

GAO

United States General Accounting Office

Briefing Report to the Chairman,  
Subcommittee on Telecommunications  
and Finance, Committee on Energy and  
Commerce, House of Representatives

August 1990

# COMPUTERS AND PRIVACY

## How the Government Obtains, Verifies, Uses, and Protects Personal Data



142109

470

RELEASED

**RESTRICTED**—Not to be released outside the  
General Accounting Office unless specifically  
approved by the Office of Congressional  
Relations.



United States  
General Accounting Office  
Washington, D.C. 20548

Information Management and  
Technology Division

B-239819

August 3, 1990

The Honorable Edward J. Markey  
Chairman, Subcommittee on  
Telecommunications and Finance  
Committee on Energy and Commerce  
House of Representatives

Dear Mr. Chairman:

Your June 23, 1989, letter requested information on how federal agencies obtain, verify, use, and protect personal data; how individuals are made aware of information collected about them; what telecommunications and network facilities agencies' systems use to transmit data; and what effect new technologies have on the sharing of personal data. On May 11, 1990, we briefed your staff on the results of our review. This report expands on the information provided at that briefing.

To respond to your request, we sent a comprehensive questionnaire to 189 federal agencies to collect data on their information management practices and use of computer technology. We received responses from 178 agencies, for a 94-percent response rate. We did not independently validate the agencies' responses; however, we reviewed and edited all questionnaires and contacted agency personnel when additional information or clarification was necessary. By providing a quantitative summary of government activities in this area, this report should facilitate discussions on how to most appropriately provide both individual privacy protection and effective government operations.

A more detailed discussion of our objectives, scope, and methodology appears in section 1. Appendix I summarizes general laws relating to privacy and computer security, appendix II shows the number of federal systems reported to contain personal information, and appendix III contains our questionnaire with agencies' responses.<sup>1</sup>

---

## Overview

Almost every federal agency collects and uses personal information in carrying out its responsibilities. The 178 agencies reported that, as of early 1989, they maintained about 2,000 predominantly computerized

---

<sup>1</sup>We have omitted specialized laws, such as the Health Care Quality Improvement Act of 1986, which contain privacy provisions applicable only to specific systems.

systems containing personal information. Almost 83 percent of these systems are covered by the Privacy Act, which governs federal agencies' handling of personal information. In recent years, advances in computers and communications technology have had a major impact on information activities by making it easier for agencies to maintain, manipulate, and share personal information on large numbers of individuals. These applications have been promoted as a means of increasing agencies' efficiency and effectiveness; however, privacy experts have raised concerns about their impact on personal privacy.

---

## Agencies Have Hundreds of Computer Systems Containing Extensive Personal Information

Agencies gave us detailed information on their 910 largest computerized systems containing personal information. These systems—which include payroll, personnel, and program systems—contain extensive data, ranging from names and social security numbers to financial and health information, on many aspects of individuals' lives. Agencies use this information for such purposes as determining initial eligibility for federal programs, investigations, and statistical studies. The Privacy Act requires agencies to publish in the Federal Register a notice about their systems of records containing personal information. However, agencies reported that they did not comply with this requirement for 292 of these systems.

Computers and advanced technologies—such as computer networking—are widespread throughout the federal government. Some 78 percent of the 910 large computerized systems are networked through telecommunications facilities, and many of these systems can be accessed by a variety of federal, state, and local agencies, as well as by private organizations. These organizations use the accessed information for such purposes as initial eligibility/certification determinations and investigations. Section 2 of this report presents information on how agencies obtain, validate, use, and protect personal information; how they make individuals aware of systems containing personal information; and what network and telecommunications facilities the systems use.

---

## New Computer Applications Have Had a Major Impact on How Agencies Use Personal Information

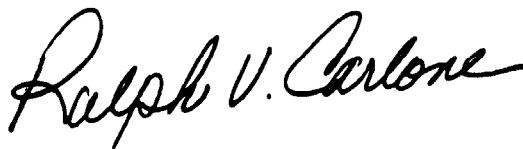
Computers and communications technologies have enabled agencies to use personal information in new applications designed to detect and prevent fraud, waste, and abuse. Such applications include computer matching, used to compare two or more automated sets of records to identify similarities or differences in data; front-end verification, used to verify personal information on government application forms; and computer profiling, used to determine types of individuals more likely to exhibit behaviors of interest to an agency. Section 3 details the extent of computer matching, front-end verification, and computer profiling within the federal government, and describes how the information resulting from these applications is used.

---

As agreed with your office, we did not obtain written comments from the agencies on a draft of this report. Unless you publicly announce the contents of this report earlier, we plan no further distribution of it until 30 days after the date of this letter. We will then send copies to the agencies, and make copies available to others upon request.

This information was compiled under the direction of Jack L. Brock, Jr., Director, Government Information and Financial Management, who can be reached at (202) 275-3195 should you require further information or have any questions about this report. Other major contributors are listed in appendix IV.

Sincerely yours,



Ralph V. Carlone  
Assistant Comptroller General

# Contents

---

Letter		1
Section 1		6
Introduction: Privacy in a Computerized Society	Objectives, Scope, and Methodology	8
Section 2		10
Government Maintains Vast Amounts of Personal Information	Agencies Use Computers to Collect and Store Personal Information	10
	Security Issues Relating to Systems Containing Personal Information	21
Section 3		24
Applications of New Information Technology Are Widespread Throughout the Government	Computer Matching Is Used Extensively for Many Purposes	24
	Agencies Use Front-End Verification to Determine Eligibility	31
	Agencies Conduct Computer Profiling to Identify Behaviors of Interest	32
Appendixes		
	Appendix I: Summary of General Legislation Relating to Privacy and Computer Security	36
	Appendix II: Number of Federal Systems Containing Personal Information, as Reported by Federal Agencies	41
	Appendix III: U.S. General Accounting Office Survey of Computers, Networks, and Privacy	44
	Appendix IV: Major Contributors to This Report	68
Tables		
	Table 2.1: Controls in Place in Agencies' 910 Largest Systems	22
	Table 3.1: Numbers and Purposes of Agencies' Computer Matching Activities	26
	Table 3.2: Federal Agencies That Participated in Computer Matching With State Agencies	29

---

---

Table 3.3: Federal Agencies That Participated in Computer Matching With Local Agencies	29
Table 3.4: Federal Agencies That Participated in Computer Matching With Private Organizations	30
Table 3.5: Organizations With Which Agencies Participated in Computer Matching Activities	30

---

**Figures**

Figure 2.1: A Federal Register Notice of an Air Force System of Records	11
Figure 2.2: Percentage of Systems Containing Data Covered by the Privacy Act About Which Information Was Published in the Federal Register	12
Figure 2.3: Agencies' Methods of Notifying Individuals	13
Figure 2.4: Sources From Which Agencies Obtain Data	14
Figure 2.5: Procedures Agencies Use to Ensure Complete and Accurate Information	15
Figure 2.6: Purposes for Which Organizations Access Systems	16
Figure 2.7: Procedures Used to Verify Third-Party Information Collected Electronically	17
Figure 2.8: Organizations That Have Access to Systems	18
Figure 2.9: Number of Systems Accessed for Unknown Purposes	19
Figure 2.10: Types of Networks Through Which Systems Are Accessed	20
Figure 3.1: Percentage of Agencies That Used Their Employees as Computer Matching Subjects	27
Figure 3.2: Types of Information Developed by Agencies That Conduct Computer Profiling	33
Figure 3.3: Agencies' Use of Computer Profiles	34

---

**Abbreviations**

FOIA	Freedom of Information Act
GAO	General Accounting Office
IMTEC	Information Management and Technology Division
OMB	Office of Management and Budget

# Introduction: Privacy in a Computerized Society

---

Many of the existing legal protections for and safeguards on the use of personal information maintained by federal agencies date back to 1974. At that time the Congress passed the Privacy Act of 1974 (P.L. 93-579), which established governmentwide standards for the protection of privacy. For some time, privacy issues had been a focus of public attention—in part as a result of congressional inquiries in the 1960s and early 1970s into wiretapping, mail openings, and burglaries by government employees, harassment of individuals for political purposes, and the questionable use of individuals' personal records.

In 1973 a committee appointed by the Secretary of Health, Education, and Welfare to study the impact of computers on record keeping recommended giving individuals more control over personal information concerning them maintained by government agencies and private organizations. The committee recommended the enactment of a federal "Code of Fair Information Practice," which would apply to both computerized and manual systems. The code, which incorporated principles designed to protect the privacy of individuals, served as the intellectual framework for the Privacy Act of 1974.

In enacting the Privacy Act, the Congress codified information principles requiring federal agencies to take certain actions:

- Collect, maintain, and use only relevant and accurate information.
- Permit individuals to gain access to information about themselves and to correct or amend such information.
- Permit individuals to determine what records concerning themselves are collected, maintained, used, and disseminated. In this regard, agencies are required to publish in the *Federal Register* a notice of the existence and nature of all systems of records containing personal information.<sup>1</sup>
- Generally permit individuals to prevent records about themselves obtained by an agency for one purpose from being used for another purpose without their consent.
- Provide adequate safeguards to ensure information security and confidentiality.

---

<sup>1</sup> A system of records is any group of records under an agency's control in which information is retrieved by an individual's name or by an identifying number, symbol, or other identifying particular assigned to an individual. How the information is retrieved (by a personal identifier) and not the substantive content determines whether the information is covered by the act.

Personal information is not covered by the act if the system in which it is contained does not meet the definition of a “system of records” or is specifically exempted.<sup>2</sup>

Additionally, the act provided for criminal penalties for officers of agencies that violate it, and civil remedies for citizens when agencies do not comply with it. For example, individuals can seek judicial relief to force access to or correction of records that agencies maintain on them and recover damages after an unlawful disclosure or violation of their rights under the act that results in an adverse determination. The Office of Management and Budget (OMB) was assigned responsibility for overseeing agencies’ implementation of the act.

When the Privacy Act was passed, most federal record systems were manual; computers were used to store and retrieve information, rather than to manipulate and share it. However, in the ensuing years, advances in computer and communications technology have had a major impact on agencies’ information practices. These technologies have enabled agencies to share and manipulate information in ways largely unforeseen in 1974. High-speed, high-capacity computers enable agencies to search large numbers of record systems and instantaneously retrieve information. Similarly, the linkage of records through computer networks allows a vast increase in the exchange of information as well as the number of people having access to it.

These technologies have facilitated new ways to use, correlate, and manipulate information collected. For example, computer matching—a major application facilitated by computer technology—compares information from two or more automated lists or files and can involve thousands of records. Front-end verification and computer profiling are other applications facilitated by computer technology. These new applications have made it easier for agencies to access, share, and process information and to carry out their missions effectively and efficiently. However, they have also increased opportunities for inappropriate or unauthorized use of personal information and have made it more difficult to oversee agencies’ information management practices and to safeguard individuals’ rights.

---

<sup>2</sup>Seven specific Privacy Act exemptions exist, covering information such as law enforcement activities, investigatory material and statistical records.



---

## **Objectives, Scope, and Methodology**

This report was requested by the Chairman, Subcommittee on Telecommunications and Finance, House Committee on Energy and Commerce, who asked that we provide information on

- federal agencies' largest computer and network systems containing information on U.S. citizens and how agencies obtain, verify, and protect this information;
- the telecommunications facilities and networks used to transmit the personal information in these systems and how the networked information is used;
- the effect of new technologies on the sharing of information across these networks and the extent to which personal information is matched with that contained in other systems; and
- the extent to which individuals are made aware of records concerning them and the recourse they have if they find incorrect information or if there has been unauthorized disclosure of information.

To obtain this information, we developed and sent a comprehensive questionnaire to 189 federal cabinet and subcabinet-level and independent agencies. To develop our questionnaire and identify privacy concerns, we analyzed privacy and security laws, OMB's guidance on agencies' responsibilities in maintaining and sharing personal information, and earlier reports prepared by us and by the President's Council on Integrity and Efficiency, the Office of Technology Assessment, and the Privacy Protection Study Commission. In addition, we spoke with computer security and information technology experts, privacy interest groups, and scholars at the Massachusetts Institute of Technology, Harvard University, Northeastern University, and The George Washington University in Washington, D. C., and Boston, Massachusetts.

We pretested our questionnaire with officials from the Department of the Air Force, Department of Energy, Department of Education, Department of Labor, Department of Housing and Urban Development, the Food and Nutrition Service of the Department of Agriculture, the Social Security Administration of the Department of Health and Human Services, and the Selective Service System. We used pretest results to refine our questionnaire.

We used a contractor for mailing the questionnaires, designing a data base, and entering agency responses into the data base. We verified the contractor's data entry on a random-sample basis. We queried the data base and analyzed results. We did not validate questionnaire responses; however, we reviewed and edited all questionnaires and followed up

---

**Section 1**  
**Introduction: Privacy in a**  
**Computerized Society**

---

with agency officials when additional information was needed. Since the data-collection methods involve self-reporting by the respondents, we expected adverse findings to be somewhat underreported.

We received responses from 178 agencies—a 94-percent response rate. Appendix II lists the agencies that responded to our questionnaire, as well as those that did not, and shows for each agency that responded the number of systems containing personal information. Appendix III reproduces our questionnaire and agency responses to each question. In some cases, questions were preceded by a filter question, which instructed respondents to skip a number of subsequent questions if they responded to the filter question in a certain way. The reader is cautioned to account for these questions when comparing responses to specific questions with statistics cited in the report. In addition, because certain questions allowed the respondents to choose more than one alternative, the sum of the numbers of responses for each alternative may not equal the total number of respondents for that question.

---

# Government Maintains Vast Amounts of Personal Information

---

Federal agencies are making significant use of computer technology to store, process, and share personal information. Much of this information is subject to the Privacy Act of 1974. This information is maintained in about 2,000 program management, payroll, personnel, financial, and other types of systems and is used by agencies for purposes such as making payments and determining program eligibility. Although agencies collect much of the information directly from individuals, personal information is also collected—sometimes electronically—from third-party sources. Agencies use various methods to inform individuals about the information they maintain; however, individuals are not always informed about such information. Many agencies share the personal information they maintain with other federal, state, and local agencies, as well as with the private sector.

