Chapter 3

Computer Matching To Detect Fraud, Waste, and Abuse

Contents

Tables

Figure

Chapter 3

Computer Matching To Detect Fraud, Waste, and Abuse

SUMMARY

Computer matching involves the comparison of two or more sets or systems of computerized records to search for individuals who may be included in more than one file. Matching can be done manually with paper files. But, as a practical matter, time and cost requirements make manual matching prohibitive in cases involving a large number of records. The primary impetus for Federal and State use of computer matching is to detect fraud, waste, and abuse in government welfare and social service programs. However, computer matching has broad applicability to government programs and activities.

Computer matching has the potential to improve the efficiency of government recordkeeping and management of government programs. It is widely used by many States and foreign countries, the private sector, and increasingly by the Federal Government, where the technique is strongly supported by the Office of Management and Budget (OMB) and the inspectors general, among others, and has been endorsed in several public laws.

However, a number of problems have been identified in Federal computer matching activities, including weak oversight, little persuasive evidence or documentation of cost-effectiveness, widely variable record quality, and little consideration of the implications for privacy and civil liberties.

In computer matching, the basic policy conflict is between the efficient management of government programs (including effective law enforcement) and the rights of individuals. The fourth amendment protects "persons, houses, papers, and effects" against unreasonable government searches and seizures. The Privacy Act of 1974 requires that information collected for one purpose not be used for another purpose, unless, among other exemptions, it falls within a "routine use. Under OMB guidelines, personal information used in computer matches can be disclosed under the routine use exemption.

OTA'S assessment of computer matching technology and policy issues found that:

- Although Congress has legislated general and specific restrictions on agency disclosure of personal information, it has also endorsed computer matching and other record linkages in various programmatic areas specified in several public laws. Thus, congressional actions appear to be contradictory.
- It is difficult to determine how much computer matching is being done by Federal agencies, for what purposes, and with what results. However, OTA estimates that in the 5 years from 1980 to 1984, the number of computer matches nearly tripled.
- As yet, nG firm evidence is available to determine the costs and benefits of computer matching and to document claims made by OMB, the inspectors general, and others that computer matching is cost-effective.
- The effectiveness of computer matches used to detect fraud, waste, and abuse can be compromised by inaccurate data.
- c There are numerous procedural guidelines for computer matching, but little or no oversight, follow-up, or explicit consideration of privacy implications.
- As presently conducted, computer matching programs may raise several constitutional questions, e.g., whether they violate protection against unreasonable search and seizure, due process, and equal pro-

tection of the laws. But, as presently interpreted by the courts, the constitutional provisions provide few, if any, protections for individuals who are the subjects of matching programs.

- The Privacy Act as presently interpreted by the courts and OMB guidelines offers little protection to individuals who are the subjects of computer matching.
- The courts have been used infrequently as a forum for resolving individual grievances over computer matching, although some organizations have brought lawsuits.
- Computer matches are commonly conducted in most States that have the computer capability. At least four-fifths of the States are known to conduct computer matches, most in response to Federal directives.
- All Western European countries and Canada are using computer matching or record linkages, to an increasing degree, as a technique for detecting fraud, waste, and abuse.
- In designing policy for computer matching, consideration of the following factors is important:
  - — which records to make available for computer matches and for what purposes,
  - —approval required before a match takes place,
  - —notice to individuals,
  - —whether to require a cost-benefit analysis,
  - —verification of hits, and
  - —appropriate action to be taken against an individual who has submitted false information.

In response to the OTA survey of Federal agencies, OTA determined that:

- Forty-three percent of agency components that reported participation in computer matching activities (16 out of 37) said that the matches were required or authorized by legislation.
- Eleven cabinet-level departments and four independent agencies carried out a total of 110 matching programs, with a total of 553 matches conducted from 1980 to April 1985.
- In the 5 years from 1980 to 1984, the number of computer matches nearly tripled.
- For 20 percent of the matches reported, information was available on the number of records matched, number of hits, and percent of hits verified.
- Despite the low percentage of respondents providing information on reported matches, the number of separate records used in the reported matching programs totaled over 2 billion; the total number of records matched was reported to be over 7 billion due to multiple matches of the same records.
- The percentage of hits (i.e., matches between the specific items of interest in two different records) verified to be accurate ranged from 0.1 to 100 percent.
- Sixty-eight percent (25 of 37) of the agencies indicating that they participated in matching programs said that procedures were used to ensure that the subject record files contain accurate information.

INTRODUCTION

Computer matching involves the electronic comparison of two or more sets or systems of personal records. [1] Matching is used to check for individuals who should not appear in two systems of records, as in the case of Federal employees above a certain salary level and persons receiving food stamps. Matching can also be used to locate individuals who should appear in two systems of records but do not; for example, males registered for the draft and males over the age of 18 with driver's licenses. Although manually comparing the contents of

[1] The Office of Management and Budget (OMB) Guidelines, issued May 11, 1982, define computer matching as "a procedure in which a computer is used to compare two or more automated systems of records or a system of records with a set of non-Federal records to find individuals who are common to more than one system or set."

two record systems is a traditional audit technique, this practice becomes prohibitive when dealing with massive record systems that are not uniformly comparable with other record systems. Computers greatly facilitate such comparisons.

Because of the number of people who may be subject to computer matching and because it can be done without their knowledge, computer matching has raised a number of policy questions. The basic conflict is between the efficient management of government programs and the rights of individuals.

It is well known that government programs are subject to fraud, waste, and abuse. Although the problem is not peculiar to welfare programs, fraud and waste in these programs have been particularly well documented. For example, the General Accounting Office (GAO) reviewed improper payments for fiscal year 1978-79 in 5 of the 58 federally supported welfare programs, and estimated that Federal and State welfare agencies spent about $867 million on erroneous welfare payments because recipients had not properly reported their income and assets.[2]

Since 1977, computer matching has been used extensively by a number of Federal departments and State agencies. Some specific examples of matching include:

1. recipients of Aid to Families With Dependent Children (AFDC) matched with the Social Security Administration's earnings record,
2. the Veterans Administration's rolls matched with the supplemental security income (SS1) benefit rolls,
3. AFDC recipients matched with Federal civilian and military payrolls, and
4. State AFDC rolls matched with other State AFDC rolls.

In general, matching is used to detect unreported income, unreported assets, duplicate benefits, incorrect social security numbers, overpayments, ineligible recipients, incongruous entitlements (SS1 checks mailed to deceased individuals, mothers claiming more children than exist), present addresses of individuals (Parent Locator Service, Student Loan defaulters), and providers billing twice for the same service.

In order to facilitate computer matching, a number of computerized databanks have been created solely for matching purposes. One example is the Medicaid Management Information System that contains information on recipient records, provider data, and claims-processing information.[3] A proposed computerized databank is the Internal Revenue Service (IRS) Debtor Master File that will contain the names of all delinquent Federal borrowers to match against tax returns.[4]

A central policy issue is whether and under what conditions the use of computer matching is appropriate, given the rights of individuals who are the subjects of matching and given the possible long-term societal effects of general electronic searches, as elaborated below.

As discussed in chapter 2, public opinion polls indicate that Americans value their privacy and generally expect that activities in one area of their lives are kept separate from those in other areas. In the 1983 Harris Survey, most Americans (from two-thirds to three fourths) responded that agencies that release the information they gather to other agencies or individuals are seriously invading personal privacy.[5] Two-thirds or more of Americans surveyed believed that the following government information practices would entail a "serious invasion of privacy"—the IRS not keeping individual tax records confidential (84 percent perceived this as a serious invasion); the Fed-

[2]U.S. General Accounting Office, "Legislative and Administrative Changes To Improve Verification of Welfare Recipients Income and Assets Could Save Hundreds of Millions," liRD-82-9, Jan. 14, 1982.

[3]U.S. Department of Health and Human Services. Health Care Financing Administration, "Medicare and Medicaid Data Book," 1982.

[4]Judith A. Sullivan, "IRS To Create Debtor File," *Government Computer News*, Nov. 8, 1985, pp. 1, 70.

[5]Louis Harris& Associates, Inc., *The Road After 1984: A Nationwide Survey of the Public and Its Leaders on the New Technology and Its Consequences for American Life*, (conducted for Southern New England Telephone for presentation at The Eighth International Smithsonian Symposium, December 1983), table 1-6.

eral Bureau of Investigation not keeping information about individuals confidential (82 percent viewed as serious invasion); and the Census Bureau not keeping information about individuals confidential (73 percent viewed as serious invasion). Yet, in a 1979 survey, 87 percent of respondents believed that government agencies were justified in using computers to check welfare rolls against employment records to identify people claiming benefits to which they are not entitled. However, they were less supportive (68 percent) of the IRS use of matching to check tax returns against credit card records.[G]

Public opinion polling results suggest that Americans recognize that a balance must be struck between individual rights and the protection of society. A majority of the public believes that there are some costs in terms of privacy that must be paid in order to have a more lawful society. In response to the statement: "In order to have effective law enforcement, everyone should be prepared to accept some intrusion into their personal lives, " 57 percent agreed and 36 percent disagreed.[7] Public opinion research also indicates that Americans have certain expectations about the scale of government monitoring activities. Americans assume that government investigations are predicated on evidence of individual wrongdoing and that procedural standards and safeguards exist for investigative behavior. The public overwhelmingly believes the police should not be able to tap the telephones of members of suspicious organizations without obtaining a court order. A large majority of the public is concerned about protecting records from examination by public authorities without a court order. Over 80 percent of the public believes that the police should not be able to examine the bank records of suspicious individuals without a court order.[8]

Computer matches can also conflict with the expectation of being treated as an individual. Computer matches are inherently mass or class investigations, as they are conducted on a category of people rather than on specific individuals. In theory, no one is free from these computer searches; in practice, welfare recipients and Federal employees are most often the targets.

