressmen and top aides	Leaders: Corporate executives	Leaders: Media: science editors	Leaders: Superintendents of schools
Base	1,256	100	100	100	100
A Federal law 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:					
Favor	92%	85%	72 0/0	94 "/0	94 "10
Oppose	7	12	26	5	5
Federal laws that would make it a criminal offense if the privacy of an individual were violated by an information-collecting business or organization:					
Favor	83	80	79	94	88
Oppose	14	10	17	5	12
A Federal law that would call for the impeachment of any public official who used confidential information to violate the privacy or take away the freedom of an individual or a group of individuals without a proper court order or a court trial:					
Favor	81	69	89	85	91
Oppose	17	26	10	15	8
Federal laws that would require punishment for those in authority responsible for computer mistakes, such as mistakes that hurt people's credit ratings, harm companies, or endanger lives:					
Favor	71	53	37	69	61
Oppose	25	41	61	25	37
Federal laws that could put companies out of business which collected information about individuals and then shared that information in a way that violated the privacy of the individual:					
Favor	68	65	78	78	77
Oppose	30	27	20	20	21
Federal regulations on just what kind of information about an individual could be combined with other information about the same individual:					
Favor	66	77	65	81	87
Oppose	28	18	31	16	13

[a]Response to Would you favor or oppose (READ EACH ITEM)?

SOURCE Lou Is Harris & Associates, Inc , *The Road After 1984 A Nationwide Survey of the Public and* Its *Leaders on the New Technology and its* ***Consequences for*** American Life (conducted for the Southern New England Telephone for presentation at the Eighth International Smithsonian Symposium December 1983)

In *Eisenstadt v. Baird, 405* U.S. *438 (1972),*[68] the Court extended the right to privacy beyond the marriage relationship to lodge in the individual:

> If the right of the individual means anything, it is the right of the *individual,* married or single, to be free from unwarranted governmental intrusion into matters so fundamentally affecting a personas the decision whether to bear or beget a child.

Roe v. Wade, 410 U.S. 113 (1973),[69] further extended the right of privacy "to encompass a woman's decision whether or not to terminate her pregnancy. " The Court argued that the right of privacy was "founded in the Fourteenth Amendment's concept of personal liberty and restrictions upon state action. The District Court had argued that the source of the right was the ninth amendment reservation of right to the people.

[68]In which the Court struck down a Massachusetts law that made it a felony to prescribe or distribute contraceptives to single persons.

[69]In which the Court struck down the Texas abortion statute.

In the earliest case that raised the issue of the legitimate uses of computerized personal information systems, the Court avoided the central question of whether the Army's maintenance of such a system for domestic surveillance purposes "chilled' the first amendment rights of those whose names were contained in the system.[70] In two cases decided in 1976, the Court did not recognize either a constitutional right to privacy that protected erroneous information in a flyer listing active shoplifters" or one that protected the individual's interests with respect to bank records.[72] In *Paul v. Davis,* the Court specified areas of personal privacy considered "fundamental":

> matters relating to marriage, procreation, contraception, family relationships, and child rearing and education.[73]

Davis' claim of constitutional protection against disclosure of his arrest on a shoplifting charge was 'far afield from this line of decisions" and "we decline to enlarge them in this manner. "7[4] In *United States v. Miller,* the Court rejected Miller's claim that he had a fourth amendment reasonable expectation of privacy in the records kept by banks "because they are merely copies of personal records that were made available to the banks for a limited purpose, " and ruled instead that "checks are not confidential communications but negotiable instruments to be used in commercial transactions. '[75]

In *Whalen v. Roe,* the Court for the first time recognized a right of information privacy, noting that the constitutionally protected "zone of privacy" involved two kinds of interests—"One is the individual interest in avoiding disclosure of personal matters, and another is the interest in independence in making certain kinds of important decisions. "7[6G] In this case, a unanimous Court upheld a New York law requiring the State to maintain computerized records of prescriptions for certain drugs, because "the New York program does not, on its face, pose a sufficiently grievous threat to either interest to establish a constitutional violation. "[77] The Court held that as long as the security of a computer is adequate and the information is only passed to appropriate officials, sensitive information may be stored and retrieved without an invasion of a person's right to privacy. In another case in 1977,[78] the Court used a test similar to the one developed in *Whalen,* i.e., balancing the extent of the privacy intrusion against the interests that the intrusion advanced, holding that:

> In sum, appellant has a legitimate expectation of privacy in his personal communications. But the constitutionality of the Act must be viewed in the context of the limited intrusion of the screening process, of appellant's status as a public figure, of this lack of any expectation of privacy in the overwhelming majority of the materials, of the important public interest in preservation of the materials, and of the virtual impossibility of segregating the small quantity of private materials without comprehensive screening.[79]

The court did reaffirm that one element of privacy is "the individual interest in avoiding disclosure of personal matters. "8°

In subsequent lower court cases involving the question of information privacy, the circuit courts have not uniformly followed *Whalen v. Roe.*[81] For example, the Seventh and Ninth Circuit Courts have used autonomy interests rather than informational privacy in-

[70] *Laird v. Tatum* 408 U.S. 1 (1972).