---

## Agencies Use Computers to Collect and Store Personal Information

Agencies reported that, as of January 1989, they collected and stored personal information on individuals in approximately 2,000 predominantly computerized systems. Agencies identified 910 systems as their largest computerized systems containing personal information. Data maintained in these systems include social security numbers; names and addresses; and financial, health, education, demographic (e.g., race, sex), and occupational/regulatory information. Data in about 91 percent of these systems are covered by the Privacy Act.

---

## How Individuals Are Made Aware of Information Collected About Them

Under the Privacy Act, agencies are required to publish information about their systems of records in the Federal Register. The purpose of this is to prevent agencies from maintaining secret files on individuals by giving the public notice of agency record-keeping practices. However, concerns have been raised that the Federal Register is not the best means of notification since it is not easily accessible to most people. Information published in the Federal Register is to include a description of the categories of records maintained, types of sources for the information, and purposes of the records. An example of a Federal Register entry is illustrated in figure 2.1.

Section 2  
Government Maintains Vast Amounts of  
Personal Information

Figure 2.1: A Federal Register Notice of an Air Force System of Records

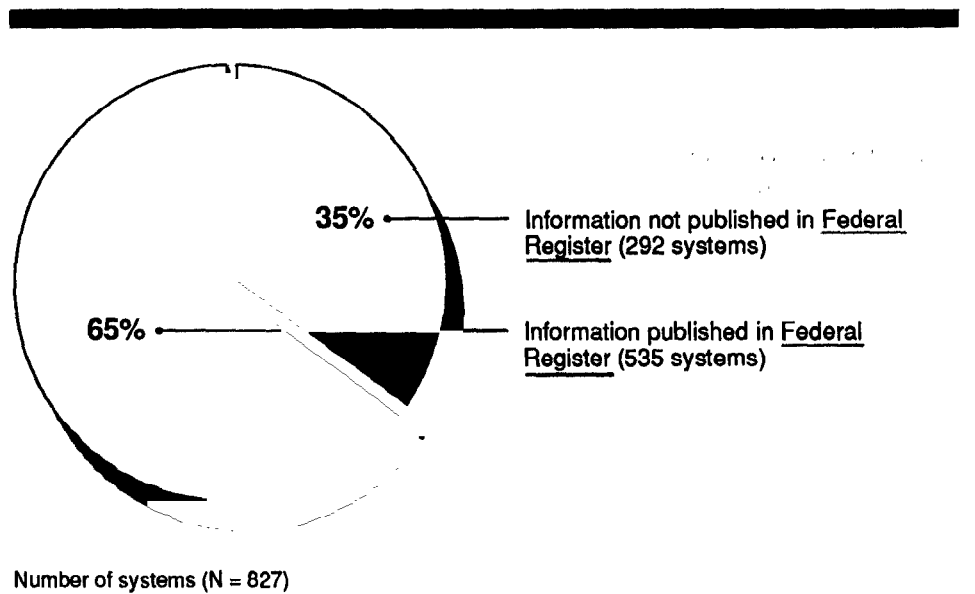
<b>F010 AF A</b>	
<b>System name:</b> 010 AF A Automated Orders Data System.	<b>Safeguards:</b> Records are accessed by person(s) responsible for servicing the records in performance of their official duties who are properly screened for need-to-know. Records are protected by computer system software.
<b>System location:</b> Any location where temporary duty travel orders are published at all levels down to and including Air Force squadrons. Official mailing addresses are in the Department of Defense directory in the appendix to the Air Force's systems notices.	<b>Retention and disposal:</b> Orders are maintained for one year after the year in which they are published. Identification data is maintained until the individual is reassigned.
<b>Categories of individuals covered by the system:</b> All Air Force civilian employees and military members who perform temporary duty travel.	<b>System manager(s) and address:</b> Director of Administration, Headquarters United States Air Force Washington, DC. Local System Manager, base director or chief of administration.
<b>Categories of records in the system:</b> All temporary duty travel orders published by the organization maintaining the system also contains identification data on individuals who perform travel.	<b>Notification procedure:</b> Requests from individuals should be addressed to the local system manager.
<b>Authority for maintenance of the system:</b> 10 USC 8012, Secretary of the Air Force: Powers and duties; delegation by.	<b>Record access procedures:</b> Individuals can obtain assistance in gaining access from the Local System Manager.
<b>Purpose(s):</b> Used to prepare temporary duty travel orders and to determine status of individual orders.	<b>Contesting record procedures:</b> The Air Force's rules for access to records and for contesting and appealing initial determinations by the individual concerned may be obtained from the System Manager and are published in Air Force Regulation 12-35.
<b>Routine uses of records maintained in the system, including categories of users and the purposes of such uses:</b> Records from this system of records may be disclosed for any of the blanket routine uses published by the Air Force.	<b>Record source categories:</b> Information is obtained from personnel records and travel order requests prepared by clerical staff serving the individual traveler.
<b>Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:</b>	<b>Exemptions claimed for the system:</b> None.
<b>Storage:</b> Maintained on computer.	
<b>Retrievability:</b> Filed by name, Social Security Number, or Air Force Service Number.	

Source Federal Register, Privacy Act Issuances, 1987 Compilation, Vol. III, pp. 204-205

**Section 2  
Government Maintains Vast Amounts of  
Personal Information**

Agencies reported that they use the Federal Register to publish information about most of their Privacy Act record systems. Although 827 (91 percent) of agencies' 910 largest systems were reported to contain information covered by the act, information on only 535 (65 percent) was published in the Federal Register. (See fig. 2.2.)

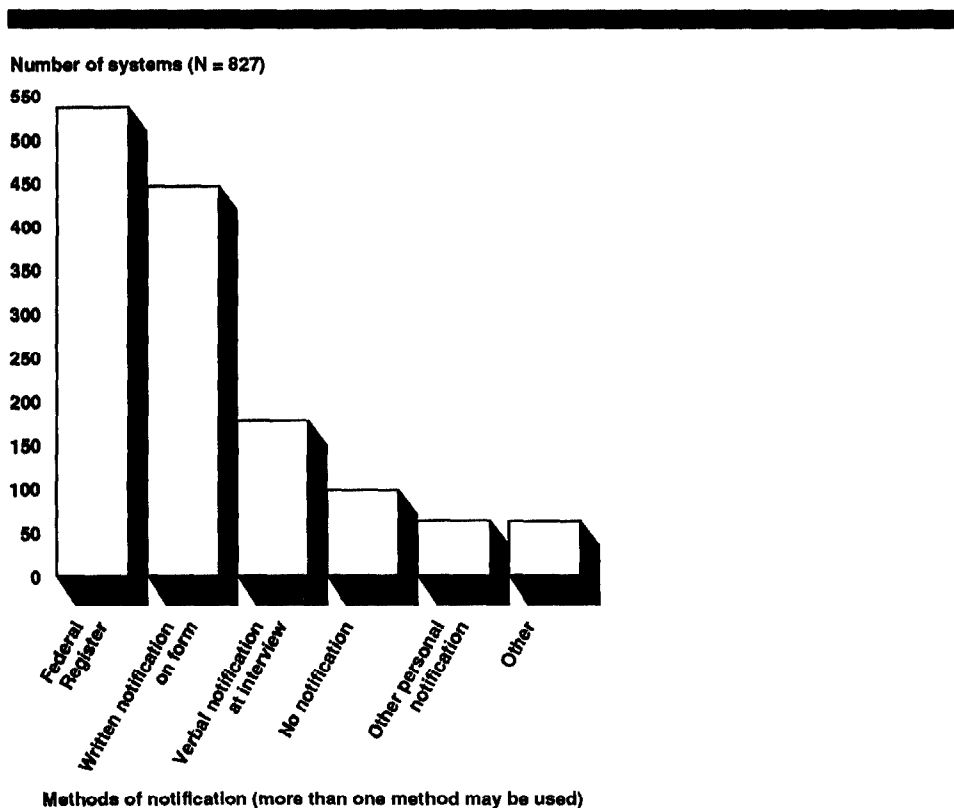
**Figure 2.2: Percentage of Systems Containing Data Covered by the Privacy Act About Which Information Was Published in the Federal Register**



**Section 2  
Government Maintains Vast Amounts of  
Personal Information**

Written notification on the form (e.g., benefits application) was the second most used notification method (used for 445, or 54 percent, of the systems). Other notification methods used included (1) verbal notification at the time the information is collected (176, or 21 percent) and (2) other methods, such as leave and earnings statements (63, or 8 percent). There were 97 systems covered by the Privacy Act for which no notification was provided. (See fig. 2.3.) These questionnaire results indicate that agencies do not always comply with the Privacy Act's notification provisions.

**Figure 2.3: Agencies' Methods of Notifying Individuals**

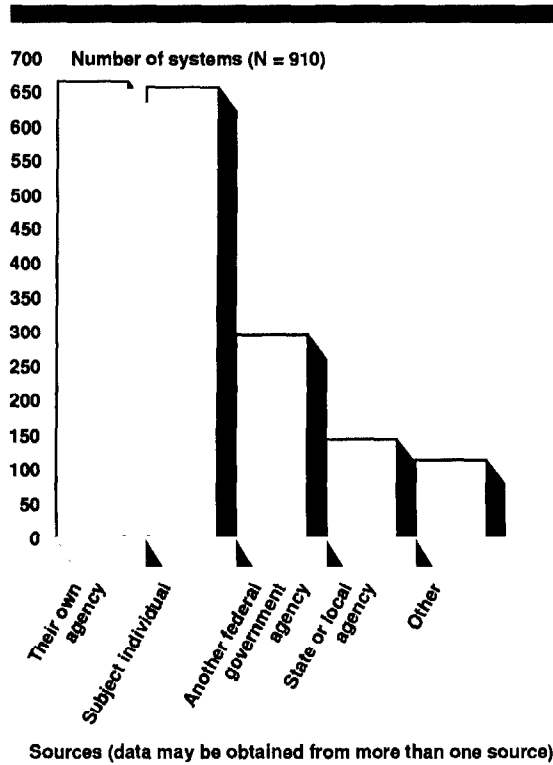


Section 2  
Government Maintains Vast Amounts of  
Personal Information

How Agencies Collect,  
Validate, and Use Personal  
Information

Agencies reported that they obtained personal information from various sources, sometimes more than one. Sources include federal, state, and local agencies, and the subject individuals themselves. Agencies reported that for over 70 percent of their largest 910 systems, personal information was obtained from the individuals themselves and/or within their own agency. (See fig. 2.4.)

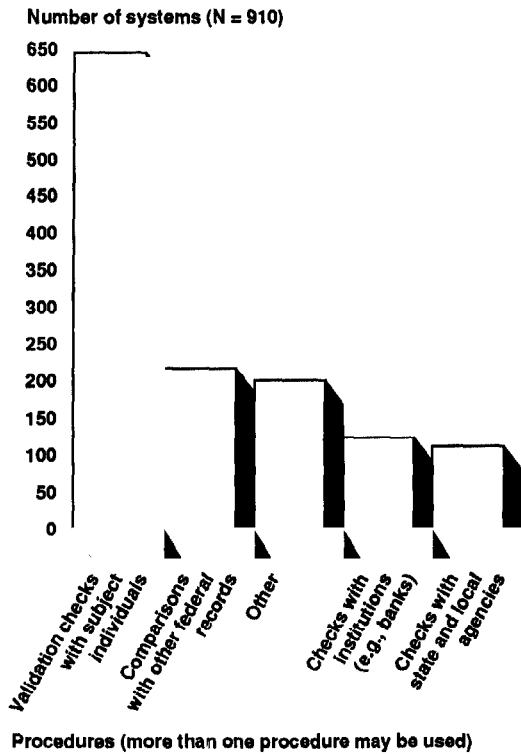
Figure 2.4: Sources From Which  
Agencies Obtain Data



Section 2  
Government Maintains Vast Amounts of  
Personal Information

Agencies reported that the information maintained in 71 percent of their 910 largest systems was validated by checking with the individual. This practice allows individuals to correct inaccurate information, as well as to control information about themselves. Additional methods of validation included (1) comparison with other federal agencies' records, (2) checking with institutions, such as banks and schools, and (3) checking with state and local agencies. (See fig. 2.5.)

Figure 2.5: Procedures Agencies Use to Ensure Complete and Accurate Information

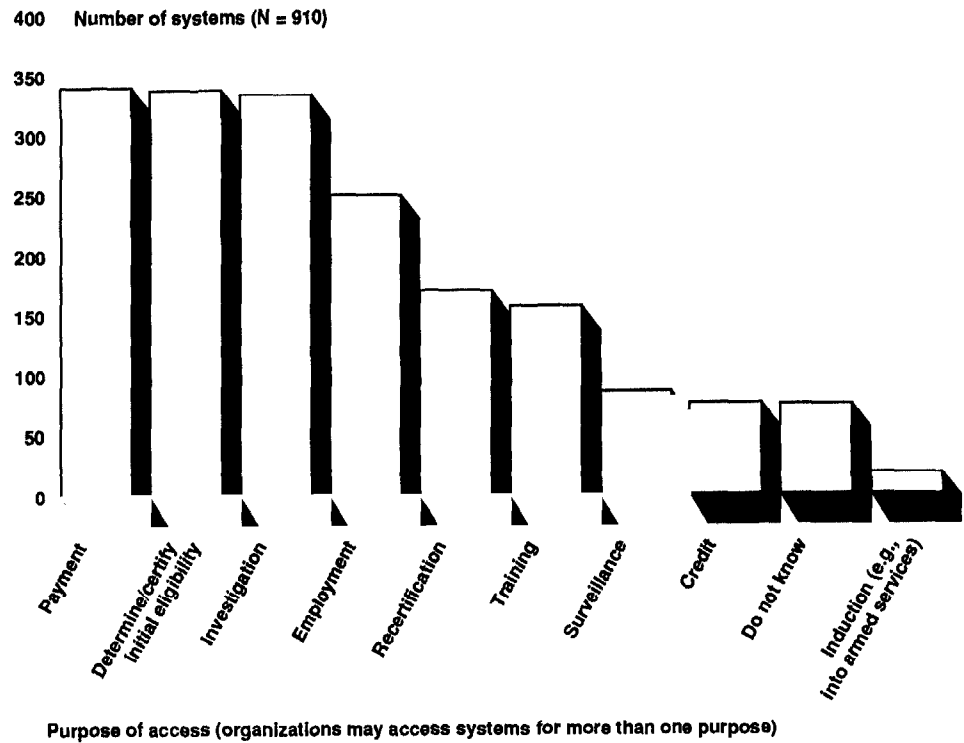




Section 2  
Government Maintains Vast Amounts of  
Personal Information

Federal agencies and other organizations use the information they obtain primarily for (1) payment (340, or 37 percent, of the systems), (2) initial eligibility/certification determinations (338, or 37 percent), and (3) investigations (334, or 37 percent). (See fig. 2.6.)