[7]Louis Harris & Associates, Inc., and Alan F. Westin, *The Dimensions of Privacy: A National Opinion Research Survey of Attitudes Toward Privacy* (conducted for Sentry Insurance, 1979), table 9.3.

[7]Ibid., table 2.2.

[8]1bid., table 8.3.

BACKGROUND

Technology

In conducting a computer match, one computer file is compared with another using software that instructs the computer to search for certain patterns, e.g., duplicate social security numbers, same names, identical addresses. Before a match is conducted, agency personnel need to determine whether the relevant data are formatted in a similar fashion on the two or more systems being matched. If not, then the data need to be reformatted or the software must be designed to take the differences into account.

Files can be compared either by using computer tapes of the record systems or by direct electronic linkages of computers. At the present time, the matching of tapes is the procedure commonly used. However, as systems become more compatible and costs drop, direct electronic linkages between/among systems are likely to increase.

During the match, computer files are compared on the basis of a specified data element as an identifier, generally the social security number. Experience from early computer matches suggested that social security numbers were often inaccurate. In order to ensure the effectiveness of a computer match, a search for erroneous social security numbers can be conducted before the match. Additionally, the

identifier used for the match can be the social security number plus another data element, such as the first few letters of a last name.

The social security number is not essential to computer matches as databases can also be searched for combinations of selected factors; however, a unique identifier makes matching far easier. In 1981, congressional legislation required that every member of a household receiving food stamps must have a social security number. Such a requirement makes matching more efficient because it is easier to identify duplicate or fraudulent recipients.

The resulting match produces information on individuals who are common to the two files; for example, an individual who has not repaid a Federal student loan may also be a Federal employee, or a physician may have billed Medicaid twice for the same service. Once the match has identified the files having duplicate or similar information, these files are considered "hits." The hits must then be verified manually to determine whether the same individual is really involved and whether there is cause to believe that the individual has committed fraud.

Policy History

In the early 1970s, a few States began to use computer matching to check AFDC recipients against wage information from the State Employment Security agencies. The first major computer match at the Federal level was Project Match, announced in November 1977 by Joseph Califano, Secretary of the Department of Health, Education, and Welfare (HEW). Project Match compared computer tapes of welfare rolls and Federal payroll files in 18 States, New York City, the District of Columbia, and parts of Virginia. The goal was to detect government employees who were fraudulently receiving AFDC benefits. Privacy advocates in Congress, members of the Privacy Protection Study Commission, the American Civil Liberties Union, and others criticized the proposed match as a "fishing expedition. "

There were disputes within the general counsel's office at HEW regarding the legal implications of conducting these matches, especially in light of the Privacy Act "routine use' provisions.' There were also disputes between HEW and the Civil Service Commission (CSC) and the Department of Defense (DOD), neither of which wanted to release its tapes because of the routine use provision. 1° The general counsel at CSC raised two concerns regarding the compatibility of the proposed match with the routine use provision of the Privacy Act: first, "it is evident that this information on employees was not collected with a view toward detecting welfare abuses, " and second, "that disclosure of information about a particular individual at this preliminary stage is (not) justified by any degree of probability that a violation or potential violation of law has occurred. "11 CSC and DOD eventually released their tapes to HE W—CSC justifying the transfer on the argument that HEW could get the information under the Freedom of Information Act if it so chose, and DOD justifying the transfer as a new 'routine use' under the Privacy Act. HEW lawyers, themselves, were additionally concerned that the results of the match would need to be transferred to the employing departments for verification, which would also raise Privacy Act issues. As table 6 indicates, it was possible to justify under existing law all record transfers required by Project Match.

While Project Match was under way, an interagency advisory group of Federal personnel officials questioned whether Federal employees should be notified under the Privacy

---

'See Jake Kirchner, "Privacy-A History of Computer Matching in the Federal Government, " *Computerworld*, Dec. 14, 1981, pp. 1-16. Section 3b of the Privacy Act establishes the conditions under which an agency can disclose personal information to another party without the prior consent of the individual. One of these conditions of disclosure is *'for a routine use, " defined as "the use of such record for a purpose which is compatible with the purpose for which it was collected" [3(a)(7)]. All routine uses are to be published in the *Federal Register*, including "the categories of users and the purpose of such use" [3(e)(4)(D)].

[10]For correspondence, see Kirchner, Op. cit., and pp. 122-125 of U.S. Congress, Senate, Hearings Before the Senate Subcommittee on Oversight of Government Management, Committee on Governmental Affairs, *Oversight of Computer Matching To Detect Fraud and Mismanagement in Government Programs* (Washington DC: U.S. Government Printing Office, Dec. 15-16, 1982) [hereafter referred to as the Cohen hearings].

[11]See Cohen hearings, op. cit., p. 123.

Table 6.—Project Match Information Disclosures

Disclosure	Justification
Health, Education, and Welfare Department disclosure of social security number and birth dates to other agencies	**Exception in Privacy Act**
Office of Personnel Management disclosure to Health, Education, and Welfare Department	**Public interest outweighs personal privacy outlined** in the Privacy Act and information could be obtained under the Freedom of Information Act
Defense Department disclosure of military personnel on active duty to Health, Education and Welfare Department	Exception under "routine use" of the Privacy Act
State government disclosure of State Aid to Families With Dependent Children (AFDC) rolls to Health, Education, and Welfare Department	Privacy Act does not apply to States; no Federal law barring such disclosure
State government disclosure of State AFDC rolls to Federal employer agencies	New "routine use" published in the Federal Register based on original routine uses
Agencies disclosure of annotated work sheets to the Health, Education, and Welfare Department	HEW Inspector General Statute requiring agencies to respond to information requests by Inspector General
Agencies disclosure of civil or criminal proceedings to Health, Education, and Welfare Department	Exception in Privacy Act
Health, Education, and Welfare Department disclosure to State or local agencies	Exception in "routine use" of Privacy Act to assist States and localities enforce violated statutes
Agencies refer information and case to Department of Justice when lawbreaking is suspected	Exception under "routine use" or law enforcement exception of the Privacy Act
Agencies referral of cases to other agencies when lawbreaking is suspected or for investigation of government employees	For administrative action authorized by the "routine uses" of Privacy Act

SOURCE Kenneth James Langan, "Computer Matching Programs A Threat to Privacy" *Columbia Journal of Law and Social Problerns, VOI. 15, No 2, 1979,* pp. 149-150

Act of the record transfers. The Department of Justice argued against notification, saying, "We view Project Match as a law enforcement program, designed to detect suspected violations of various criminal statutes in (government) operations." 12 Opponents of the match pointed out that such a view was hardly consistent with the "routine use" concept.[13] By March 1978, Project Match had identified 7,100 employees who were possibly ineligible for welfare. But, it had also generated so much information that agency officials could not follow up adequately to determine the validity of that information.[14]

After Project Match was completed, Secretary Califano advocated more Federal use of matching and tried **to access** private sector company files. This increased public pressure for justification of matching under the Privacy Act, and OMB and the Carter White House began to take a more active role in the process. In late 1977, OMB sent a letter to Representative Richardson Preyer to explain the Administration's justifications for Project Match, concluding that 'the requirement of compatible purpose in the routine use is difficult and is ultimately largely a matter of judgment."5

While Project Match was being run, the White House was concurrently conducting its Privacy Initiative, following the 1977 report of the Privacy Protection Study Commission. The conflict between the goals of the Privacy Initiative and Project Match was not ignored within the White House, but remained unresolved. In response to concerns about Project Match's privacy implications, OMB took on the task of writing guidelines for computer matching, with input from the President Office of Telecommunications Policy and the White House Privacy Initiative.

In 1979, Congress required States to conduct wage matching for AFDC recipients. Because

"Kirchner, op. cit., p. 7.

[13]See testimony of John Shattuck of the American Civil Liberties Union, Cohen hearings, op. cit., p. 80.

[14]Laura B. Weiss, "Government Steps Up Use of Computer Matching To Find Fraud in Programs, " Congressional *Quarterly Weekly Report,* Feb. 26, 1983, p. 432.

[5]Kirchner, op. cit., p. 10.

computer matching was perceived as an efficient tool for managing benefit programs, States increasingly began to use it for a number of programs and with a number of sources, including private institutions such as employers and banks. One of the largest and best publicized of the State efforts occurred in Massachusetts in 1982 when welfare recipients were matched against bank records, identifying about 600 people who had bank accounts larger than regulations allowed. About 160 of those persons identified received termination notices. But for more than 110 of these 160 persons, the identification based on the computer match was later determined to be based on erroneous information, e.g., inaccurate social security number or bank account for burial expenses held in trust. 'G

Since 1979, concern about the size and efficiency of the Federal Government and the increase in the Federal deficit has made management a policy priority for both Congress and the executive branch. One effect has been to encourage the use of computer matching, especially as a technique to detect fraud, waste, and abuse. In 1981, President Reagan established the President's Council on Integrity and Efficiency (PCIE), chaired by the Deputy Director of OMB, to enhance interagency efforts to reduce fraud and waste, and to give the inspectors general a direct link to the President. PCIE projects include: 1) a long-term computer matching project; 2) Project Clean Data (i.e., standardization of data elements); and 3) an inventory of State computer matching software packages. President Reagan has also formed the President's Council on Management Improvement, composed of the senior management official from each major department and agency (including central management agencies—OMB, the General Services Administration, and the Office of Personnel Management), the Assistant to the President for Policy Development, and the Assistant to the President for Presidential Personnel. Its purpose is to advise the President and to oversee agency implementation of management reforms.