[71] *Paul v. Davis* 424 U.S. 693 (1976).

'*United States v. Miller* 425 U.S. 435 (1976).

[73] *Paul v. Davis,* 424 U.S. 693, 713 (1976).

[74] Id. at 713.

"*U.S. v. Miller,* 425 U.S. 435, 442 (1976). In response to this decision, Congress passed the Right to Financial Privacy Act of 1978 (Public Law 95-630) providing bank customers with some privacy regarding records held by banks and other financial institutions and providing procedures whereby Federal agencies can gain access to such procedures.

[76] *Whalen v. Roe* 429 U.S. 589, 599-600 (1977).

"Id. at 600.

[78] *Nixon v. Administrator of General Services, 433* U.S. 425, in which the Court upheld a Federal law that required the national archivists to examine written and recorded information accumulated by the President. Nixon challenged the act's constitutionality on the grounds that it violated his right of privacy.

[79] Id. at 465.

""Id. at 457.

[81] See Gary R. Clouse, "The Constitutional Right to Withhold Private Information, " *Northwestern University Law Review,* vol. 77, 1982, p. 536.

terests as the basis for their rulings .82 In *McElrath v. Califano,* the Seventh Circuit Court reiterated that the constitutional right to privacy extends only to those personal rights deemed "fundamental" or "implicit in the concept of ordered liberty, " and that "the claim of the appellants to receive welfare benefits on their own informational terms does not rise to the level of a constitutional guarantee. "[83] In *St. Michael's Convalescent Hospital v. California,* the Ninth Circuit Court ruled that:

> As in Paul v. *Davis,* their [appellants] claim is not based upon any contention that the public disclosure of the cost information will "restrict [their] freedom of action in a sphere contended to be private. " We conclude that no cognizable constitutional right of privacy is implicated here. *4

In 1980, the Third Circuit used *Whalen* to uphold the National Institute for Occupational Safety and Health's request that an employer produce certain medical records of its employees." The Court ruled that:

> The privacy interest asserted in this case falls within the first category referred to in *Whalen v. Roe,* the right not to have an individual's private affairs made public by the government. There can be no question that an employee's medical records, which may contain intimate facts of a personal nature, are well within the ambit of materials entitled to privacy protection.[86]

In a 1981 case involving the compilation and disclosure of juveniles' social histories, the Sixth Circuit explicitly addressed the question of the relationship between *Paul v. Davis* and *Whalen v. Roe,* stating that:

> We do not view the discussion of confidentiality in *Whalen v. Roe* as overruling *Paul v. Davis* and creating a constitutional right to have all government action weighed against the resulting breach of confidentiality. The Supreme Court's discussion makes reference to only two opinions—Griswold v. *Connecticut, supra* in which the court found that several of the amendments have a privacy penumbra, and *Stanley v. Georgia, supra,* a first amendment case—neither of which support the proposition that there is a general right to nondisclosure.[87]

The Sixth Circuit Court went on to state that:

> . . . absent a clear indication from the Supreme Court we will not construe isolated statements in *Whalen* and *Nixon* more broadly than their context allows to recognize a general constitutional right to have disclosure of private information measured against the need for disclosure.[88]

The Supreme Court has not yet accepted a case to clarify the meaning and breadth of *Whalen.*

Wee: McElrath v. Califano, 615 F.2d 434 (7th Cir. 1980) which upheld Federal and State regulations that require all family members to disclose their social security numbers as a condition for receiving Aid to Families With Dependent Children benefits; and *St. Michael Convalescent Hospital v. California, 643* F.2d 1369 (9th Cir. 1981) which upheld a California statute requiring that all health care providers who are reimbursed through the Medi-Cal program release their cost information to the public.

[83] *McElrath v. Califano,* 615 F.2d 434,441 (7th Cir. 1980).

[84] *St. Michael Convalescent Hospital v. California, 643* F.2d 1369, 1375 (9th Cir. 1981).

[85] *United States v. Westinghouse, 638* F.2d 570 (3d Cir. 1980).

[86] Id. at 577.

[87] *J.P. v. DeSanti,* 653 F.2d 1080, 1089 (6th Cir. 1981).

[88] Id.