Figure 2.6: Purposes for Which Organizations Access Systems



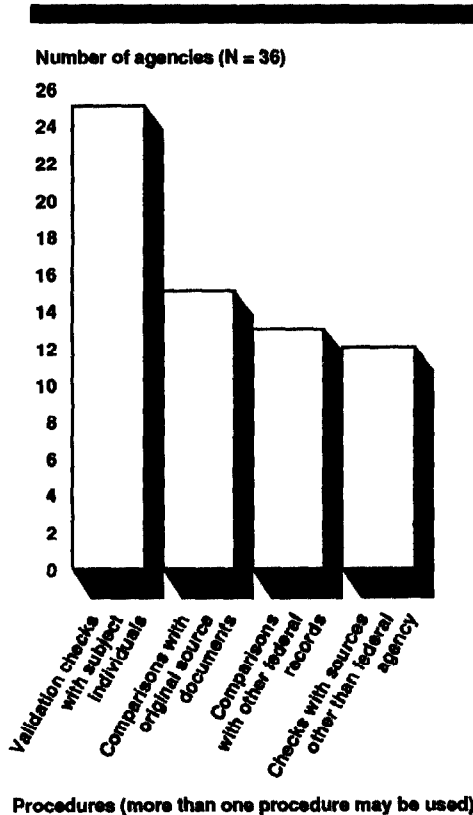
**Section 2  
Government Maintains Vast Amounts of  
Personal Information**

**Agencies Collect Third-Party Information Electronically**

Agencies also obtain and verify information from third-party sources. Of the 178 agencies responding to our questionnaire, 36 (20 percent) reported that they collected personal information electronically from third-party sources, such as state divisions of motor vehicles, credit bureaus, and insurance companies. Agencies use third-party information for debt collection (e.g., repayment of education loans), enforcement, and prescreening (e.g., to determine whether an individual meets specified qualifications).

Agencies use various methods, sometimes more than one, to ensure the accuracy of third-party information. Of the 36 agencies, 25 validate information with subject individuals and 15 compare information with original source documents. Other means used to ensure the accuracy of third-party information included (1) comparing information with other federal agencies' records (13 agencies) and (2) validating information with sources other than federal agencies (12 agencies). (See fig. 2.7.)

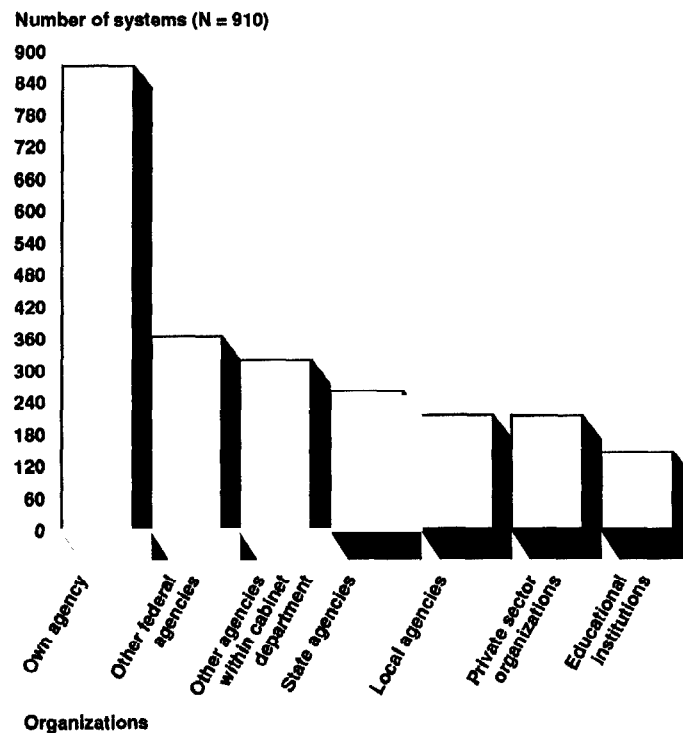
**Figure 2.7: Procedures Used to Verify Third-Party Information Collected Electronically**



**Many Systems Are  
 Accessed by a Variety of  
 Organizations**

Information in 509 (56 percent) of the agencies' 910 largest systems can be accessed by a variety of organizations, such as other agency components within cabinet-level departments; other federal agencies; state and local agencies; and private organizations, such as health care providers, marketing companies, and insurance companies. (See fig. 2.8.)

**Figure 2.8: Organizations That Have  
 Access to Systems**

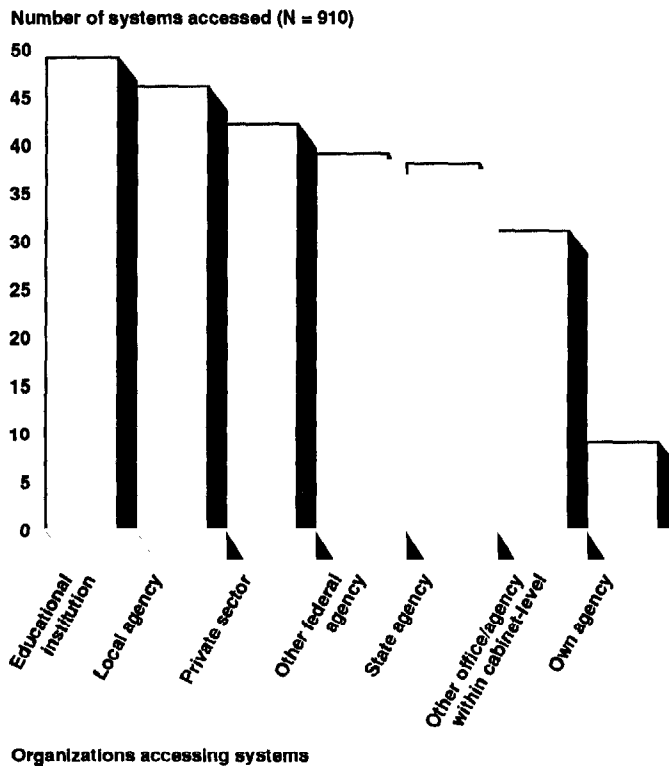


Seventy-nine systems (9 percent) can be accessed by all of these entities, as well as the agencies responsible for them. One system—the Federal Election Commission’s mail list system containing individuals’ addresses—is accessed solely by the private sector.

Section 2  
Government Maintains Vast Amounts of  
Personal Information

Some of the purposes for which these organizations use the accessed information are initial eligibility/certification determinations, payment, investigation, and employment purposes. However, for 75 (8 percent) of the 910 systems, agencies responsible for the systems reported that they did not know the purposes for which the personal information was being accessed by other organizations. For example, agency respondents reported that they did not know how accessed information was being used by (1) their own agency for 9 systems (1 percent), (2) educational institutions for 49 systems (5 percent), (3) local organizations for 46 systems (5 percent), and (4) private organizations for 42 systems (5 percent). (See fig. 2.9.)

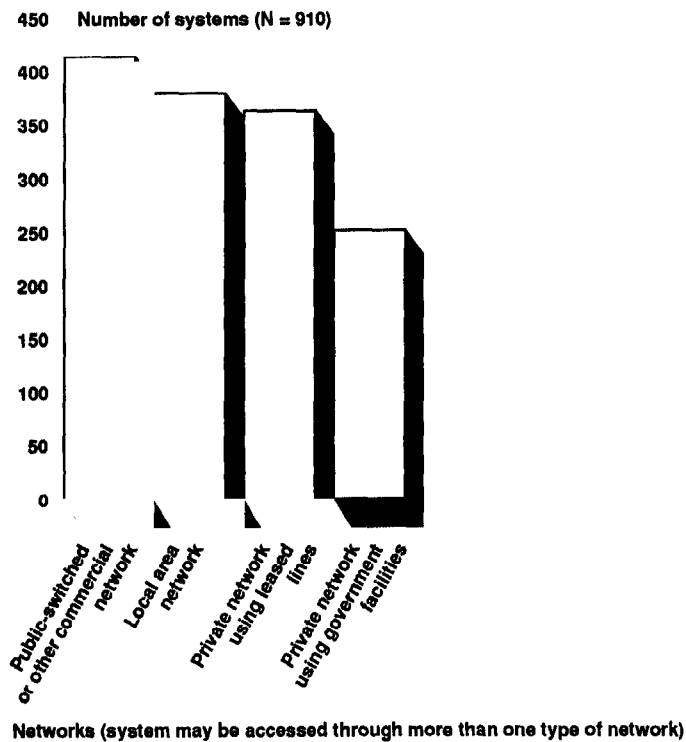
Figure 2.9: Number of Systems Accessed for Unknown Purposes



**Most Agencies' Largest  
 Systems Are Accessed  
 Through Networks**

Federal, state, local, and private organizations have access to personal information maintained in many federal agencies' computerized systems through various types of networks. Some 707 of the agencies' 910 largest systems (78 percent) are accessed through one or more communications networks. Of the 910 systems, 413 (45 percent) are accessed through a public-switched network, such as AT&T and MCI, or through a commercial network, such as Tymnet and Telenet; 379 (42 percent) are accessed through a local area network; 363 (40 percent) are accessed through a private network using private-leased lines; and 251 (28 percent) are accessed through a private network using government-owned facilities. (See fig. 2.10.)

**Figure 2.10: Types of Networks Through Which Systems Are Accessed**



---

## Security Issues Relating to Systems Containing Personal Information

Security controls are needed to protect the personal information stored and processed in computer systems from unauthorized disclosure and modification. We asked agencies to provide us with information on (1) the types of security controls they have implemented in their 910 largest systems, (2) computer security weaknesses identified under the Federal Managers' Financial Integrity Act, and (3) security breaches in their systems. This information is not intended to provide an assessment of the security of these systems, but to provide examples of the types of security controls used, security problems encountered, and agency efforts to address these problems.

---

## Computer Security Controls Agencies Use to Safeguard Their Systems

The Congress passed the Computer Security Act of 1987 in response to concerns that the federal government was not adequately addressing the security and privacy of its sensitive information. The act required, among other things, that agencies develop a security and privacy plan for each system containing sensitive information.<sup>1</sup> Guidance developed by OMB for federal agencies to follow in preparing their computer security plans segregated computer security measures into six basic control categories: management, development, operational, technical, support system security measures, and security awareness and training for employees.

Most of these categories consist of several security controls that address an underlying security objective. For instance, "assigning security responsibilities," "conducting risk assessments," and "screening personnel" are examples of specific security controls that address the broader security category of management controls. Depending on the functions and importance of a particular system, as well as acceptable levels of risks, one or more controls may be necessary within each category to provide an adequate level of security.

We asked agencies to identify the controls they have implemented for each security category outlined in OMB's guidance. Table 2.1 lists the controls within each security category that agencies reported as being in place for their 910 largest systems.

---

<sup>1</sup>The act defines sensitive information as any unclassified information that in the event of loss, misuse, or unauthorized access or modification could adversely affect the national interest, conduct of a federal program, or the privacy to which individuals are entitled under the Privacy Act of 1974.

**Section 2  
Government Maintains Vast Amounts of  
Personal Information**

**Table 2.1: Controls in Place in Agencies' 910 Largest Systems.**

<b>Security controls</b>	<b>Percentage of systems with security controls in place</b>
<b>Management controls</b>	
Assignment of security responsibility	95
Documented risk assessment	53
Undocumented risk assessment	24
Personnel screening	66
<b>Development controls</b>	
Security specifications	83
Design, review, and testing	80
Certification	46
<b>Operational controls</b>	
Production, input/output controls	90
Contingency planning	63
Audit detection	60
Software maintenance control	77
Documentation	74
<b>Security awareness and training controls</b>	
Security awareness and training measures	91
<b>Technical controls</b>	
User authentication	89
Access controls	94
Data integrity controls	77
Audit trails	65
<b>Support system security measures</b>	
Activity monitoring	78
Security measures for support systems	76

**Security Weaknesses Identified Under the Financial Integrity Act**

Under the Federal Managers' Financial Integrity Act, federal agencies are required, on an ongoing basis, to evaluate the ability of their internal control systems to protect federal programs against fraud, waste, abuse, and mismanagement. For fiscal year 1988, 13 agencies reported that they had identified material weaknesses in the security of their computerized systems containing personal information. For fiscal year 1989, 10 agencies responded that they had identified such material weaknesses. For example, the Department of the Treasury reported, for fiscal year 1988, that programmers had access to both data files and production programs for the departmental salaries and expenses system. This control weakness allowed employees access to more information than was

---

**Section 2  
Government Maintains Vast Amounts of  
Personal Information**

---

needed to perform their jobs and, as a result, increased the risk of fraudulent behavior. To correct this problem, Treasury implemented a password security system to prevent programmers from accessing data files of systems for which they also write programs.

---

**Agencies Reported 34  
Security Breaches**

Agencies reported 34 instances of security breaches in their computerized systems containing personal information in fiscal years 1988 and 1989. Two agencies reported 13 incidents of unauthorized access in fiscal year 1988; 5 agencies reported 21 incidents in fiscal year 1989. Thirty of the 34 incidents involved unauthorized access to personal information by personnel otherwise authorized to use the system. For example, in one case, an employee modified his own personal information to benefit himself financially. In two other cases, unauthorized users gained access to agencies' systems by using passwords others had disclosed to them. In another case, an agency's contractor was allowing third-party access to a system that the agency intended to be confidential.