In 1982, President Reagan established the President Private Sector Survey on Cost Control, popularly known as the Grace Commission, to study management problems in government. Its major finding was "that the Federal Government has significant deficiencies from managerial and operating perspectives, resulting in hundreds of billions of dollars of needless expenditures . . . "[7] There have been criticisms of the Grace Commission's cost figures and its methodology .18 In 1982, the Reagan Administration also announced Reform '88, a program to increase efforts to reduce waste, fraud, and abuse, and to restructure the management and administrative systems of the Federal Government.

[15]Ross Gelbspan, "Computer Matching Stirs Up Criticism," *Boston Globe*, June 9,1985, p. A 1, cont. A4.

[17]Ellen Law, "Grace Reports To the President," *Government Computer News*, March 1984, p. 4.

"Steven Kelman, "The Grace Commission: How Much Waste in Government?' *The Public Interest, No.* 78, winter 1985, pp. 62-82.

FINDINGS

Finding 1

Although Congress has legislated general and specific restrictions on agency disclosure of personal information, it has also endorsed computer matching and other record linkages in various programmatic areas specified in several public laws. Thus, congressional actions appear to be contradictory.

As discussed in chapter 2, Congress has passed a number of laws that give an individ*ual* certain rights with respect to controlling the use of personal information, and that place restrictions on the ways in which agencies may legitimately use such information. These laws speak both to general agency practices (e.g., the Privacy Act of 1974) and to the practices of specific agencies, (e.g., Section 6103 of the Tax Reform Act of 1976).

Congress has also legislated a number of exchanges of information among agencies. Congressional concern with detecting fraud, waste, and abuse has resulted in several major legislative endeavors that have been viewed as authorizing computer matching. First is the establishment of inspectors general offices in a number of Federal agencies to identify and reduce fraud, waste, and abuse, and to identify and prosecute perpetrators (Public Law 94-452, Public Law 94-505, Public Law 97-252). The Departments of Health and Human Services, Energy, Defense, and 15 other Federal agencies have inspectors general. The inspectors general are potentially very powerful officers who:

> . . . have complicated reporting relationships involving department and agency heads, and Congress and its many committees. IGs can bypass department/agency general counsels and take matters directly to the Criminal Division of the Justice Department. They can initiate audits and investigations at any time, which can cover fraud, abuse, and any and all management deficiencies. [19]

Inspectors general employ a variety of techniques, including: 1) vulnerability assessments to assess the risk of loss in programs, 2) management control guides, 3) fraud bulletins and memos, 4) fraud control training, 5) hotlines for reports of wrongdoing, and 6) audit follow-up procedures. Matching, profiling, and front-end verification are used by inspectors general.

A second legislative endeavor that is perceived as encouraging data-sharing among agencies is the Paperwork Reduction Act of 1980 (Public Law 96-51 1), which gives OMB Federal information oversight authority and the responsibility y to promote the effective use of information technology. It establishes an Office of Information and Regulatory Affairs within OMB to carry out the purposes of the act, oversee agency compliance, and set up a Federal Information Locator System to register all information collection requests. OMB Circular A-130 was issued in December 1985 as an integrative policy statement on information resource management policies, including privacy and matching.[20]

A statute that may encourage the sharing of information within an agency is the Federal Managers Financial Integrity Act of 1982 (Public Law 97-255), which requires periodic evaluations of and reports on agency systems of internal control and action to reduce fraud, waste, abuse, and error. OMB Circular A-123 (October 28, 1981) complements the act by mandating an improvement in internal control systems, including a requirement that agency heads issue specific internal control directives and review plans for all components of their agencies. Inspectors general have the responsibility to review directives. OMB Assistant Director Wright and Comptroller General Bowsher have pledged that:

> OMB and GAO plan to work together very closely in implementing the Act and in assuring that the momentum already built up within the agencies for improved internal control is sustained.[21]

A fourth statute that encourages exchanges of personal information is the Debt Collection Act of 1982 (Public Law 97-365), which establishes a system of data-sharing between Federal agencies and private credit reporting agencies in order to increase the collection of delinquent nontax debts. The act permits agencies to:

1. refer delinquent nontax debts to credit bureaus to affect credit ratings;
2. contract with private firms for collection services;
3. require applicants for Federal loans to supply their taxpayer identification numbers (social security numbers);
4. offset the salaries of Federal employees to satisfy debts owed the government;
5. screen credit applicants against IRS files to check for tax delinquency;

[19] John D. Young, "Reflections On the Root Causes of Fraud, Abuse and Waste in Federal Social Programs," *Public Administration Review, 1983,* p. 366.

[20] Office of Management and Budget, "Management of Federal Information Resources," Circular No. A-130, Dec. 12, 1985.

[21] Office of Management and Budget, "Agencies to Tighten Internal Control Systems," OMB 82-26 (President Task Force on Management Reform), Oct. 8, 1982.

6. turn over to private contractors the mailing addresses of delinquent debtors obtained from IRS;
7. extend from 6 to 10 years the statute of limitations for collection of delinquent debts by administrative offset; and
8. charge interest, penalties, and administrative processing fees on delinquent nontax debts.

The law requires agencies to provide due process to individuals before using any of the newly authorized methods of collection. The law provides safeguards to preserve the confidentiality of taxpayer information, and civil and criminal penalties are included when taxpayer addresses are improperly disclosed. OMB estimates that the improved procedures and newly available tools will result in an additional $500 million in annual collections.[22] OMB has decided that:

> Rather than creating a new bureaucracy to implement the credit reporting provisions of the Debt Collection Act, the existing nationwide network of commercial and consumer credit bureaus will be under contract to provide this service for all departments and agencies.[23]

The statute requiring the most far-reaching data-sharing is the Deficit Reduction Act of 1984 (DEFRA) (Public Law 98-369), which requires the establishment of new State information systems for verification purposes and the use of verification in a number of federally funded State-administered programs. This 1,2 10-page law provides tax reforms and spending reforms, primarily by amending the Social Security Act and Internal Revenue Code. Provisions that are relevant to management and efficiency are in Subtitle C—' Implementation of Grace Commission Recommendations, " Section 2651.

The major changes in the Social Security Act mandated by DEFRA include requiring States or State agencies to: 1) have an income and eligibility system, 2) obligate recipients to supply their social security numbers and require States to use those numbers in the administration of programs, 3) compel employers to keep quarterly wage information, 4) exchange relevant information with other State agencies and with the Department of Health and Human Services, and 5) notify recipients and applicants that information available through the system will be requested and utilized. The programs that must participate in the income verification program are: AFDC; Medicaid; unemployment compensation; food stamps; and any State program under a plan approved under Titles I, X, XIV, or XVI of the Social Security Act. Under DEFRA, no Federal, State, or local agency may terminate, deny, suspend, or reduce any benefits of an individual until such agency has taken appropriate steps to independently verify information.

DEFRA provides certain procedural rights for the individual, including that the agency shall inform the individual of the findings made on the basis of verified information, and give the individual an opportunity to contest such findings. DEFRA makes a number of changes in the Internal Revenue Code, including that the Commissioner of Social Security shall, on request, disclose information on earnings from self-employment, wages, and payments on retirement income to any Federal, State, or local agency administering one of the following programs: AFDC; medical assistance; supplemental security income; unemployment compensation; food stamps; State-administered supplementary payments; and any benefit provided under a State plan approved under Titles I, X, XIV, or XVI of the Social Security Act. Information with respect to unearned income may also be disclosed from the IRS files to the above agencies.

In addition to these broad endorsements of and requirements for computer matches, there are a number of statutes that authorize specific computer matches (see table 7).

Congressional restrictions on agency disclosures of personal information and congres-

[22] Office of Management and Budget, "OMB Announces Progress in Administration's Debt Collection Effort ," OMB82-32 (Reform '88 Communications), Dec. 15,1982.

[23] Office of Management and Budget, "Government to Use Credit Bureaus to Cut Delinquent Debts; Delinquency Growth Halted, OMB83-29(Public Affairs Management), Sept. 23, 1983.

Table 7.—Statutes Authorizing Specific Computer Matches

Tax Reform *Act of* 1976, Public Law 94-455, permitted the Department of Health, Education, and Welfare to search the databanks of other Federal agencies to locate parents who fail to pay child support.

Social Security Amendments of 1977, Public Law 95-216, required States to use wage data in determining eligibility for Aid to Families With Dependent Children (AFDC) Program benefits by providing them access to earnings information held by the Social Security Administration (SSA) and State employment security agencies.

Food Stamp Act Amendments of 1977, Public Law 96-58, granted access to employer-reported wage information for recipients of supplementary security income (SSI) benefits.

Food Stamp Act Amendments of 1980, Public Law 96-249, amended the Internal Revenue Code and the Social Security Act to allow State food stamp agencies to obtain and use wage, benefit, and other information in SSA files and those of State unemployment compensation agencies.

Food Stamp and Commodity Distribution Amendments of 1981, Public Law 97-98, required States to obtain and use earnings information obtained from employers.

Department of Defense Authorization Act of 1983, Public Law 97-252, required the Secretary of Education to prescribe methods for verifying that individuals receiving any grant, loan, or work assistance under Title IV of the Higher Education Act of 1965 had complied with registration as necessary under the Military Selective Service Act.