---

# Applications of New Information Technology Are Widespread Throughout the Government

---

Computer matching, front-end verification, and profiling are applications of information technology facilitated by technological advances, such as computer networks. Computer matching, the electronic comparison of two or more sets of records, is used by federal agencies for such purposes as uncovering unreported income, erroneously reported tax information, and duplicate benefits. Some 46 agencies reported that they participated in computer matching. Front-end verification, used when an individual applies for government benefits, employment, or services to determine whether the individual is a qualified applicant, was used by 28 agencies. Computer profiling, which involves searching a record system to determine characteristics of individuals most likely to engage in behaviors of interest (e.g., tax evasion), was used by 37 agencies. These three applications have been supported by organizations such as OMB and the inspectors general as effective means of detecting fraud, waste, and abuse; however, their use has raised privacy and constitutional concerns.

---

## Computer Matching Is Used Extensively for Many Purposes

Computer matching, as discussed in OMB's June 19, 1989, final guidance interpreting the provisions of the Computer Matching and Privacy Act of 1988, is the electronic comparison of records from (1) two or more automated federal systems of records or (2) federal systems of records with nonfederal records to identify similarities or dissimilarities in the data. To facilitate computer matching, a number of data bases have been created. Often, the data bases contain information on beneficiaries under different government programs.

Organizations support computer matching as a means of improving government efficiency and strengthening program management. The President's Council on Integrity and Efficiency and OMB have attributed substantial savings and recoveries of overpayments in federal benefits programs to the use of computer matching. Savings can be realized from matching records of recipients in federal benefit programs with the files of other agencies or programs to verify the eligibility of individuals receiving benefits. For example, the Social Security Administration matches its supplemental security income benefit file with the Internal Revenue Service's tax data to identify potential overpayments and investigates and resolves identified cases. As a result of this computer matching effort, the Social Security Administration estimated savings of \$184.1 million for fiscal years 1986 through 1988.

However, privacy advocates have raised a number of concerns regarding the effect of computer matching on individuals' privacy

---

**Section 3**  
**Applications of New Information Technology**  
**Are Widespread Throughout the Government**

---

rights. Some of these concerns are that (1) computer matching makes it more difficult for individuals to control information about themselves and (2) Fourth Amendment protections against unreasonable searches and seizures may be violated because of the lack of probable cause linking a crime and an individual.

In response to these concerns, the Congress enacted the Computer Matching and Privacy Protection Act of 1988, a major amendment to the Privacy Act, that became effective July 19, 1989. The act covers matches (1) involving federal benefits programs and (2) using records from federal personnel or payroll systems of records. The legislation created an important procedural framework providing for independent verification of matching results before further action can be taken; adequate notice to individuals; the right to a hearing before benefits are reduced, suspended, or terminated; and mandatory requirements for agency reporting to the Congress and OMB. Each federal agency must establish an internal data integrity board to oversee and coordinate its matching activity. Before participating in a matching program, agencies must enter into written agreements specifying the purpose of the program and the records to be matched and, where appropriate, perform a cost-benefit analysis. In cases where individuals are wrongfully affected as a result of a match subject to the act, the Privacy Act's civil remedy provisions may be applicable.

Of the 178 agencies responding to our questionnaire, 46 (26 percent) reported that they participated in computer matching as either a matching agency (the agency performing the match) or a source agency (the agency disclosing records to the matching agency for use in a match).<sup>1</sup> In each of fiscal years 1988 and 1989, 31 respondents participated as a matching agency and 35 as a source agency. The Drug Enforcement Administration and the Farmers Home Administration accounted for about 97 percent of the matches.<sup>2</sup> Most of these computer matches were for law enforcement (78 percent) and tax (18 percent) purposes. Agencies reported the numbers and purposes of their matches as shown in table 3.1.

---

<sup>1</sup>Questionnaire respondents were asked to provide information on matching activities for fiscal years 1988 and 1989. Most of this period was before the act's effective date.

<sup>2</sup>Most of the matches reported by these two agencies involved comparing information on a single individual with various agency data bases.

**Section 3**  
**Applications of New Information Technology**  
**Are Widespread Throughout the Government**

**Table 3.1: Numbers and Purposes of Agencies' Computer Matching Activities**

<b>Purpose of match</b>	<b>Matches in which agencies participated as a</b>	
	<b>Matching agency</b>	<b>Source agency</b>
Establishing or verifying federal program eligibility	681	442
Recouping payments or delinquent debts	10,208	10,183
Law enforcement	4,320,932 <sup>a</sup>	1,148
Tax purposes	16,245	1,000,024 <sup>a</sup>
Audit purposes	72	2,044
Statutory mandate	10,037	10,004
Aggregate statistical purposes <sup>b</sup>	16,099	20,055
Research/statistical purposes <sup>c</sup>	16,073	570
Other	3,471	112,373

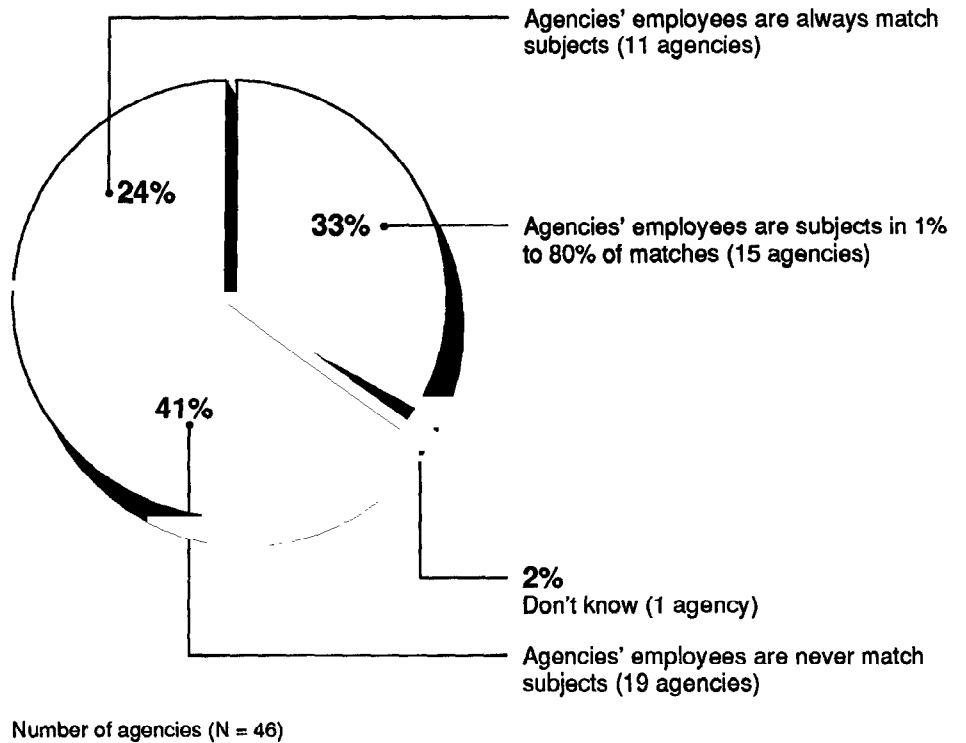
<sup>a</sup>The majority of matches in these categories involved matching information on a single individual with on-line law enforcement and tax-related data bases

<sup>b</sup>Data produced do not include information that identifies an individual.

<sup>c</sup>Data may be produced that identify an individual.

Over half (27) of the 46 agencies engaging in computer matching activities reported that they included their employees as matching subjects. Of these 27 agencies, 15 involved their employees as subjects in 1 to 80 percent of their matches, 11 involved their employees as subjects in 100 percent of their matches, and 1 did not know how many of its matches involved its employees. (See fig. 3.1.)

Figure 3.1: Percentage of Agencies That Used Their Employees as Computer Matching Subjects



### Many Matches Are Not Covered by Computer Matching and Privacy Protection Act

Many matches conducted by the federal government are exempt from the Computer Matching and Privacy Protection Act. Types of matching activities specifically exempted include matches that (1) produce aggregate statistical data without personal identifiers; (2) support any research or statistical project in which the results may include personal identifiers, but which are not used to affect an individual's rights, benefits, or privileges; (3) are conducted for law-enforcement purposes—i.e., matches performed by agencies or components whose principal function is criminal law enforcement; (4) use federal employees' personnel or payroll records for routine administrative purposes;<sup>3</sup> (5) are conducted for background investigation and foreign counterintelligence matters; (6) involve various types of tax return information; and (7) are conducted within an agency using records only from the agency's systems of records.

<sup>3</sup> According to OMB's guidance, the percentage of records in the system relating to federal employees must be greater than any other category.

---

**Section 3**  
**Applications of New Information Technology**  
**Are Widespread Throughout the Government**

---

Our questionnaire results indicated that a significant portion of governmentwide matching activity is excluded from the act. For example, in fiscal years 1988 and 1989, 11 source agencies reported that they participated in over 1 million matches for tax purposes, while 4 matching agencies reported 16,245 matches conducted for this purpose in fiscal years 1988 and 1989. Such matches are excluded from the act's coverage. In addition, 18 agencies reported that in fiscal years 1988 and 1989, they conducted about 2 million matches using only their own records.

---

**Federal Agencies**  
**Participate in Computer**  
**Matching With Many**  
**Organizations**

During fiscal years 1988 and 1989, respondents reported that they participated in computer matching not only with other federal agencies, but also with state and local agencies and private organizations. As shown in tables 3.2, 3.3, and 3.4, 21 agencies participated in computer matching with state agencies, 9 with local agencies, and 16 with private organizations.

**Section 3  
Applications of New Information Technology  
Are Widespread Throughout the Government**

**Table 3.2: Federal Agencies That Participated in Computer Matching With State Agencies**

	<b>Sent information to a state agency</b>	<b>Received information from a state agency</b>
Bureau of Labor Statistics		X
Centers for Disease Control	X	
Defense Logistics Agency	X	X
Department of Housing and Urban Development		X
Department of Veterans Affairs		X
Drug Enforcement Administration	X	
Employment and Standards Administration	X	
Environmental Protection Agency	X	
Federal Crop Insurance Corporation	X	X
Food and Nutrition Service	X	X
Health Care Financing Administration	X	
Immigration and Naturalization Service	X	X
Indian Health Service		X
Internal Revenue Service	X	X
National Highway Traffic Safety Administration	X	
Office of Information Resources Management, Department of Education	X	X
Office of Personnel Management	X	
Railroad Retirement Board	X	X
Selective Service System	X	X
Social Security Administration	X	X
Tennessee Valley Authority		X

**Table 3.3: Federal Agencies That Participated in Computer Matching With Local Agencies**

	<b>Sent information to a local agency</b>	<b>Received information from a local agency</b>
Department of Housing and Urban Development	X	X
Drug Enforcement Administration	X	
Environmental Protection Agency	X	
Immigration and Naturalization Service		X
Internal Revenue Service		X
Office of Personnel Management	X	
Selective Service System		X
Social Security Administration	X	X
Tennessee Valley Authority		X

**Section 3  
Applications of New Information Technology  
Are Widespread Throughout the Government**

**Table 3.4: Federal Agencies That Participated in Computer Matching With Private Organizations**

	Sent information to a private agency	Received information from a private agency
ACTION	X	
Centers for Disease Control	X	
Defense Logistics Agency	X	X
Department of the Army	X	
Department of Commerce	X	
Department of Labor	X	
Department of Veterans Affairs	X	
Employment and Standards Administration	X	
Farmers Home Administration	X	X
Internal Revenue Service		X
Office of Information Resources Management, Department of Education	X	X
Office of Personnel Management		X
Railroad Retirement Board		X
Social Security Administration	X	
U. S. Coast Guard	X	
U. S. Customs Service	X	

Private organizations that received information from and provide information to federal agencies include credit bureaus, banks, schools and universities, unions, insurance companies, real estate brokers, employers, health care providers and insurers, and railroads. While only 5 federal agencies reported that they received information from private organizations, 14 sent information to such organizations. (See table 3.5.)

**Table 3.5: Organizations With Which Agencies Participated in Computer Matching Activities**

Organization	Number of agencies that	
	Sent information to	Received information from
Another office/ component within agency	18	15
Another federal agency	35	33
State agency	16	14
Local agency	5	6
Private organization	14	5
Congress <sup>a</sup>	1	1

<sup>a</sup>The Department of Education participated in computer matching with the House and Senate.

---

## **Number of Individuals Affected by Computer Matches**

Individuals identified through a computer match and found ineligible to receive a specified federal benefit may have their benefits reduced, suspended, or terminated. Under the Computer Matching and Privacy Protection Act, however, agencies may take further action against individuals only after investigation and verification. Individuals must also be given advance notification and an opportunity to challenge the results before final actions are taken. Agencies reported that the number of individuals against whom further action was taken (e.g., benefits denied, reduced, or suspended) as a result of computer matching was about 3.6 million in each of fiscal years 1988 and 1989. In each of these two years, the Internal Revenue Service took further action against 3 million individuals because they had filed erroneous tax information. The Social Security Administration reported that further action had been taken against 600,000 individuals in each of the two years for various reasons, such as overpayments due to unreported increased income.

---

## **Agencies Use Front-End Verification to Determine Eligibility**

Front-end verification involves certifying the accuracy and authenticity of information supplied by an applicant by comparing it with similar information held in a computerized data base, generally obtained from a third party. For instance, an applicant's eligibility for a benefit, such as food stamps, is validated both before the applicant receives the benefit and later to determine continued eligibility. Front-end verification is similar to computer matching in that it involves an electronic search to ensure the accuracy and completeness of the personal information. Such searches through personal records have raised privacy experts' concerns about the protection of individual's privacy. However, front-end verification differs from computer matching in that it is used to

- verify information on an individual, at the time of the initial transaction, before the individual receives government benefits, employment, or services; and
- prevent, rather than detect, fraudulent activities.

Some privacy experts believe that because this procedure involves a search through a particular citizen's file rather than a general search through all files, it may constitute less of an intrusion into citizens' privacy than computer matching.

Twenty-eight agencies responded that they used front-end verification during fiscal years 1988 and 1989.