Deficit Reduction Act of 1984, Public Law 98-369, required the Internal Revenue Service (IRS) to disclose information about an individual's unearned income to State welfare agencies and the SSA to verify the income of an applicant or beneficiary of the AFDC, SSI, and food stamp programs. (Presently, IRS is required to disclose only information on earned income.) The Deficit Reduction Act also requires States to maintain a system of quarterly wage reporting as part of its income verification system.

SOURCE Off Ice of Technology Assessment

sional authorizations of computer matching place agencies in a position where the legitimacy of either a disclosure or refusal to disclose can be challenged. A prime example is *Tierney v. Schweiker, 718* F.2d 449 (1983), which involved the Social Security Administration's (SSA) use of confidential tax return information maintained by IRS for purposes of verifying the income and assets of supplemental security income recipients. SSA was acting on its congressional mandate that SSA'S determinations of eligibility be based on "relevant information [that is] verified from independent or collateral sources and additional information [that is] obtained as necessary. "[24] Two GAO reports[25] recommended that SSA use IRS tax information to verify eligibility. In deciding the case, Judge Abner Mikva recognized that:

> Much of the confusion , . . arises from conflicting signals given by the Congress. In 1972, when enacting the Social Security Amendments that instituted the Benefits program, Congress was concerned with ensuring that financially ineligible individuals not abuse the system. To this end, Congress directed the SSA to obtain as much information as possible to discover such ineligibility. In 1976, when expanding the confidentiality provisions as part of the Tax Reform Act of 1976, Congress made clear that tax information was to be absolutely confidential, subject to certain explicit exceptions. Although Congress created numerous exceptions, none was applicable to the information which SSA now seeks. When Congress speaks with two separate minds, the conflicting goals can present difficult dilemmas.[2G]

In response to the OTA survey, 43 percent of agency components that reported participation in computer matching activities (16 out of 37) said that the matches were required or authorized by legislation. However, approximately one-third of the respondents cited general statutes such as an Inspector General Act, the Debt Collection Act, or an Omnibus Reconciliation Act. Another one-third cited explicit requirements for matching, such as the Uniform Code of Child Support or Title 7, U. S. C., chapter 51, "Food Stamp Program. " Another onethird cited more general authorization, e.g., Public Law 96-473, which requires the suspension of benefits for inmates of penal institutions and is given as the basis for matches between inmate records and social security files.

Finding 2

It is difficult to determine how much computer matching is being done by Federal agencies, for what purposes, and with what results. However, OTA estimates that, in the 5 years from 1980 to 1984, the number of computer matches nearly tripled.

[24] 42 U.S.C. sec. 1383(3)(1)(B) as quoted in *Tierne-y v. Schweiker* 718 F,2d 449, 451 (1983).

[25] U.S. General Accounting Office, HRD 81-4, Feb. 4, 1981 and HRD 82-9, Jan. 12, 1982.

[26] *Tierney v. Schweiker 718* F.2d 449, 454 (1983).

There has been no accurate accounting of the number of matches that have been done at the Federal level. In part, this is a definitional problem. One distinction that affects reports of the amount of computer matching being done is that of "matching programs" versus "matches." The OMB guidelines define a "matching program" as:

> . . . a procedure in which a computer is used to compare two or more automated systems of records or a system of records with a set of non-Federal records to find individuals who are common to more than one system or set. The procedure includes all of the steps associated with the match, including obtaining the records to be matched, actual use of the computer, administrative and investigative action *on* the hits, and disposition of the personal records maintained in connection with the match. It should be noted that a singIe matching program may involve several matches among a number of participants.[27]

Based on this definition, there will be many more matches than there are matching programs, as one matching program may include a number of record sets (e.g., Office of Personnel Management (O PM) records with SSA records and OPM records with Farmers' Home Administration loans), and/or a matching program may involve a number of matches at certain intervals, e.g., yearly or monthly. However, this distinction between matching programs and matches has not always been recognized in accounts of numbers of computer matches.

A second important distinction in understanding reports on the scale of computer matching by Federal agencies is one made by OMB. Some compilations of computer matching at the Federal level include only those matches that fall under the OMB guidelines, others include both, and still others do not differentiate. OMB'S guidelines state that the following are not matching programs:

1. Matches that do not compare a substantial number of records, e.g., comparison of the Department of Education's Defaulted Student Loan database with the OPM'S Federal Employee database, would be covered; comparison of six individual student loan defaulters with the OPM file would not.
2. Checks on specific individuals to verify data in an application for benefits, done soon after the application is received.
3. Checks on specific individuals based on information that raises questions about an individual's eligibility for benefits or payments, done reasonably soon after the information is received.
4. Matches done to produce aggregate statistical data without any personal identifiers.
5. Matches done to support any research or statistical project where the specific data are not to be used to make decisions about the rights, benefits, or privileges of specific individuals.
6. Matches done by an agency using its own records .28

For the purposes of this report, the first three applications are considered front-end verification and are discussed in chapter 4. The fourth and fifth applications are not relevant to this inquiry. The sixth application does include a significant number of matching programs and matches that are relevant to this discussion, e.g., SSA and another component of the Department of Health and Human Services.

In addition to definitional problems, the rules for reporting matches may not require that all matches be reported. Notices of computer matching programs that meet the criteria in the OMB guidelines may appear in the Federal Register as a new routine use. However, if the agency providing the data believes that the system of records already contains such a use, then no additional notice in the F'ed-end Register is required. No notice is required for records that are matched within an agency.

There have been a number of attempts at determining the scale of computer matching. Figures range from 200 programs on upwards.

[27]Office of Management and Budget, "Privacy Act of 1974; Revised Supplemental Guidance for Conducting Matching Programs, " *Federal Register,* vol. 47, No. 97, May 19, 1982, p. 21657.

[28]Ibid., p. 21757.

For example, in 1982 hearings on computer matching, Senator William Cohen estimated that:

> As of January 1982, Federal agencies had completed more than 85 matching programs and State government agencies are now performing approximately 170 matches involving public assistance records, unemployment compensation records, government employee files, and in some cases, the files of private companies. These projects involve the records of hundreds of thousands of citizens.[29]

At the same hearings, Thomas McBride, former Inspector General of the Department of Labor, testified:

> So my guess is we are talking about a population of roughly 500, more or less, routine recurring matches going on, some of them subject to Federal legislative action, some of them not.[30]

The Long Term Computer Matching Project of the President's Council on Integrity and Efficiency has issued three compilations of Federal computer applications to prevent/detect fraud, waste, and abuse. These compilations do not provide complete listings of computer matching programs.[31] They include those computer matches that agencies chose to report; some agencies submitted partial reports, others appear not to have responded at all, or to only one or two of the PCIE'S requests. Some of the reported matches are one time only, others are recurring. The first compilation was distributed in 1982[32] and reported 77 matches; the second was distributed in July 1984 as an expansion and update, and reported 162 matches; and the third was distributed in January 1986 as an update, and reported 108 matches.[33] (See table 8 for breakdown by agency.)

A 1985 GAO study, *Eligibil.z"ty Verification and Privacy in Federal Benefit* Programs: A *Delicate Balance,* reported that:

> Before 1976, only two benefit program-related Federal computer matching projects were conducted. However, recent inventories of Federal and State agencies' computer matching programs show that Federal agencies had initiated 126 benefit-related matches, 38 of which were recurring as of May 1984. State agencies, as of October 1982, had initiated more than 1,200 matching projects, most of them recurring.

[29] Cohen hearings, op. cit., p. 2.

[30] 1 bid., p. 20.

[31] It does not appear that the PCIE inventory used the OMB guidelines' definition of computer matching programs. Some agencies reported matches within their agency, e.g., Department of Health and Human Services Black Lung and SSA Title II. Some agencies reported particular matches within a matching program.

[32] None of the compilations is dated. The phrase 'distributed in 1982" is used by PCIE in its second compilation to describe the first compilation.

[33] The low figures in the 1986 compilation can be attributed to two factors. The first is that some large agencies that previously had reported a number of matches did not respond, e.g., Departments of Labor, Defense, and Justice. The second factor is that many agencies have increased their use of computer screens and profiles rather than their use of computer matches. This latter factor will be discussed in ch. 4.

Table 8.—Computer Matches Reported to the PCIE Long-Term Computer Matching Project

	1982	1984	1986
Department of Agriculture	11	10	23
Department of Commerce	0	1	1
Department of Defense	0	30	0
Department of Education	1	1	0
General Services Administration	1	1	18
Department of Health and Human Services	29	58	55
Department of Housing and Urban Development	0	4	3
Department of the Interior	0	1	0
Department of Justice	8	5	0
Department of Labor	12	12	0
National Science Foundation	0	2	0
Nuclear Regulatory Commission	0	1	0
Peace Corps	0	1	0
Pension Benefit Guaranty Corp.	0	1	0
Office of Personnel Management	3	5	0
Railroad Retirement Board	0	8	1
Small Business Administration	1	1	0
Department of State	2	2	0
Tennessee Valley Authority	0	4	5
Department of the Treasury	0	3	0
Veterans Administration	9	11	2

SOURCE President's Commission on Integrity and Efficiency,

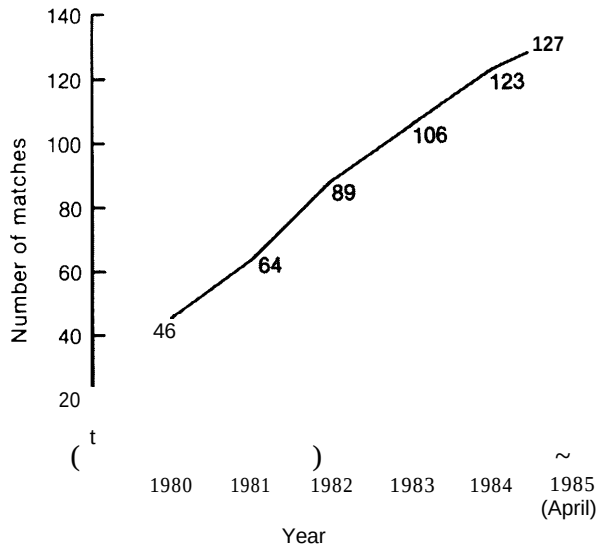
In response to the OTA survey of Federal agencies, 11 cabinet-level departments and 4 independent agencies reported conducting 110 matching programs[34] with a total of approximately 700 matches from 1980 to April 1985. The Departments of Energy and State were the only two cabinet-level departments that reported no matching programs. Of the 20 independent agencies surveyed, only three (NASA, Selective Service System, and Veterans Administration) reported any matching programs (see table 9 for a breakdown of matching programs by agency).

While the data from the responses to OTA and to PCIE are not directly comparable, the trend toward increased use of computer matches is clear (see figure 4). In the 5 years from 1980 to 1984, the number of computer matches nearly tripled.

From 1979 to 1984, OMB received only 56 reports on matching programs from Federal agencies. According to OMB records, there were 11 matches reported in 1979; 2 in 1980; 11 in 1981; 13 in 1982; 6 in 1983; and 13 in 1984. The OMB figures are obviously lower than the matching figures reported elsewhere because: 1) only those matching programs that fit the OMB definition are included; and 2) some agencies do not submit match notices under the routine use and systems of records, but instead fit matching programs into existing routine use and existing systems of records.

[34] Some of these matching programs are conducted within an agency and therefore do not fall within the OMB definition.

Figure 4.—Computer Matches Conducted From 1980 to April 1985



SOURCE: Off Ice of Technology Assessment

Table 9.—Computer Matching Programs[a] Reported to OTA

Department of Agriculture	33
Department of Commerce	1
Department of Defense	15
Department of Education	3
Department of Health and Human Services	1
Department of Housing and Urban Development	3
Department of the Interior	3
Department of Justice	6
Department of Labor	21
Department of Transportation	1
Department of the Treasury	14
National Aeronautics and Space Administration	1
Selective Service	1
Veterans Administration	7

[a] Some of these matching programs are conducted within an agency and therefore do not fall within the OMB definition.

SOURCE OTA Federal Agency Data Request

In determining the scale of computer matching activities at the Federal level, it is also important to consider the number of records that have been matched. In response to the OTA data request, information on number of records matched, number of hits, and percent of hits verified was provided for 20 percent of the matches reported. Despite this low response, the number of separate records used in the reported matching programs totaled over z billion; the total number of records matched was reported to be over 7 billion due to multiple matches of the same records.

Finding 3

As yet, no firm evidence is available to determine the costs and benefits of computer matching and to document claims made by OMB, the inspectors general, and others that computer matching is cost-effective.

Before discussing the attempts to date at estimating costs and benefits, it is important to place computer matching within a context. Computer matching is a technique that has been used primarily to detect client fraud, which is only one component of fraud, waste, and abuse. In order to accurately determine the cost-effectiveness of computer matching, the extent of client fraud must first be documented. If client fraud accounts for only a small percentage of total fraud, waste, and abuse, then other techniques to detect other types of fraud, waste, and abuse maybe more cost-effective overall. In this respect, one author cited the 1978 Annual Report of the HEW Inspector General, which estimated that the Department lost between $5.5 and $6.5 billion through management inefficiencies, program misuse, and fraud. In this instance, management inefficiencies and program misuse accounted for 97 percent of the inspector general's estimate of losses, while client fraud accounted for only 3 percent.[36]

In response to the OTA survey, only 8 percent of the agencies that reported participation in computer matching activities (3 out of 37 agencies) said that they did cost-benefit analyses prior to computer matching. Eleven percent (4 of 37) reported doing cost-benefit analyses after matching.

Various individuals and organizations have asserted that computer matching is cost-effective, but have provided little or no specific information on actual costs and benefits. For example, Joseph Wright, OMB'S Deputy Director, reported in an OMB circular that:

> The IG's are wisely using this spectacularly effective technique to reap for the American public the savings that private industry has for many years been obtaining. Use of this technique will help assure that individuals who are not entitled to receive payments don't, making more money available for those who are deserving.[3b]

Likewise, the Grace Commission concluded that:

> Computer matching is an effective management tool for identifying fraud, waste, and abuse of government benefits, entitlements and loan programs. Computer matching is useful in other ways too, such as validating billings of large government contractors. . . Recommendations in the task force reports to correct information problems related to this issue provide opportunities for cost savings and revenue of $15.9 billion over 3 years ($11.3 billion when information gaps cited in other issues in the Report are netted out).[37]

In the 1982 Cohen hearings on computer matching, former Inspector General McBride of the Department of Labor testified that:

> The hits, the overpayments, for the big benefit programs run somewhere between 1.8 up to maybe 4 percent, depending on what program you are talking about. For AFDC, the hits are probably somewhere at the lower end, because they do a little better job of verification. Food stamps is a little higher. Unemployment insurance may be even higher, in some States particularly .38

In a 1983 article, Richard Kusserow, Inspector General of the Department of Health and Human Services, reported:

> Our own Project Spectre which matches Social Security beneficiary payments with Medicare death files has led to about $7.5 million in recoveries to date. Recoveries, in this case, covers all monies collected by our investigators, including checks not cashed but debited to the treasury. We project total savings over time to reach $25.2 million.[39]

In *Computer Matching in State Admim"stered Benefi"t Programs: A Manager's Guide*

"Young, op. cit., p. 362.

[36] 0MB 83-14.

"President's Private Sector Survey on Cost Control, *A Report to the President* (1984), Part II: Issue and Recommendation Summaries, p. 82; see pp. 84-86 for examples.

[38] Cohen hearings, op. cit., p. 19.

[39] Richard P. Kusserow, "Fighting Fraud, Waste and Abuse," *The Bureaucrat,* fall 1983, p. 23.

to Decision Making,'" the quantitative benefits of computer matching include estimated savings and measures of grant reductions, collections, and corrections. The list of qualitative benefits is longer, including: increased deterrence, improved eligibility determinations, enhanced public credibility for benefit programs, more effective referral services, and improved databases.

The costs of computer matching vary according to the size of the record set, as well as the complexity, quality, and compatibility of the records. In *Computer Matching in State Administered Benefit Programs,* the quantitative costs include: hardware/software; computer processing time; space; supplies; personnel managers, data-processing staff, eligibility assistance workers, clerical workers, hearings officers, fraud investigators, collections staff, attorneys, and training staff; other public agency resources; and private institution resources. The qualitative costs include: reduced staff morale, heightened public concerns about "big brother, " increased political conflict, gamesmanship with numbers, operational inefficiencies, and diversion of resources. Definitions for these qualitative costs are not offered.

All agree that verification costs are the highest and the most difficult to compute. In *Computer Matching in State Administered Benefit Programs,* it is pointed out that:

> Follow-up is the most costly, labor-intensive part of the computer matching process. Most notably, it involves what can be a very tedious and time-consuming job of verifying hits. But it also involves other components such as making any necessary change in a recipient case status, calculating and pursuing overpayments, hearing appeals, making referrals to fraud units, and actually conducting criminal investigations and pursuing convictions.[41]

There is some disagreement as to how much verification, both in terms of number of hits verified and in terms of records and sources checked, is necessary. For example, the Department of Health and Human Services' Inspector General Kusserow has suggested that:

> For large matches, officials would have to analyze only a sample of the hits to verify the matching process. After doing this, officials should take corrective measures, proceeding cautiously against any individual where doubt exists.[42]

The PCIE Long Term Computer Matching Committee has developed some information on the costs of selected matches. For many of the matches, the information presented is very sketchy. The matches for which the PCIE offered the most complete information are listed in table 10.

David H. Greenberg and Douglas A. Wolf have recently completed a study[43] in which they constructed a cost-benefit framework (see table 11) and used it to evaluate the performance of computer wage-matching systems of welfare agencies in four areas: Camden County, New Jersey; Mercer County, New Jersey; San Joaquin County, California; and the State of New Hampshire. In each of their study sites, they reported that they obtained reliable and complete information on the costs of matching, but were unable to measure benefits as precisely. Additionally, there were some benefits, e.g., deterrent effects and positive effects on attitudes of affected parties, that they could not measure at all. Thus, they regard their test of the cost-effectiveness of wage matching to be a conservative one.

Greenberg and Wolf concluded from their four case studies that the benefits from computer matching outweighed the costs by "substantial amounts' '[44] (see table 12). If computer matching were as effective nationally, they suggested that "cost savings in the food stamp and AFDC programs would be approximately

[40] U.S. D–epartment of Health and Human Services, Office of Inspector General, *Computer Matching in State Administered Benefit Programs,* June 1984, p. 25.

[41] Ibid.

[42] Richard P. Kusserow, "The Government Needs Computer Matching To Root Out Waste and Fraud, " *Communications of the ACM,* vol. 27, No. 6, June 1984, p. 544.

[43] David H. Greenberg and Douglas A. Wolf, "Is Wage Matching Worth All the Trouble?' *Public Welfare,* winter 1985, pp. 13-20.

[44] 1 bid., p. 18.