---

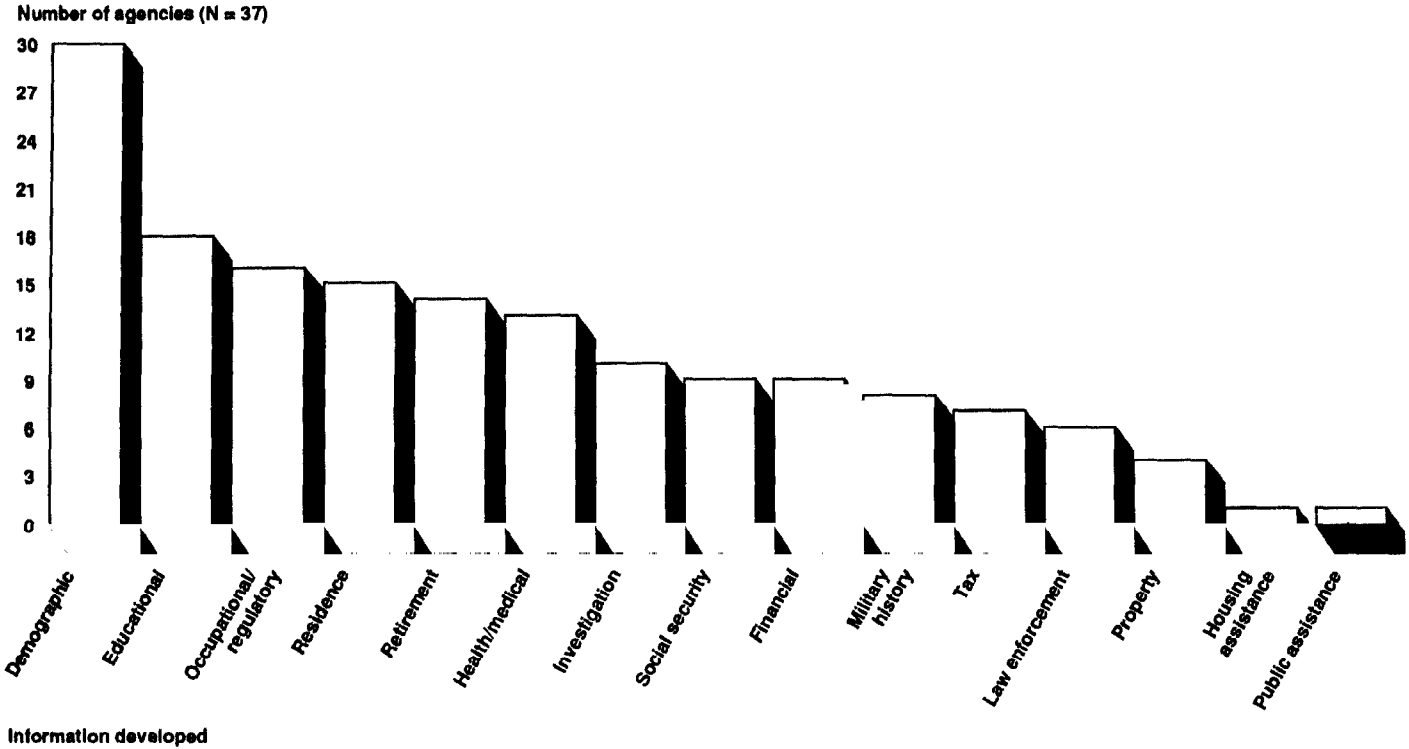
## Agencies Conduct Computer Profiling to Identify Behaviors of Interest

Computer profiling involves using inductive logic to determine the characteristics of individuals most likely to engage in behaviors of interest—for example, illegal activities. In computer profiling, a record system is electronically searched for a specified combination of data elements to construct a profile. For example, a profile may describe the characteristics of persons more likely to misrepresent information in order to receive federal aid or benefits. The profile can then be used to make judgments about individuals based on the past behavior of others who appear statistically similar. Computer profiling raises privacy and constitutional concerns because individuals may be singled out for scrutiny or different treatment before they take any action warranting such treatment. Whereas computer matching and front-end verification compare factual information, profiling compares characteristics or events that may not be indicative of the action to be prevented. Advocates of profiling, however, believe it increases agencies' efficiency and effectiveness by permitting resources to be applied more judiciously.

Thirty-seven agencies reported that they conducted computer profiling. Agencies obtain data for profiles from their own agency, other federal agencies, state and local governments, organizations, and associations. In developing profiles, agencies use social security, health, educational, financial, tax, law enforcement, property, and housing and public assistance information. (See fig. 3.2.)

Section 3  
 Applications of New Information Technology  
 Are Widespread Throughout the Government

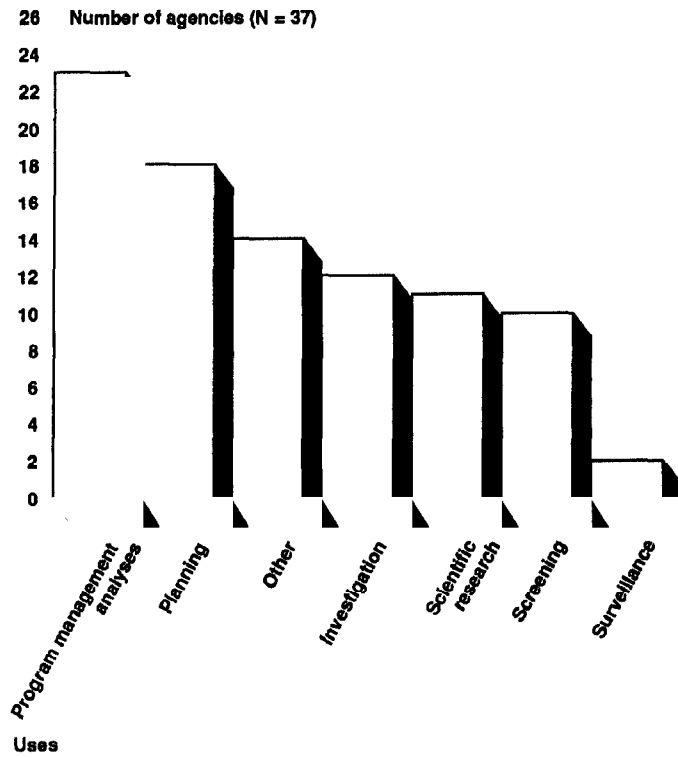
Figure 3.2: Types of Information Developed by Agencies That Conduct Computer Profiling



Agencies use profiles for many purposes, including program analyses, planning, investigation, screening, scientific research, and surveillance. (See fig. 3.3.) Two examples of agencies' computer profiling descriptions are the Social Security Administration's profiles on people most likely to have unreported changes in income, resources, and/or living arrangements; and the U.S. Secret Service's profiles of individuals most likely to commit aggressive action against a public figure.

Section 3  
Applications of New Information Technology  
Are Widespread Throughout the Government

Figure 3.3: Agencies' Use of Computer Profiles





# Summary of General Legislation Relating to Privacy and Computer Security

---

## Privacy Act of 1974, as Amended (5 U.S.C. 552a)

The Privacy Act is the primary legislation regulating the federal government's maintenance of personal information. The act establishes (1) requirements and prohibitions federal agencies must observe regarding record-keeping and disclosure practices and (2) safeguards for individuals (U. S. citizens and aliens lawfully admitted for permanent residence) against invasion of their personal privacy. Personal information is not covered by the act if the system in which it is contained does not meet the definition of a "system of records" or is specifically exempted. A system of records is any group of records under an agency's control in which information is retrieved by an individual's name or by an identifying number, symbol, or other identifying particular assigned to the individual. How the information is retrieved (by a personal identifier) and not the substantive content determines whether the information is covered by the act.

The Privacy Act, along with the Freedom of Information Act (5 U.S.C. 552), permits disclosure of most personal files to the individual who is the subject of the files. The two laws, however, restrict disclosure of personal information to others when disclosure would violate privacy interests. Agencies cannot disclose records pertaining to individuals without their consent, except under prescribed circumstances. Federal agencies must also account for disclosures made of such records.

In enacting the Privacy Act, the Congress codified information principles requiring specific actions of federal agencies:

- Publish a notice of their Privacy Act record systems in the Federal Register. (This provision was intended to prevent agencies from maintaining secret records.)
- Grant individuals access to records concerning them and an opportunity to correct inaccurate information.
- Maintain only information that is relevant and necessary to accomplish a legal purpose.
- Collect information, to the greatest extent practicable, directly from individuals when the use of the information may result in an adverse determination about individuals' rights, benefits, and privileges under federal programs.
- Maintain accurate, complete, and timely records to assure that individuals are treated fairly.
- Establish safeguards to ensure information security and confidentiality.

The Privacy Act provides civil remedies for individuals whose rights under the act have been violated, as well as criminal penalties for violation of the act. The act also contains provisions for the treatment of archival records, mailing lists, and the use of social security numbers. Government contractors are also subject to the act under certain circumstances. OMB has oversight responsibility for the Privacy Act.

---

### Freedom of Information Act, as Amended (5 U.S.C. 552)

The Freedom of Information Act (FOIA) establishes a presumption that records in the possession of Executive Branch agencies and departments are accessible to the public. FOIA sets standards for determining which records must be made available for public inspection or released to a party that requests access and which records may be withheld. The law also provides administrative and judicial remedies for those persons denied access to records. Above all, the statute requires federal agencies to provide the fullest possible disclosure of information to the public. Agencies must justify why records are not accessible to the public.

Like the Privacy Act, FOIA recognizes the legitimate need to restrict disclosure of some information. For example, agencies may withhold information classified in the interest of national defense or foreign policy, trade secrets, and criminal investigatory files. Other specifically defined categories of confidential information may also be withheld.

An essential feature of both laws is that they make federal agencies accountable for information disclosure policies and practices. While neither law grants an absolute right to examine government documents, both laws provide a right to request records and to receive a response to the request. If a requested record cannot be released, the requester is entitled to know why. The requester has a right to appeal the denial and, if necessary, challenge it in court.

---

### Computer Matching and Privacy Protection Act of 1988 (5 U.S.C. 552a Note)

The Computer Matching and Privacy Protection Act, which became effective July 19, 1989, establishes procedural safeguards affecting agencies' use of Privacy Act records in performing certain types of computerized matching programs. The act requires that agencies enter into written agreements specifying the terms under which matches are to be performed. It also provides due process rights for record subjects to prevent agencies from taking adverse actions unless they have independently verified the results of a match and given the subject 30 days' advance notice. Oversight is accomplished by having agencies publish agreements, report matching programs to the Congress and OMB, and

establish internal data integrity boards to oversee and coordinate their matching activity.

The act covers only matches having one or more of the following purposes:

- establishing or verifying initial or continuing eligibility for federal benefits programs,
- verifying compliance with the requirements (either statutory or regulatory) of such programs, or
- recouping payments or delinquent debts under such federal benefits programs.

In addition, to be covered, a match must also involve (1) the computerized comparison in an automated form; (2) individuals initially applying for benefits, individual program participants who are currently receiving or formerly received benefits, or individuals who are not the primary beneficiaries of federal benefits programs, but may derive income from them, such as health care providers; and (3) a federal benefits program. For example, if the Department of Education matched a student loan recipient data base with the Department of Veterans Affairs education benefit recipient data base for the purpose of ensuring that both agencies were maintaining current and accurate home address information, the match would not be covered since the matching purpose is not one of those listed above. If, however, the purpose of the match were to identify recipients receiving excess benefits, the match would be covered.

The Computer Matching and Privacy Protection Act brings state and local agencies within the scope of the Privacy Act when they engage in matching activities with a federal agency subject to the Privacy Act and when a federal system of records is used. The act does not cover matches between nonfederal agencies or matches involving private entities. In 1989 the Congress amended the act to extend the compliance date for agencies reporting some of their matching programs. For those programs in operation before June 1, 1989, agencies were given until January 1, 1990, to report their matching programs to the Congress and OMB.

---

**Right to Financial  
Privacy Act of 1978  
(12 U.S.C. 3401)**

The Right to Financial Privacy Act prescribes the procedures and safeguards that federal agencies must follow in obtaining access to customer financial records maintained by financial institutions. Generally, this law requires that the access be in conjunction with a legitimate law-enforcement inquiry. The act requires notification to customers about the access or subsequent transfer of their records to another agency and gives customers the right to challenge such disclosure or transfer. However, the notice and opportunity to challenge may be delayed with an appropriate judicial order. The act does not apply to customer financial records being disclosed for criminal, civil, or administrative litigation in which the government and customers are both parties. Neither does this act supercede other statutes, such as the Internal Revenue Code, in regard to accessing financial records.

---

**Electronic  
Communications  
Privacy Act of 1986  
(18 U.S.C. 2510)**

The Electronic Communications Privacy Act provides protection for electronic communications, including computer data transmissions, electronic mailboxes, cellular phones, and fiber-optic transmissions. The basic premise behind this legislation was to protect the content of private communications, regardless of how they are transmitted.

---

**Computer Security Act  
of 1987 (Public Law  
100-235)**

The Computer Security Act provides for improving the security and privacy of sensitive information in federal computer systems. The act defines sensitive information as any unclassified information which, if lost, misused, or accessed or modified without authorization, could affect the privacy to which individuals are entitled under the Privacy Act.

In general, the Computer Security Act requires that all federal agencies identify their computer systems, whether operational or under development, that contain sensitive information, establish training programs to increase security awareness and knowledge of security practices, and establish a security plan for each computer system with sensitive information. However, some federal entities are exempt from complying with the act either because they are not federal agencies as defined in the act or their computer systems are excluded from the act's application. Agencies not exempted are required to develop security plans, in accordance with the guidance issued in OMB Bulletin 88-16, showing the implementation status of 18 control measures.



---

**Federal Managers’  
Financial Integrity Act  
of 1982 (31 U.S.C.  
3512)**

The Federal Managers’ Financial Integrity Act requires ongoing evaluations of the internal control and accounting systems that protect federal programs against fraud, waste, abuse, and mismanagement. It further requires that the heads of federal agencies report annually to the President and the Congress on the condition of these systems and on their actions to correct the material weaknesses identified. For example, material weaknesses are weaknesses that could significantly impair the fulfillment of an agency mission or significantly weaken safeguards against the loss or waste of funds, property, or other assets.