Table 10.—Examples of Cost/Benefit Analyses

Costs/benefits	Selected matches					
	DO L/TVA	IRS/DOL	OPM/SSA	OPM/OPM	RRB/HCFA	USAFIVA
Equipment costs	1,500	125,000	10,950	2,291	6,124	1,000
ADP staff costs	1,200	25,000	3,213	2,142	1,831	1,150
Staff verification costs	4,500	1,000,000	94,163	12,968	15,763	96
Travel and other costs	10,000	—	39,416	—	10,028	100
Cases found	21	219	770	170	405	340
Overpayments identified	35,000	103,000	9,100,000	640,800	2,263,927	71,000
Cases with recoveries made	2	219	—	—	364	—
Overpayments recovered	2,500	139,000	—	—	993,118	—
Overpayments prevented	—	—	770	170	—	1,300
Amount prevented	—	50,000	4,089,600	46,300	—	274,000
Questioned costs	—	—	—	—	—	—
Disallowed costs	—	—	—	—	—	—

KEY: DOL = Department of Labor, TVA = Tennessee Valley Authority, IRS = Internal Revenue Service; OPM = Office of Personnel Management; SSA = Social Security Administration; RRB = Railroad Retirement Board; HCFA = Health Care Financing Administration, USAF = U S Air Force, VA = Veterans Administration.

SOURCE President's Council on Integrity and Efficiency Long Term Matchlng Committee, '(Draft/Summary of Federal Computer Applications for Prevention of Fraud and Abuse "

Table 11.—Costs and Benefits of Wage Matching

Benefits:
Restitution of previous overpayments
Savings from food stamp disqualifications
Savings from benefit reductions and discontinuances:
- prevention of future overpayments
- administrative savings

Changes in behavior and attitudes:
- deterrent effects
- improved client attitudes
- improved staff morale
- improved relations with the public

costs:
Personnel costs (salaries and fringe benefits):
- income maintenance staff
  fraud investigative staff
- district attorney staff
- other

Materials and facilities costs:
- computers
- word processors
- forms
- general overhead such as office space, telephone, supplies

SOURCE: David H. Greenberg and Douglas A Wolf, "IS Wage Matching Worth All the Trouble?"Public *We/fare,* winter 1985, p 16

Table 12.—Estimated Costs and Benefits of Computer Matching in Four Sites

	costs	Benefits	Ratio
Mercer County	$786,821	$ 932,958	1.19
Camden County	753,662	1,452,367	1.93
San Joaquin County	308,128	762,355	2.47
New Hampshire (DES Wage Crosshatch Project)	264,856	707,316	2.67

NOTE" All figures are in annual terms pertaining mainly to 1982

SOURCE David H. Greenberg and Douglas A. Wolf, "IS Wage Matching Worth All the Trouble?" *Pub/K We/fare,* winter 1985, p t8

1 or **2** percent. "[45] However, they caution that this may not be the case because they chose wage-matching programs that were functioning well:

> For example, the employer-reported data used by these systems clearly were adequate in terms of coverage, content, and timeliness. Equally important: follow-up procedures were well-structured, adequate resources were available for follow-up, and supervisors were genuinely committed to the program. Without such conditions, it certainly is possible that wage matching could prove ineffective.[46]

Finding 4

The effectiveness of computer matches that are used to detect fraud, waste, and abuse can be compromised by inaccurate data.

The Massachusetts case discussed earlier, in which 110 of the 160 termination notices that were sent following a computer match were based on erroneous information, is the best known example of use of inaccurate data. However, many matches experience some problems with inaccurate data, and, in part, computer matching can be effective in detecting errors in data.

[45] Ibid.
[46] Ibid.

One indicator, although not complete, of the quality of data used in computer matching is the percentage of hits verified as accurate. In response to the OTA survey, this percentage ranged from 0.1 to 100 percent. For example:

The Department of Housing and Urban Development conducted computer matches to identify tenants in five different cities who had not reported all income when applying for federally assisted housing. The hit rates varied from about 6 to 54 percent, and the hit verification rates varied from 13 to 55 percent. The actual number of matches that resulted in valid hits ranged from 0.8 to 29 percent.

- The Department of Commerce Inspector General's office conducted a match to identify departmental employees who were collecting unemployment benefits. A total of 22,000 records were matched resulting in 98 hits, of which about 10 percent were verified.
- The Department of Education conducted a match to identify current and former Federal employees who were delinquent on student loans. About 10 million records were matched resulting in 46,860 hits, of which 100 percent were verified, according to Department officials.
- The Veterans Administration conducted a match to identify Federal employees and annuitants who were erroneously receiving VA compensation. About 15 million records were matched resulting in 5,166 hits, of which about 23 percent were verified.

For the majority of matches reported to OTA, information on hits verified was either unknown or unavailable.

Proponents of matching programs are taking measures to improve the quality of data used in matches. SSA has developed a computer software program to screen social security numbers and pull out inaccurate or incongruous numbers. Other agencies engaging in matching programs are likewise concerned. In response to the OTA survey, 68 percent (25 of 37) of the agencies indicating that they participated in matching programs said that procedures were used to ensure that the subject record files contain accurate information.

Finding 5

There are numerous procedural guidelines for computer matching, but little or no oversight, follow-up, or explicit consideration of privacy implications.

Program personnel appear to have substantial discretion in deciding whether or not to use computer matching as an audit technique or means to detect fraud, waste, and abuse. There are few internal agency checks. The Inspector General's Office may be involved in planning a computer match; and the General Counsel's Office and the Privacy Act officer may be involved. But it appears that there are no agency or general policy guidelines regarding what types of information should be matched, against which records of what other agencies, and for what purposes. These substantive issues are rarely addressed.

For those matching programs that meet the OMB definition, agencies providing information "are responsible for determining whether or not to disclose personal records from their systems and for making sure they meet the necessary Privacy Act disclosure when they do. " In making this determination, agencies are instructed to consider the following:

- legal authority for the match;
- purpose and description of the match;
- description of the records to be matched;
- whether the record subjects have consented to the match; whether disclosure of records for the match would be compatible with the purpose for which the records where originally collected, i.e., whether disclosure under a' 'routine use' would be appropriate; whether the soliciting agency is seeking the records for a legitimate law enforcement activity; or any other provision of the Privacy Act under which disclosure may be made;
- description of additional information that may be subsequently disclosed in relation to "hits";

- subsequent actions expected of the agency providing information (e.g., verification of the identity of the "hits" or follow-up with individuals who are "hits"); and
- safeguards to be afforded the records involved, including disposition.

However, neither the source agency, the matching agency, nor OMB is accountable for the decision whether or not to disclose records for a matching program. For matching programs that do not fall under the OMB guidelines, there are no formal procedures or guidelines-one program manager may ask another for access to records for matching purposes, and no one else need know.

OMB has developed a number of procedural guidelines. The initial guidelines, *OMB Guidance to Agencies on Conducting Automated Matching Programs,* became effective on March 30, 1979. The purpose of the guidelines was "to aid agencies in balancing the government need to maintain the integrity of Federal programs with the individual's right to personal privacy. " Under the guidelines, a match was to be performed "only if a demonstrable financial benefit can be realized that significantly outweighs the costs of the match and any potential harm to individuals that could be caused by the matching program. " To this end, the guidelines required documentation of benefits, costs, potential harm, and alternatives considered to detect or curtail fraud and abuse or to collect debts owed to the Federal Government (see 5a of guidelines for listing). A report describing the match (see 9b.1 and 2 of guidelines for details) was to be submitted, 60 days before the match was initiated, to the Director of OMB, the Speaker of the House, and the President of the Senate. Necessary notices of system of records, new or altered systems, or routine use were to republished in the *Federal Register,* allowing 30 days for public comment. Any disclosures of personal information during the match were to be made in accordance with the "routine use" limitations noted in the *Federal Register.* Unless it was a continuing matching program, the guidelines stipulated that personal records should be destroyed or returned to the source agency within 6 months. The guidelines also suggested that matching should be done in-house by agency personnel, not by contractors.

The application of these guidelines was not very satisfactory for any party concerned. Agencies did not conduct cost-benefit analyses in a systematic fashion; instead, they were quickly estimated when asked for by OMB in order to comply with the letter of the guidelines. There was almost no public comment in response to matches proposed in the *Federal Register.* There was little congressional reaction to matching programs. There was minimal to no oversight by OMB; it processed the necessary paperwork, but never 'disapproved' a match. In part, OMB'S behavior can be attributed to the lack of clarity in the guidelines concerning its role. For example, it was not clear from the guidelines whether OMB had the authority to disapprove a match.

Based on the unsatisfactory experience under the 1979 guidelines, the PCIE'S Long Term Computer Matching Project decided that one of its first projects would be to revise the OMB guidelines. In conjunction with advice from PCIE, OMB'S *Revised Supplementary Guidance for Conducting Matching Programs* became effective May 1,1982. The 1982 guidelines simplified the administrative reporting requirements of the 1979 guidelines by eliminating the cost-benefit analysis, reducing the notice and reporting requirements, and exempting intra-agency matching programs. Publication of "routine uses" in the *Federal Register* was still required, but the 30-day public comment period for matching reports and advance notice to Congress and OMB were eliminated.

OMB and PCIE also developed a Model *Control System for Conducting Computer Matching Projects Involving Individual Privacy Data (1983).* The Model Control System is designed to provide procedural guidance to agencies conducting computer matching projects to help them comply with the Privacy Act and the OMB guidelines. The model includes 10 steps that agencies should follow:

1. define the match program,
2. determine the feasibility of the match,
3. establish matching and follow-up procedures,
4. confer with the agencies providing information,
5. publish routine use notice,
6. make a matching report,
7. obtain the agency data file,
8. conduct computer matching,
9. analyze and refine the raw hits, and
10. perform follow-up procedures.