# Number of Federal Systems Containing Personal Information, as Reported by Federal Agencies

	Computerized systems containing personal information		
	Total number of systems <sup>a</sup>	Systems covered by the Privacy Act <sup>a</sup>	Largest systems <sup>b</sup>
<b>Cabinet departments</b>			
Department of Agriculture	109	87	90
Department of Commerce	49	47	39
Department of Defense	363	360	102
Department of Education	20	20	10
Department of Energy	43	43	10
Department of Health and Human Services	274	210	78
Department of Housing and Urban Development	20	20	10
Department of the Interior	70	70	64
Department of Justice	201	169	53
Department of Labor	96	38	44
Department of Transportation	59	54	57
Department of the Treasury	78	70	65
Department of Veterans Affairs	35	35	10
<b>Subtotal</b>	<b>1,417</b>	<b>1,223</b>	<b>632</b>
<b>Independent agencies</b>			
ACTION	3	2	3
Administrative Conference of the United States	1	1	1
Agency for International Development	9	8	9
Appalachian Regional Commission	1	1	1
Arms Control and Disarmament Agency	0	0	0
Commission on Civil Rights	5	5	5
Commodity Futures Trading Commission	17	17	10
Consumer Product Safety Commission	2	2	2
Environmental Protection Agency	98	20	10
Equal Employment Opportunity Commission	5	5	5
Farm Credit Administration	6	6	6
Federal Communications Commission	66	66	10
Federal Deposit Insurance Corporation	17	17	10
Federal Election Commission	8	8	8
Federal Emergency Management Agency	39	25	10
Federal Energy Regulatory Commission	20	20	10
Federal Labor Relations Authority	2	2	2
Federal Maritime Commission	1	1	1
Federal Mediation and Conciliation Service	0	0	0
Board of Governors of the Federal Reserve System	40	22	10
Federal Retirement Thrift Investment Board	1	1	1
Federal Trade Commission	15	14	10

(continued)

**Appendix II  
Number of Federal Systems Containing  
Personal Information, as Reported by  
Federal Agencies**

Cabinet departments	Computerized systems containing personal information		
	Total number of systems <sup>a</sup>	Systems covered by the Privacy Act <sup>a</sup>	Largest systems <sup>b</sup>
General Services Administration:			
Federal Supply Service	0	0	0
Information Resources Management Service	0	0	0
Public Buildings Service	1	0	1
Interstate Commerce Commission	15	5	10
Merit Systems Protection Board	6	6	6
National Aeronautics and Space Administration	33	19	10
National Archives and Records Administration	2	2	2
National Credit Union Administration	3	3	3
National Labor Relations Board	7	6	7
National Mediation Board	1	0	1
National Science Foundation	15	15	10
Nuclear Regulatory Commission	29	29	10
Occupational Safety and Health Review Commission	2	2	2
Office of Management and Budget	2	2	2
Office of Personnel Management	12	11	10
Office of the Special Counsel	3	3	3
Office of Thrift Supervision	7	5	7
Overseas Private Investment Corporation	1	1	1
Peace Corps	11	11	10
Pension Benefit Guaranty Corporation	5	5	5
Railroad Retirement Board	7	7	7
Securities and Exchange Commission	16	5	10
Selective Service System	4	4	4
Small Business Administration	9	9	9
Tennessee Valley Authority	23	23	10
United States International Trade Commission	4	2	4
United States Postal Service	15	15	10
<b>Subtotal</b>	<b>589</b>	<b>433</b>	<b>278</b>
<b>Total</b>	<b>2,006</b>	<b>1,656</b>	<b>910</b>

<sup>a</sup>Includes predominantly computerized systems maintained by agencies at the end of calendar year 1988.

<sup>b</sup>Agencies identified up to 10 of their largest computerized systems containing personal information

<sup>c</sup>Formerly the Veterans Administration.

Note. One hundred twenty-seven cabinet and subcabinet-level agencies responded to our questionnaire. The Agency for International Development consolidated its responses with the United States Trade and Development Program. Cabinet, subcabinet, and independent agencies that did not respond include: the Office of Human Development Services (Department of Health and Human Services), the Bureau of International Labor Affairs (Department of Labor), the Pension and Welfare Administration (Department of Labor), the Department of State, the General Services Administration, the Federal Property Resources Service (General Services Administration), the National Transportation Safety Board, and the Office of Information Regulatory Affairs (Office of Management and Budget). We received the fol-

---

**Appendix II  
Number of Federal Systems Containing  
Personal Information, as Reported by  
Federal Agencies**

---

lowing agencies' questionnaire responses too late to be included in our analyses: the Agricultural Stabilization and Conservation Service (Department of Agriculture) and the Export-Import Bank of the United States. The Central Intelligence Agency reported that it could not respond to the questionnaire without exposing sensitive intelligence methodology.

# U.S. General Accounting Office Survey of Computers, Networks, and Privacy

## U.S. GENERAL ACCOUNTING OFFICE SURVEY OF COMPUTERS, NETWORKS, AND PRIVACY

### INTRODUCTION

The U.S. General Accounting Office has been requested by the Chairman of the Subcommittee on Telecommunications and Finance, House Committee on Energy and Commerce, to review federal computers and network systems containing personal information. In response, we are using this questionnaire to obtain information from federal agencies on computerized systems containing personal information which may or may not be subject to the Privacy Act.

### INSTRUCTIONS

To assist you in completing this questionnaire, we are providing an attachment with a list of terms and definitions. Please read the attachment before responding to the questionnaire. We occasionally ask for information where estimates may be provided. However, unless otherwise instructed, specific information is requested.

Please return the completed questionnaire in the enclosed self-addressed envelope no later than December 22, 1989, to:

Araceli Contreras  
U.S. General Accounting Office  
Room 6905, 441 G Street, N.W.  
Washington, D.C. 20548.

Please respond to the following questions as they relate to your agency as listed on the above label. As noted in the cover letter, we are asking each department component to complete a separate

questionnaire. If you have any questions, please call Mary Brewer at (202) 275-0471 or Araceli Contreras at (202) 275-3178. Thank you for your help.

Please provide the name of the one person whom we may contact to clarify information, if necessary.

Name: \_\_\_\_\_

Title: \_\_\_\_\_

Department: \_\_\_\_\_

Address: \_\_\_\_\_

Telephone No: \_\_\_\_\_

### COMPUTER AND NETWORK SYSTEMS CONTAINING PERSONAL INFORMATION (GENERAL)

1. Please estimate the number of predominantly computerized systems containing personal information maintained by your agency at the end of calendar year 1988. (ENTER NUMBER.)

2,006 Systems

2. Please estimate the number of the above (Question 1) systems which are covered by the Privacy Act. (ENTER NUMBER.)

1,656 Systems

**Appendix III  
U.S. General Accounting Office Survey of  
Computers, Networks, and Privacy**

**MANAGEMENT OF COMPUTERIZED SYSTEMS CONTAINING PERSONAL INFORMATION (SPECIFIC)**

Please provide the following information for your 10 largest (i.e., based on the number of master records and number of transactions) computerized systems containing personal information whether or not they are covered by the Privacy Act. Please provide the following information for each of these systems.

We have used the instruction '(ENTER ALL CODES THAT APPLY.)' throughout the questionnaire. For each question requiring this response, enter in the space provided, the number (code) beside the response that is most characteristic of the system. In addition, keep the systems in the same order throughout the questionnaire. When responding 'other', please specify no more than 3 items under this category.

3. Full name and other identifier of system.

	SYSTEM 1	SYSTEM 2	SYSTEM 3	SYSTEM 4	SYSTEM 5	SYSTEM 6	SYSTEM 7	SYSTEM 8	SYSTEM 9	SYSTEM 10
1) 150 2) 129 3) 113 4) 102 5) 93 6) 84 7) 71 8) 60 9) 56 10) 52										
4. Is the information in this system covered by the Privacy Act? (ENTER ONE CODE.)  1. Yes (GO TO QUESTION 6.) 2. No (GO TO QUESTION 5.)	1) 827 2) 83									
5. If the information in this system is not covered by the Privacy Act, please indicate the reasons. (ENTER CODE.)  1. Exempted 2. Not retrieved by a personal identifier 3. Other (SPECIFY.)	1) 15 2) 55 3) 13									

**Appendix III  
U.S. General Accounting Office Survey of  
Computers, Networks, and Privacy**

	SYSTEM 1	SYSTEM 2	SYSTEM 3	SYSTEM 4	SYSTEM 5	SYSTEM 6	SYSTEM 7	SYSTEM 8	SYSTEM 9	SYSTEM 10
<p>6. What agencies or parties operate the system on your behalf? <u>Operator</u> of a federal computer system is a federal agency, contractor of a federal agency, or other organization that processes information using a computer system on behalf of the federal government to accomplish a federal function. (ENTER ALL CODES THAT APPLY.)</p> <p>1. Your own agency 2. Your cabinet-level department 3. Another federal agency 4. Contractor (not state or local government) 5. Grantee (not state or local government) 6. State or local government 7. Other (SPECIFY.)</p>	<p>1) 783 2) 70 3) 80 4) 163 5) 1 6) 16 7) 2</p>									
<p>7. What types of information are collected and maintained in this system? (ENTER ALL CODES THAT APPLY.)</p> <p>1. Health/Medical 2. Investigation 3. Education 4. Housing assistance 5. Public assistance 6. Tax information 7. Social Security number 8. Retirement 9. Financial 10. Credit 11. Military history 12. Residence (address) 13. Demographic (e.g., age, sex, race, etc.) 14. Selective Service registration 15. Property (e.g., real estate, personal, etc.) 16. Occupational/regulatory (e.g., personnel pay, pilot certification, etc.) 17. Law enforcement 18. Other (SPECIFY.)</p>	<p>1) 186 2) 170 3) 220 4) 23 5) 22 6) 185 7) 638 8) 174 9) 345 10) 58 11) 156 12) 474 13) 413 14) 39 15) 76 16) 337 17) 81 18) 194</p>									

**Appendix III  
U.S. General Accounting Office Survey of  
Computers, Networks, and Privacy**

	SYSTEM 1	SYSTEM 2	SYSTEM 3	SYSTEM 4	SYSTEM 5	SYSTEM 6	SYSTEM 7	SYSTEM 8	SYSTEM 9	SYSTEM 10
<p>8. From whom does your agency obtain the data entered into this system? (ENTER ALL CODES THAT APPLY.)</p> <p>1) Your own agency 2) The subject individual 3) Another federal government agency 4) State or local agency 5) Other (SPECIFY.)</p>	<p>1) 663 2) 655 3) 294 4) 143 5) 112</p>									
<p>9. How does your agency obtain the data entered into this system? (ENTER ALL CODES THAT APPLY.)</p> <p>1) Hard copy 2) Electronic (e.g., floppy disk, tape, etc.) 3) Other (SPECIFY.)</p>	<p>1) 801 2) 481 3) 56</p>									
<p>10. How are individuals and/or groups made aware of records your agency maintains on them in this system? (ENTER ALL CODES THAT APPLY.)</p> <p>1) Federal Register 2) Written notification on form 3) Verbal notification at interview 4) Other personal notification (SPECIFY.) 5) Other (SPECIFY.) 6) Do not notify</p>	<p>1) 553 2) 470 3) 182 4) 67 5) 71 6) 131</p>									
<p>11. Which of the following procedures does your agency perform to ensure that personal information maintained in this system is complete and accurate? (ENTER ALL THAT APPLY.)</p> <p>1) Comparison with other federal agencies' records 2) Validation checks with subject individuals 3) Validation checks with state and local agencies 4) Validation checks with institutions (e.g., banks, etc.) 5) Other (SPECIFY.)</p>	<p>1) 215 2) 643 3) 110 4) 122 5) 198</p>									



**Appendix III  
U.S. General Accounting Office Survey of  
Computers, Networks, and Privacy**

	SYSTEM 1	SYSTEM 2	SYSTEM 3	SYSTEM 4	SYSTEM 5	SYSTEM 6	SYSTEM 7	SYSTEM 8	SYSTEM 9	SYSTEM 10
<p>12. What personal identifiers are used to access the records in this system? (ENTER ALL CODES THAT APPLY.)</p> <p>1. Name 2. Social Security number 3. Date of birth 4. Account number (e.g., bank, Medicare, etc.) 5. Military I.D. 6. Relative's name (e.g., parents)/responsible individual (e.g., guardian information) 7. Other (SPECIFY.)</p>	<p>1) 706 2) 577 3) 151 4) 221 5) 24 6) 31 7) 104</p>									
<p>13. Which of the following organization (see parts A-G below) have access (automated or manual) to information in this system? (ENTER ALL CODES THAT APPLY.)</p> <p>A. Your own agency: For what purpose? (ENTER ALL CODES THAT APPLY.)</p> <p>1. To determine initial eligibility/certify 2. Recertification 3. Investigation 4. Surveillance 5. Employment 6. Credit 7. Training 8. Payment 9. Induction 10. Other (SPECIFY.) 11. Do not know</p>	<p>A1) 316 A2) 151 A3) 276 A4) 66 A5) 217 A6) 51 A7) 150 A8) 323 A9) 15 A10) 274 A11) 9</p>									

**Appendix III  
U.S. General Accounting Office Survey of  
Computers, Networks, and Privacy**

	SYSTEM 1	SYSTEM 2	SYSTEM 3	SYSTEM 4	SYSTEM 5	SYSTEM 6	SYSTEM 7	SYSTEM 8	SYSTEM 9	SYSTEM 10
(QUESTION 13 CONTINUED)										
13. Which of the following organization have access (automated or manual) to information in this system? (ENTER ALL CODES THAT APPLY.)	B1) 82 B2) 46 B3) 111 B4) 18 B5) 75									
B. Other offices/agencies within cabinet-level department (e.g., IRS within the Department of the Treasury):	B6) 14 B7) 28 B8) 75 B9) 3 B10) 86 B11) 31									
For what purpose? (ENTER ALL CODES THAT APPLY.)										
1. To determine initial eligibility/certify										
2. Recertification										
3. Investigation										
4. Surveillance										
5. Employment										
6. Credit										
7. Training										
8. Payment										
9. Induction										
10. Other (SPECIFY.)										
11. Do not know										
C. Other federal agencies:	C1) 101 C2) 47 C3) 132 C4) 15 C5) 84 C6) 22 C7) 25 C8) 106 C9) 4 C10) 114 C11) 39									
For what purpose? (ENTER ALL CODES THAT APPLY.)										
1. To determine initial eligibility/certify										
2. Recertification										
3. Investigation										
4. Surveillance										
5. Employment										
6. Credit										
7. Training										
8. Payment										
9. Induction										
10. Other (SPECIFY.)										
11. Do not know										

**Appendix III  
U.S. General Accounting Office Survey of  
Computers, Networks, and Privacy**

(QUESTION 13 CONTINUED)

13. Which of the following organization have access (automated or manual) to information in this system? (ENTER ALL CODES THAT APPLY.)