Agencies are not required to follow the Model Control System, or to report to OMB on which procedures were followed.

In late 1983, OMB developed a *Computer Match Checklist* that must be on file for review by OMB, GAO, or other Federal entities. The checklist must be completed by both the agency providing information and the agency conducting the match immediately following *Federal Register* publication of an intent to match. Items on the checklist include: compliance with notification requirements, number of individuals whose records are to be matched, contractor involvement, and the date on which a cost/benefit analysis on the match will be available. Estimates of cost/benefit analyses are to be attached to the checklist.

In December 1985, OMB issued Circular A-130, *Management of Federal Information Resources,* which directs agencies to review annually every matching program in which they have participated, either as a matching or source agency, to ensure that the requirements of the Privacy Act, the OMB Matching Guidelines, and the OMB Model Control System and Checklist have been met. Additionally, agencies are to include in the Privacy Act Annual Report the number and description of matching programs participated in as a source or matching agency.

Finding 6

As presently conducted, computer matching programs may raise several constitutional questions, e.g., whether they violate protection against unreasonable search and seizure, due process, and equal protection of the laws. But, as presently interpreted by the courts, the constitutional provisions provide few, if any, protections for individuals who are the subjects of matching programs.

The fourth amendment provides individuals the right "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures. " The fourth amendment presumption, reinforced by case law and by the presumption of innocence additionally reflected in the fifth and sixth amendments, is that searches are not warranted unless there is indication of a crime. If there is probable cause of a crime and the individual's involvement, then a court may issue a search warrant. Fourth amendment case law has resulted in the concept of "expectation of privacy. "

The question of whether or not computer matches raise fourth amendment issues turns, in large part, on the 'expectation of privacy" that individuals have in records about them maintained by a third party, in this case primarily a government agency. Based on the Supreme Court ruling in United *States v. Miller, 425* U.S. 435 (1976), records that are held by a third party, and used by that party for administrative purposes, are considered the property of the third party. Under such circumstances, the individual does not have an assertible fourth amendment privacy interest in those records. Although *Miller* applied to records held by a bank, the logic of the holding may apply similarly to records held by the government.

In *Jaffess v. Secretary HE W, 393* F. Supp. 626 (S.D. N.Y. 1975), a district court allowed a computer match of recipients of veterans' disability benefits with those receiving social security benefits. The court held that the disclosure under the matching program was 'for the purpose of proper administration. Jaffess had not reported his social security income, and after the match his {eterans' benefits were reduced. He claimed that a constitutional right of privacy protected his records. The court rejected this claim:

> ... the present thrust of decisional law does not include within its compass the right of an individual to prevent disclosure by one governmental agency to another of matters obtained in the course of transmitting agency's regular functions.[47]

But, the legal question of what kind of fourth amendment "expectation of privacy" an individual has when he or she fills out a form and swears that the information provided is true and correct has not been specifically decided. Nor has the question of the privacy rights of Federal workers in information provided and maintained for employment purposes. In both instances, statutes, especially the Privacy Act, may give more precise legal guidance than the U.S. Constitution. However, the constitutional question could still be subject to further litigation.

A second fourth amendment issue that is raised by computer matches is the scope of the search. Computer matches are general electronic searches of, frequently, millions of records. Under the fourth amendment, searches are not to be overly inclusive—no 'fishing expeditions" or "dragnet investigations. " Yet, in matches, many people who have not engaged in fraud are subject to the computer search. If matches were to be considered a fourth amendment search, then some limitations on the breadth of the match and/or justifications for a match may be necessary. For example, the agency may need to show that a less intrusive means to carry out the search was not available, and that procedural safeguards limiting the dangers of abuse and agency discretion were applied. These may also be required under due process protections as discussed below.

A final fourth amendment issue that may be raised by computer matches is that of suspicion that criminal activity is occurring. If the purpose of a match is to produce evidence that someone has defrauded the government, then a computer match could be regarded as a search under the fourth amendment. Such a match may also conflict with the presumption of innocence, as reflected in the fourth and fifth amendments, if the individual is required to prove that he or she has not engaged in wrongdoing. If the purpose of a match is to detect and correct errors, and not to detect wrongdoing, then a match would probably not be regarded as a search under the fourth amendment.

The *due process* clause of the fifth[48] (Federal Government) and 14th (State governments) amendments ensures procedural protections before the government takes action against an individual. Generally, this clause has been held to require that individuals be given notice of their situation, the opportunity to be heard, and the opportunity to present evidence on their own behalves. In agency proceedings, this constitutional principle is given specific meaning in the Administrative Procedures Act (1946). Additional elements of due process that apply specifically to eligibility for benefit programs include: the right to a pre-termination hearing, placing the burden of proof *on* the gOVernment to prove ineligibility if the individual swears to eligibility, and entitlement to benefits pending resolution. These procedural due process protections were extended to welfare recipients in *Goldberg v. Kelly, 397* U.S. 254 (1970).

Under the 1979 OMB guidelines, notice of a proposed match is to be published in the Fed*eral Register 30* days before to allow time for comments. Many have questioned the adequacy of this, as the vast majority of individuals do not read the *Federal Register.* Additionally, there is evidence that agencies have not complied with the 30-day time period and that some agencies have provided notice *after* the match was well under way.[49] This requirement was eliminated in the 1982 OMB guidelines. DEFRA now requires more specific no-

"Kenneth James Langan, "Computer Matching Programs: A Threat to Privacy?" *Columbia Journal of Law and Social Problems,* vol. 15, No. 2, 1979, pp. 158-159.

"It does not specifically provide for equal protection, but the Court ruled in *Bolling* v. *Sharpe* (347 U.S. 497, 19854) that "the concepts of equal protection and due process, both stemming from our American ideal of fairness, are not mutually exclusive" and that the fifth amendment also provided equal protection.

[49]See Cohen hearings, op. cit.

tice prior to some matches. It is important to recognize that notice can take place at various points in the matching process, i.e., before the match occurs, once an individual appears as a "hit," and prior to any outside verification. Notice can also be provided rather passively, e.g., a statement on a form, or requiring the active acknowledgment of the individual. Based on results of the OTA survey, 8 percent (3 out of 37 agency components) of the agencies reporting that they participated in computer matching said that individual subjects of the match had provided written consent prior to a match.

Once a match has taken place, the resulting "hits" are further investigated in order to verify their status. At this time, these individuals may not be given notice of their situation, or the opportunity to be heard and present evidence on their own behalves. They may not be notified until and unless the agency decides to take some action against them. Based on the Court's ruling in *Goldberg,* due process would require a hearing for an individual whose benefits are to be terminated or lowered based on information from computer matching. Such hearings may be quasi-judicial in nature, but the individual would not have the right to a lawyer or jury, the burden of proof would be on the individual, and the individual may incriminate himself or herself in these hearings. If such hearings are the starting point for an investigation leading to criminal charges, then it maybe necessary to conduct them in a more formal judicial setting.

The *equal protection* clause of the 14th and, by implication, the fifth amendments prohibits the States and Federal Government from creating legal categories and taking actions that discrimin ate against members of that category (e.g., race, national origin, and gender). Economic status has never been regarded as a *sus*pect classification,'" and therefore the government interest in subjecting welfare recipients to computer matching would only need to be rationally related to a legitimate purpose of the government. In this case, the purpose, i.e., detecting fraud, waste, and abuse, would probably be regarded as legitimate, and the means chosen, i.e., computer matching, rationally related.

Despite this development of constitutional decisions, matching may conflict with the equal protection clause in that categories of people, not individual suspects, are subject to these electronic searches. In the computer matching that has been done to date, two groups of people—welfare recipients and Federal employees—have been used frequently. This is true despite arguments by supporters of matching that computer matches are effective tools in a number of situations. Although the Grace Commission and others have recognized the usefulness of matching in detecting fraud, waste, and abuse in government contracting, it has not been used to any significant extent for this purpose. DEFRA, in its section incorporating the Grace Commission recommendations, did not require or endorse the use of matching in government contracting.

Finding 7

The Privacy Act as presently interpreted by the courts and OMB guidelines offers little protection to individuals who are the subjects of computer matching.

The Privacy Act gives individuals certain rights of notice, access, and correction in order that they may control information about themselves. It also places certain requirements on agencies to make certain that the information they maintain is relevant, timely, and complete.

Under the Privacy Act, the individual has the right to prevent information being used without his or her consent for a purpose other than that for which it was collected. An exception to this rule is if information falls within a "routine use" of the particular record system. Under the OMB Matching Guidelines, matching can be considered such a routine use; therefore, individual consent is not required. Many argue that matching of information is

"*see* *Dandridge v. Williams, 397* U.S. 471 (1970) and San *Antonio Independent School District v. Rodriguez, 411* U.S. 1 (1973).

not consistent with the legislative intent that information should be used only for the purpose collected. As table 6 indicated, it is quite easy to find justification in the Privacy Act for disclosures of information for matching purposes.

Additionally, the Privacy Act requires agencies to 'collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs" [see.e(2)]. In computer matching, information that will be used to determine whether benefits should be eliminated, decreased, or increased is collected from third parties-not from the individual.