D. State agencies:

For what purpose? (ENTER ALL THAT APPLY.)

1. To determine initial eligibility/certify
2. Recertification
3. Investigation
4. Surveillance
5. Employment
6. Credit
7. Training
8. Payment
9. Induction
10. Other (SPECIFY.)
11. Do not know

E. Local agencies:

For what purpose? (ENTER ALL CODES THAT APPLY.)

1. To determine initial eligibility/certify
2. Recertification
3. Investigation
4. Surveillance
5. Employment
6. Credit
7. Training
8. Payment
9. Induction
10. Other (SPECIFY.)
11. Do not know

	SYSTEM 1	SYSTEM 2	SYSTEM 3	SYSTEM 4	SYSTEM 5	SYSTEM 6	SYSTEM 7	SYSTEM 8	SYSTEM 9	SYSTEM 10
D1)	67									
D2)	22									
D3)	76									
D4)	15									
D5)	46									
D6)	14									
D7)	8									
D8)	52									
D9)	0									
D10)	68									
D11)	38									
E1)	54									
E2)	19									
E3)	57									
E4)	13									
E5)	43									
E6)	13									
E7)	7									
E8)	35									
E9)	0									
E10)	49									
E11)	46									

**Appendix III  
U.S. General Accounting Office Survey of  
Computers, Networks, and Privacy**

(QUESTION 13 CONTINUED)

13. Which of the following organization have access (automated or manual) to information in this system? (ENTER ALL CODES THAT APPLY.)

F. Educational institutions (private and public):

For what purpose? (ENTER ALL CODES THAT APPLY.)

- 1. To determine initial eligibility/certify
- 2. Recertification
- 3. Investigation
- 4. Surveillance
- 5. Employment
- 6. Credit
- 7. Training
- 8. Payment
- 9. Induction
- 10. Other (SPECIFY.)
- 11. Do not know

G. Private sector (e.g., banks, physicians, employers, credit bureaus, etc.) (SPECIFY.)

For what purpose? (ENTER ALL CODES THAT APPLY.)

- 1. To determine initial eligibility/certify
- 2. Recertification
- 3. Investigation
- 4. Surveillance
- 5. Employment
- 6. Credit
- 7. Training
- 8. Payment
- 9. Induction
- 10. Other (SPECIFY.)
- 11. Do not know

	SYSTEM 1	SYSTEM 2	SYSTEM 3	SYSTEM 4	SYSTEM 5	SYSTEM 6	SYSTEM 7	SYSTEM 8	SYSTEM 9	SYSTEM 10
F1)	21									
F2)	3									
F3)	6									
F4)	1									
F5)	22									
F6)	6									
F7)	14									
F8)	14									
F9)	0									
F10)	49									
F11)	49									
G1)	46									
G2)	12									
G3)	14									
G4)	3									
G5)	33									
G6)	33									
G7)	5									
G8)	46									
G9)	0									
G10)	69									
G11)	42									

**Appendix III  
U.S. General Accounting Office Survey of  
Computers, Networks, and Privacy**

	SYSTEM 1	SYSTEM 2	SYSTEM 3	SYSTEM 4	SYSTEM 5	SYSTEM 6	SYSTEM 7	SYSTEM 8	SYSTEM 9	SYSTEM 10
<p>14. In what form, if at all, is the information from this database released? (ENTER ALL CODES THAT APPLY.)</p> <p>1. Hard copy 2. Electronic (e.g., floppy disk, tape, etc.) 3. Other (SPECIFY.) 4. Cannot be released</p>	<p>1) 700 2) 411 3) 38 4) 164</p>									
<p>15. How does your agency accept requests for the release of information from this system? (ENTER ALL CODES THAT APPLY.)</p> <p>1. In person 2. Written request 3. Telephone 4. Electronic (e.g., floppy disk, tape, etc.) 5. Other (SPECIFY.)</p>	<p>1) 365 2) 750 3) 230 4) 110 5) 19</p>									
<p>16. Through which of the following kind of network (see parts A-E below) is this system accessed? (ENTER ALL CODES THAT APPLY.)</p> <p>A. Public-switch network (i.e., AT&amp;T, Sprint, and MCI): (ENTER CODE.)</p> <p>1. Yes 2. No</p> <p>B. Other commercial network (e.g., Tymnet, Telenet, etc.): (ENTER CODE.)</p> <p>1. Yes 2. No</p>	<p>A1) 254 A2) 637</p> <p>B1) 258 B2) 627</p>									

**Appendix III  
U.S. General Accounting Office Survey of  
Computers, Networks, and Privacy**

(QUESTION 16 CONTINUED)

16. Through which of the following kind of network is this system accessed? (ENTER ALL CODES THAT APPLY.)

**C. Local area network:**

Agencies or parties operating network (ENTER ALL CODES THAT APPLY.)

- 1. System is not accessed via local area networks (GO TO QUESTION 16D.)
- 2. Own agency
- 3. Another federal agency
- 4. Contractor (not state or local government)
- 5. Grantee (not state or local government)
- 6. State or local government
- 7. Other (SPECIFY.)

**D. Private network using leased lines:**

Agencies or parties operating network. (ENTER ALL CODES THAT APPLY.)

- 1. System is not accessed via private network using leased lines (GO TO QUESTION 16E.)
- 2. Own agency
- 3. Another federal agency
- 4. Contractor (not state or local government)
- 5. Grantee (not state or local government)
- 6. State or local government
- 7. Other (SPECIFY.)

	SYSTEM 1	SYSTEM 2	SYSTEM 3	SYSTEM 4	SYSTEM 5	SYSTEM 6	SYSTEM 7	SYSTEM 8	SYSTEM 9	SYSTEM 10
C1)	474									
C2)	361									
C3)	13									
C4)	20									
C5)	0									
C6)	1									
C7)	10									
D1)	450									
D2)	298									
D3)	37									
D4)	97									
D5)	0									
D6)	1									
D7)	12									

**Appendix III  
U.S. General Accounting Office Survey of  
Computers, Networks, and Privacy**

(QUESTION 16 CONTINUED)		SYSTEM 1	SYSTEM 2	SYSTEM 3	SYSTEM 4	SYSTEM 5	SYSTEM 6	SYSTEM 7	SYSTEM 8	SYSTEM 9	SYSTEM 10
16. Through which of the following kind of network is this system accessed? (ENTER ALL CODES THAT APPLY.)  E. Private network using government-owned facilities:  Agencies or parties operating network. (ENTER ALL CODES THAT APPLY.)  1. System is not accessed via private network using government-owned facilities (GO TO QUESTION 17.) 2. Own agency 3. Another federal agency 4. Contractor (not state or local government) 5. Grantee (not state or local government) 6. State or local government 7. Other (SPECIFY.)	E1)	578									
	E2)	198									
	E3)	32									
	E4)	49									
	E5)	0									
	E6)	1									
	E7)	6									
17. For which of the following is there authorized access via dial-up? (ENTER ALL CODES THAT APPLY.)  1. Systems programs (i.e., software used in the operating system) 2. Applications 3. Diagnostics (e.g., diagnostics to identify a system problem) 4. Routine or general maintenance 5. Other (SPECIFY.)	1)	306									
	2)	511									
	3)	274									
	4)	284									
	5)	11									

**Appendix III  
U.S. General Accounting Office Survey of  
Computers, Networks, and Privacy**

	SYSTEM 1	SYSTEM 2	SYSTEM 3	SYSTEM 4	SYSTEM 5	SYSTEM 6	SYSTEM 7	SYSTEM 8	SYSTEM 9	SYSTEM 10
<p>18. What restrictions are imposed on individuals with authorized dial-up access to the system? (ENTER ALL CODES THAT APPLY.)</p> <p>1. Ability to read personal data 2. Modify personal data 3. Add personal data 4. Delete personal data 5. Other (SPECIFY.) 6. Not applicable</p>	<p>1) 420 2) 327 3) 325 4) 316 5) 73 6) 358</p>									
<p>19. What controls are <u>in place</u> to protect the information maintained in your computerized systems against alteration and unauthorized access? (See OMB's guidance for preparing and submitting agency security plans, OMB Bulletin No. 88-16, July 6, 1988.) (ENTER ALL CODES THAT APPLY.)</p> <p>A. MANAGEMENT CONTROLS:</p> <p>1. Assignment of security responsibility 2. Documented risk assessment 3. Undocumented risk assessment 4. Personnel screening 5. None of the above management controls are in place</p> <p>B. DEVELOPMENT CONTROLS:</p> <p>1. Security specifications 2. Design, review and testing 3. Certification 4. None of the above development controls are in place</p>	<p>A1) 868 A2) 486 A3) 219 A4) 601 A5) 5</p>									
	<p>B1) 752 B2) 729 B3) 415 B4) 47</p>									



**Appendix III  
U.S. General Accounting Office Survey of  
Computers, Networks, and Privacy**

(QUESTION 19 CONTINUED)

19. What controls are in place to protect the information maintained in your computerized systems against alteration and unauthorized access? (See OMB's guidance for preparing and submitting agency security plans, OMB Bulletin No. 88-16, July 6, 1988.) (ENTER ALL CODES THAT APPLY.)

**C. OPERATIONAL CONTROLS:**

1. Production, input/output controls
2. Contingency planning
3. Audit detection
4. Software maintenance control
5. Documentation
6. None of the above operational controls are in place

**D. SECURITY AWARENESS AND TRAINING:**

1. Security awareness and training measures
2. Security awareness and training measures not in place

**E. TECHNICAL CONTROLS:**

1. User authentication
2. Access controls
3. Data integrity controls
4. Audit trails
5. None of the above technical controls are in place

**F. SUPPORT SYSTEM SECURITY MEASURES (i.e., physical or facilities security control)**

1. Activity monitoring
2. Security measures for support systems
3. None of the above support system security measures are in place

	SYSTEM 1	SYSTEM 2	SYSTEM 3	SYSTEM 4	SYSTEM 5	SYSTEM 6	SYSTEM 7	SYSTEM 8	SYSTEM 9	SYSTEM 10
C1) 820 C2) 571 C3) 542 C4) 701 C5) 669 C6) 13										
D1) 830 D2) 65										
E1) 813 E2) 858 E3) 701 E4) 595 E5) 5										
F1) 713 F2) 694 F3) 69										

**Appendix III  
U.S. General Accounting Office Survey of  
Computers, Networks, and Privacy**

20. For those controls that are not in place, please indicate which of the following, if any, are reasons they are not in place. (ENTER ALL CODES THAT APPLY.)

- 1. Budget constraints
- 2. Risk assessment indicated control were not necessary
- 3. Difficulty in hiring qualified employees
- 4. Lack of adequate guidance
- 5. Other (SPECIFY.)
- 6. Not applicable

	SYSTEM 1	SYSTEM 2	SYSTEM 3	SYSTEM 4	SYSTEM 5	SYSTEM 6	SYSTEM 7	SYSTEM 8	SYSTEM 9	SYSTEM 10
1)	147									
2)	121									
3)	30									
4)	33									
5)	45									
6)	523									

Appendix III  
U.S. General Accounting Office Survey of  
Computers, Networks, and Privacy

**COMPUTER MATCHING AND FRONT-END VERIFICATION**

Please respond to the following questions for all of your agency's systems containing personal information

21. Did your agency participate in computer matching activities with another agency as a (A) matching agency (the agency performing the match) or (B) source agency (the agency disclosing records to the matching agency for use in the match) at any time during fiscal years (FYs) 1988 and 1989? Computer matching is defined as the computerized comparison of two or more automated lists or files to identify inconsistencies or irregularities among the lists or files. (CHECK YES OR NO FOR EACH YEAR.)

YEAR	(A) AS A MATCHING AGENCY?		(B) AS A SOURCE AGENCY?	
	YES	NO	YES	NO
	(1)	(2)	(1)	(2)
FY 1988	[31]	[117]	[35]	[112]
FY 1989	[31]	[116]	[35]	[112]

(IF NO TO (A) AND (B), GO TO QUESTION 32.)

22. For each purpose listed below, please estimate to the extent available the number of intra-agency and inter-agency (including federal, state and local agencies) computer matches in which your agency participated during FY 1988 and FY 1989. We recognize that intra-agency (within your agency component) matches are not covered by the Computer Matching and Privacy Protection Act of 1988. However, if possible, please include the number for intra-agency matches in your calculations. (ENTER '0' IF NONE.)

PURPOSE	MATCH	SOURCE
1. Establishing or verifying eligibility for a federal program	681	442
2. Recouping payments or delinquent debts	10,208	10,183
3. Law enforcement purposes	4,320,932	1,148
4. Tax purposes	16,245	1,000,024

(QUESTION 22 CONTINUED)

PURPOSE	MATCH	SOURCE
5. Audit purposes	72	2,044
6. Statutory mandate	10,037	10,004
7. Aggregate statistical purposes (data produced does not include information that could be used to identify an individual)	16,099	20,055
8. Research/statistical purposes (data may be produced and retained that could be used to identify an individual)	16,073	570
9. Other (SPECIFY.)	3,471	112,373
<b>GRAND TOTAL</b>	<b>4,393,818</b>	<b>1,156,843</b>

Appendix III  
U.S. General Accounting Office Survey of  
Computers, Networks, and Privacy

23. Of the computer matches conducted by your agency in FY 1988 and FY 1989, what percent of these matches involved your agency employees as subjects? (ENTER NUMBER.)

\_\_\_\_\_ Percent (RESULTS ARE LISTED BELOW)

0% - 19 agencies

1% to 80% - 15 agencies

100% - 11 agencies

1 agency did not know the percentage

24. How many intra-agency matches did your agency conduct during FY 1988 and FY 1989 where all the information used had been collected by your agency? (ENTER NUMBER.)

(1) 575,210 Matches in FY 1988

(2) 1,185,209 Matches in FY 1989

(3) 10 agencies Do not maintain records on intra-agency matches

25. When participating in computer matches during FY 1988 and FY 1989, (1) to whom did your agency send information and (2) from what sources did your agency receive/access information? (CHECK ALL THAT APPLY.)

Organization	Your Agency Sent Information To (1)	Your Agency Received/ Accessed Information From (2)
1. Another office/ component within your agency	18	15
2. Another federal agency	35	33
3. State agency	16	14
4. Local agency	5	6
5. Private organization (Identify up to five types.) 1. _____ 2. _____ 3. _____ 4. _____ 5. _____	14	5
6. OTHER (SPECIFY)	1	1

Appendix III  
U.S. General Accounting Office Survey of  
Computers, Networks, and Privacy

26. In addition to your notice of computer matches in the Federal Register, how often, if ever, does your agency provide separate written notification to subject individuals that they are involved in a computer match? (CHECK ONE.)
1. [13] Always or almost always
  2. [ 2] Most of the time
  3. [ 1] About half the time
  4. [ 1] Sometimes
  5. [28] Never or almost never (GO TO QUESTION 28.)
27. When individuals are advised that their personal information may be used in matching programs, which of the following information is provided to the subject individual? (CHECK ALL THAT APPLY.)
1. [14] The purpose of the match
  2. [ 2] When and how often the matches will occur
  3. [ 8] What information will be matched
  4. [ 9] How the matched information will be used
  5. [ 4] Other (SPECIFY.) \_\_\_\_\_  
\_\_\_\_\_
28. Does your agency verify data produced from a 'hit'? (CHECK ONE.)
1. [31] Yes (GO TO QUESTION 29.)
  2. [14] No (GO TO QUESTION 30.)
29. What are your agency's steps and procedures for verifying data produced from a 'hit'? (CHECK ALL THAT APPLY.)
1. [21] Asking the subject individual
  2. [19] Tracing the computer output to the original document
  3. [20] Conducting independent investigation and confirmation
  4. [ 4] Other (SPECIFY.) \_\_\_\_\_  
\_\_\_\_\_
30. How many individuals have been adversely affected (e.g., denied benefits, indicted, etc.) as a result of a computer match initiated by your agency during FY 1988 and FY 1989? (ENTER NUMBER.)
- (1) 3,611,677 individuals in FY 1988
  - (2) 3,624,984 individuals in FY 1989
31. Has your agency developed an appeals process for individuals/institutions who have been adversely affected as the result of a 'hit'? (CHECK ONE.)
1. [20] Yes
  2. [23] No
32. Has your agency used computerized front-end verification during fiscal years 1988 and 1989 when individuals applied for federal programs, benefits, employment or services? Front-end verification is the certification of the accuracy and authenticity of information supplied by an applicant that is checked against similar information held in a computerized database, generally of a third party. (CHECK ONE.)
1. [ 28] Yes
  2. [117] No

Appendix III  
U.S. General Accounting Office Survey of  
Computers, Networks, and Privacy

THIRD PARTY INFORMATION AND PROFILING

33. Does your agency collect in electronic form (all electro-magnetic or optical media and on-line access) from third party sources (e.g., credit bureaus, death records, Division of Motor Vehicles) any information from which you can identify individuals? (CHECK ONE.)

1. [ 36] Yes (GO TO QUESTION 34.)
2. [113] No (GO TO QUESTION 37.)

34. From what sources does your agency collect this information? (CHECK ALL THAT APPLY.)

1. [11] Credit bureaus
2. [12] Division of Motor Vehicles
3. [ 5] Educational institutions
4. [10] Law enforcement agencies
5. [ 6] Court reviews
6. [ 2] Insurance bureaus
7. [ 5] Bureau of Vital Statistics
8. [23] Other (SPECIFY.)

35. For what purpose was this information collected? (CHECK ALL THAT APPLY.)

1. [12] Enforcement
2. [13] Debt collection
3. [10] Pre-screening
4. [ 9] Denial of benefits
5. [22] Other (SPECIFY.)

36. What are your agency's procedures for assuring the accuracy of this information? (CHECK ALL THAT APPLY.)

1. [13] Comparison with other federal agencies' records
2. [12] Validation checks with sources other than federal agencies
3. [25] Validation checks with subject individuals
4. [15] Comparison with source document
5. [ 5] Other (SPECIFY.)

37. Does your agency use computer programs to develop generic profiles of types of individuals or categories of individuals? Computer profiling is the searching through a record system for a specified combination of data elements, i.e., the profile. For example, a profile could describe the characteristics of persons more likely to misrepresent information in order to receive federal aid or benefits. (CHECK ONE.)

1. [ 37] Yes (GO TO QUESTION 38.)
2. [113] No (GO TO QUESTION 42.)

Appendix III  
U.S. General Accounting Office Survey of  
Computers, Networks, and Privacy

38. What types of information are developed in the profile (CHECK ALL THAT APPLY.)

1. [13] Health/medical
2. [10] Investigation
3. [18] Education
4. [ 1] Housing assistance
5. [ 1] Public assistance
6. [ 7] Tax information
7. [ 9] Social Security
8. [14] Retirement
9. [ 9] Financial
- 10.[ 8] Military history
- 11.[15] Residence (address)
- 12.[30] Demographic (e.g., age, sex, race, etc.)
- 13.[ 4] Property (e.g., real estate, personal, etc.)
- 14.[16] Occupational/regulatory (e.g., personnel pay, pilot certification, etc.)
- 15.[ 6] Law enforcement
- 16.[ 6] Other (SPECIFY.) \_\_\_\_\_

39. If your agency develops generic profiles, please describe below the types of profiling your agency performs (e.g., categories of taxpayers more likely to be under-reporting taxable income or types of people more likely to be engaging in illegal drug activity).

30 agencies commented.  
7 agencies did not comment.

40. What are the sources of input data for your agency's generic profiles? (CHECK ALL THAT APPLY.)

1. [35] Own agency
2. [ 8] Federal agencies
3. [ 7] State or local government
4. [ 2] Organization or association
5. [ 5] Other (SPECIFY.) \_\_\_\_\_

41. For what uses does your agency develop profiles? (CHECK ALL THAT APPLY.)

1. [23] Program management analyses
2. [11] Scientific research
3. [18] Planning
4. [ 2] Surveillance
5. [10] Screening
6. [12] Investigation
7. [14] Other (SPECIFY.) \_\_\_\_\_

Appendix III  
 U.S. General Accounting Office Survey of  
 Computers, Networks, and Privacy

**SECURITY CONTROLS**

(Questions 42 thru 50, below, refer to the systems listed in Question 3.)

42. During FY 1988 and FY 1989, did your agency identify any material weaknesses in the security of predominantly computerized systems containing personal data (i.e., systems identified in Question 3) based on its evaluations under the Federal Managers Financial Integrity Act (FMFIA) of 1982? (CHECK ONE.)

Year	IDENTIFIED MATERIAL WEAKNESS	
	Yes (1)	No (2)
1. FY 1988	13	133
2. FY 1989	10	136

43. Please provide copies of reports on security weaknesses in the systems identified in Question 3 that your agency prepared under the FMFIA as well as those prepared by the President's Council on Integrity and Efficiency (PCIE), internal agency report, and any consultant report for FY 1988 and FY 1989. [ 29 ] agencies provided reports [121] agencies did not

44. During FY 1988 and FY 1989, were there any incidents of unauthorized access or exceeding authorized access to personal information maintained in any of your agency's systems identified in Questions 3? Exceeding authorized access is to access a computer with authorization and to use such access to read, obtain, or alter personal information in the computer that the accessor is not entitled to access.

- 1. [ 6 ] Yes (GO TO QUESTION 45.)
- 2. [135] No (GO TO QUESTION 48.)
- 3. [ 8 ] Do not know (GO TO QUESTION 48.)

45. To your knowledge, how many separate incidents were detected in FY 1988 and FY 1989 in these systems? (ENTER NUMBER.)

\_\_\_\_\_ 13 \_\_\_\_\_ Incidents detected in  
 FY 1988

\_\_\_\_\_ 21 \_\_\_\_\_ Incidents detected in  
 FY 1989

46. How were you made aware of these incidents? (CHECK ALL THAT APPLY.)

- 1. [ 3 ] Audit reports generated by the system
- 2. [ 4 ] Word of mouth  
 [ 4 ] confirmed  
 [ 1 ] unconfirmed
- 3. [ 2 ] Destruction of computer file system
- 4. [ 1 ] Denial of services
- 5. [ 1 ] Other (SPECIFY.) \_\_\_\_\_

47. Please describe below some examples of the incident that have occurred in these systems since October 1987.

5 agencies commented.  
 1 agency did not comment.



Appendix III  
 U.S. General Accounting Office Survey of  
 Computers, Networks, and Privacy

48. Please consider the systems that you identified in QUESTION 3. Listed below are problems that an agency might have with maintaining its computerized systems containing personal information. Based on your experience, for each problem listed below, please enter the number of systems having these problems, if any, in the appropriate categories. (ENTER NUMBER IN APPROPRIATE CATEGORIES.)

NOTE: THE TOTAL NUMBER OF SYSTEMS INDICATED FOR EACH PROBLEM SHOULD EQUAL THE NUMBER OF SYSTEMS IDENTIFIED IN QUESTION 3.

PROBLEMS WITH MAINTAINING SYSTEMS IDENTIFIED IN QUESTION 3	Not A Problem (1)	Little Extent (2)	Some Extent (3)	Moderate Extent (4)	Great Extent (5)	Very Great Extent (6)
1. Volume of data	713	48	75	39	27	8
2. Volume of internal and external requests for personal data	781	33	42	33	18	3
3. Non-standardized data	744	77	39	38	6	4
4. Quality of data supplied by the subject individual or third party	597	170	91	39	11	1
5. Software and hardware problems	544	181	117	31	30	7
6. Inadequate guidance/timeframes from central management agencies	695	73	83	22	15	5
7. Insufficient staff/resources	450	88	200	97	65	10
8. Incidents of unauthorized access/exceeding authorized access	881	26	3	0	0	0
9. Network security	844	47	8	3	0	0
10. Other (SPECIFY.) _____ _____ _____	39	10	3	2	6	1

Appendix III  
U.S. General Accounting Office Survey of  
Computers, Networks, and Privacy

49. Consider the problems, if any, that were indicated above. In your opinion, what are the three most significant problems in your agency? (ENTER CODE FROM QUESTION 48; FOR EXAMPLE, 'VOLUME OF DATA' IS CODE '1'.)

1. 7 Most significant problem (Insufficient staff/resources)
  2. 4 Second most significant problem (Quality of data supplied by the subject individual or third party)
  3. 5 Third most significant problem (Software and hardware problems)
  4. 52 agencies had no significant problems
50. Please elaborate on the problems that you ranked above. (Use additional paper, if necessary.)

81 agencies commented.  
69 agencies did not comment.

51. If you have any comments that you would like to make about the questionnaire or computer security in general, please provide them below.

42 agencies commented.  
108 agencies did not comment.

52. REMINDER: PLEASE PROVIDE COPIES OF FMFIA, PCIE, AGENCY AND CONSULTANT REPORTS FOR FISCAL YEARS 1988 AND 1989 (QUESTION 43.)

Thank you for your cooperation.

ATTACHMENT

DEFINITION OF TERMS

Computer matching - the computerized comparison of two or more automated lists or files of personal information to identify inconsistencies or irregularities among the lists or files.

Computer profiling - the searching through a record system (or record systems) for a specified combination of data elements, i.e., the profile (e.g., types of people more likely to be engaging in illegal drug activity).

Computer system - any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception, of data or information. This includes computers; ancillary equipment; software, firmware, and similar procedures; services, including support services; and related resources.

Exceeding authorized access - to access a computer with authorization and to use such access to read, obtain, or alter personal information in the computer that the accessor is not entitled to access.

Hit - one or more data elements in two or more automated files that appear to be identical or similar when compared (e.g., name, Social Security number, address, date of birth, and the like).

Network - the composition of a communications medium and all attached components for transferring information. Such components may include, but are not limited to, host computers, communication circuits, packet switches, telecommunications controllers, key distribution centers, access control centers, technical control devices, and other components used by the network.

Operator of a federal computer system - a federal agency, contractor of a federal agency, or other organization that processes information using a computer system on behalf of the federal government to accomplish a federal function.

Personal data - any type of information on an individual.

Personal identifier - the name of an individual, or some identifying number (e.g., Social Security number), symbol, or other identifying particular assigned to the individual.

ATTACHMENT

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

Third-party information - information obtained on an individual from sources other than the subject individual.

Unauthorized access - to gain access to a computer without expressed or implied authorization or permission for purposes of reading, obtaining, altering, or destroying information.

---

# Major Contributors to This Report

---

**Information  
Management and  
Technology Division,  
Washington, D.C.**

Linda D. Koontz, Assistant Director  
Jerilynn B. Hoy, Assignment Manager  
Mary T. Brewer, Evaluator-in-Charge  
Araceli Contreras, Evaluator

---

**Boston Regional Office**

James S. Jorritsma, Regional Assignment Manager  
C. Jeff Appel, Senior Evaluator  
Elizabeth Q. Nacar, Evaluator  
Susan Wong, Evaluator

---

**Human Resources  
Division, Washington,  
D.C.**

Luann M. Moy, Social Scientist

---

**Requests for copies of GAO reports should be sent to:**

**U.S. General Accounting Office  
Post Office Box 6015  
Gaithersburg, Maryland 20877**

**Telephone 202-275-6241**

**The first five copies of each report are free. Additional copies are \$2.00 each.**

**There is a 25% discount on orders for 100 or more copies mailed to a single address.**

**Orders must be prepaid by cash or by check or money order made out to the Superintendent of Documents.**

---

**United States  
General Accounting Office  
Washington, D.C. 20548**

**Official Business  
Penalty for Private Use \$300**

**First-Class Mail  
Postage & Fees Paid  
GAO  
Permit No. G100**

---