Although not specifically prohibited in the Privacy Act, the legislative history reflects censure of a national data center. The linking of systems in computer matching can be regarded as moving towards a de facto national data center or national recipient system. Additionally, new computerized databases are being created solely for the purpose of providing information for computer matches and other record searches. The Federal Government, under the auspices of the inspectors general, is developing a national computerized file of deceased individuals (who have no rights under the Privacy Act) for screening beneficiary records and preventing payments to deceased persons. Two other examples mentioned previously are the Medicaid Management Information System and the proposed IRS Debtor Master file. The State wage reporting systems, required under the proposed DEFRA regulations, could also be regarded as the first stage of a national data system.

The OMB guidelines require that the files used for matching be returned to the custodian agency or destroyed. However, since there is no oversight of this, records could be used for additional purposes.

Finding 8

The courts have been used infrequently as a forum for resolving individual grievances over computer matching, although some organizations have brought lawsuits.

It does not appear likely that the courts will protect individual privacy in computer matching programs .51 There are at least four reasons. The first is that the courts have not extended constitutional protections for computerized records, and the fourth amendment "search and seizure" doctrine has not been applied. The second reason is that courts only require rationality in such programs, i.e., that the means used be reasonably related to a legitimate government purpose. The purpose of achieving efficiency and detecting fraud, waste, and abuse is a legitimate one. With respect to the choice of means, courts have traditionally given deference to administrative discretion. The third reason is that when courts balance individual privacy against the public interest, the weight generally favors the public interest—all else being equal. The fourth reason is that the damage requirements of the Privacy Act are so difficult to prove that they act as a deterrent to its use.

Additionally, with large-scale computer matching, no one individual is sufficiently harmed to litigate a claim and most individuals are not even aware of the match. The cases that have gone to court have generally been brought by welfare rights organizations. These cases include:[52]

> *15, 844 Welfare Recipients v. King, 474* F. Supp. 1374 (D. Mass., 1979)–State welfare agency was required to restore benefits to recipients whose aid had been terminated either by fraud investigators improperly acting as caseworkers, or by caseworkers improperly acting as fraud investigators.
>
> *Tierney v. Schweiker, 718* F. 2d *449* (D.C. Cir., 1983)–Coerced signatures to notice-and-consent forms, extracted from SS1 recipients in preparation for an IRS matching, were invalidated because the agency action violated IRS confidentiality rules.

[51] Langan, op. cit., p. 175.

[52] *See: Henry Korman, "Creating the Suspicious Class—Surveillance of the Poor by Computer Matching, " unpublished paper, August 1985, esp. pp. 52-53.

Greater Cleveland Welfare Rights Organization v. Bauer, 462 F. Supp. 1313 (N. D. Ohio, 1978)–An Ohio wage match was invalidated insofar as subject AFDC recipients were not informed of use of their social security numbers as identifiers in the match.

Lessard v. Atkins, CA 82-3389-MA (D, Mass., Apr. 23, 1985)–Defendants in a bank match case agreed to both the use of secondary identifiers and enhanced follow-up investigations that plaintiffs argued were required by Federal law.

Finding 9

Computer matches are conducted in most States that have the computer capability. At least four-fifths of the States are known to conduct computer matches, most in response to Federal directives.

In many respects, the personal information gathered by State agencies is more sensitive and more extensive than that gathered by Federal agencies. [51] Many Federal agencies fund programs that are administered through the States (or local educational agencies). The Federal agencies do not store individually identifiable information on all of the beneficiaries of these programs, but the States do. Federal auditors regularly have access to individually identifiable information to monitor program effectiveness, but the personal data on all participants is not stored in Federal agencies themselves.

At the State level, the following information is typically stored: income or business taxpayer records in the revenue department; driving records in the Department of Motor Vehicles; public assistance in the welfare agency; drug and alcohol treatment records in the appropriate agencies; communicable diseases and abortions in the Department of Health; treatment at State institutions in the Departments of Health, Mental Health, or Public Health; current earnings in the quarterly reports submitted by employers (a few States require reporting less often) to the unemployment security office; criminal records and criminal intelligence in the State police or Department of Public Safety; educational, financial aid, and vocational training information in the Department of Education; occupational information in the various State licensing boards (attorneys, beauticians, auctioneers, boxers, vendors, physicians, etc.); patient information and physicians earnings records in the State agency administering Medicaid; suspicions of child abuse in the appropriate State agency; and birth records of adoptees in the adoption agency.

Most matching occurs in programs that are federally funded or controlled by Federal law. For example, States conduct matches in unemployment insurance programs to detect fraudulent and duplicative payments, and to monitor employers' contributions. Forty-one States reported conducting such matches, and 23 States reported matching unemployment insurance records with other jurisdictions. [54] Less than 20 States report matching for workers' compensation programs. [55] In public assistance programs, States generally match recipient files against quarterly wage reports submitted by employers to detect recipients who are receiving wages over an allowable limit. An OTA survey of eight States revealed that six (California, Colorado, Georgia, Illinois, Indiana, and Michigan) conducted such matches, while two States (Florida and Minnesota) did not. DEFRA now requires that this be done by all States.

Other examples of State matching activities include:

- Thirty-seven States submit social security numbers of welfare recipients to SSA for computerized verification that the numbers are accurate.
- At least two States, Massachusetts and Maryland, have authorizations in their laws for the public assistance program to conduct computer matches against the accounts of all bank customers in the State.

[53] Information for this section is derived from Robert Ellis Smith, *Report on Data Protection and Privacy in Seven* Selected States, OTA contractor report, February 1985.

[54] See U.S. Department of Labor Inspector General, *Inventory of Computer Matching Activities in State Labor and Related Agencies, 1982.*

[55] Ibid.

- The Iremigration and Naturalization Service is encouraging States to match motor vehicle, welfare, and unemployment files with its databank of current registered aliens. Colorado, Illinois, and California have agreed. California must approve new regulations before this can be done, and the regulations have not yet been published.
- California, Minnesota, and several other States conduct Project Intercept. Lists of persons owing money to the State—either in delinquent taxes, welfare overpayments or frauds, faulty unemployment compensation, etc.—or those reported delinquent in child support payments are submitted to the public assistance agency (or any other agency making periodic payments) so that the amount owed is offset against the State payments. This is also done with tax refund checks (not only in the States, but by the IRS as well).
- Many States compare their lists of recipients, whether public assistance, unemployment compensation, or other payment programs, against comparable lists of recipients in neighboring jurisdictions, to determine who is "double-dipping." Examples are Virginia's unemployment compensation records matched with those of Maryland and the District of Columbia; or Indiana's records matched with those of Kentucky.

There are other generic exchanges of personal data by most States that are significant, although they may not be classified strictly as "matches." Many of them predate the current Federal initiative on matching, which began in 1978. They include:

- Motor vehicle departments in 49 States provide lists of young, male drivers to the Selective Service System for matching against lists of men who have registered for a military draft. Objections, based on invasion of privacy, were expressed in many States. Some laws or regulations governing DMVS seem to prohibit such disclosures. But in the end, the Selective Service System had nearly 100 percent participation.
- More than 80 percent of the motor vehicle departments disclose driving records and accident reports to Dataflo Systems, a division of Equifax, Inc., so that Dataflo can computerize the data and market it to insurance companies. The abstract includes social security number, driver's license number, birth date, physical description, restrictions on the permit, and a chronological list of violations. An insurance company can then query one of five regional computers operated by Dataflo.
- Motor vehicle departments also disclose suspended or revoked licenses to the National Driver Register operated by the U.S. Department of Transportation in Washington and, in turn, query the system when persons apply for drivers' licenses.
- Just about all motor vehicle departments rent mailing lists of licensees and of automobile owners to mailing list firms and other marketers. A report by the Secretary of State of Illinois in 1983 stated that 44 States answered in the affirmative when surveyed on whether they rent mailing lists. The other six States did not respond. Many States, however, have regulations or laws limiting, if not fully prohibiting, such disclosures.
- Every State with a State income tax has an agreement with the IRS to exchange computerized data on its taxpayers with IRS and to receive comparable information from IRS.

An analysis of State matching activities in light of State Privacy Acts or Fair Information Practices Acts indicates that the presence of such laws does not deter computer matching. However, it often assures that there is a review of a State agency's decision to match, that there are specific procedures to follow, and that information is checked for accuracy. The critical factor in determining the extent of matching at the State level appears to be the size of the population. States with larger populations engage in more computer matching than States with smaller populations.

Finding 10

All Western European countries and Canada are using computer matching or record linkages, to an increasing degree, as a technique for detecting fraud, waste, and abuse.

In general, the specific uses of matching in Western Europe and Canada are similar to those in the United States—primarily in social welfare programs.[56] In Western European countries, computer matching and other record linkage issues are handled within the context of data protection laws and oversight. In general, European data protection laws require the advice or consent of the data protection agency before any records can be Linked. A brief review of matching activities in different countries follows.

Canada

The Canadian Privacy Act of 1982 does not address computer matching specifically, but does contain the principle that information should be used only for the purpose for which it was collected. The Canadian Privacy Commissioner, John W. Grace, has spoken out strongly on the privacy implications of matching. As he sees it:

> That computer-matching is carried on in the name of efficiency, good government and law enforcement makes it potentially a more, not less, dangerous instrument in the State's hands."

Specific instances of matching include: opening Federal databanks to obtain information for collecting alimony and child support payments from recalcitrant fathers, Revenue Canada's matching of a provincial voters' list with tax records to identify individuals who had not filed tax returns, and matches by the Canadian Employment and Immigration Commission to detect overpayment of unemployment insurance benefits.

Sweden

Under Section 2 of the Data Act, specific permission is required from the Data Inspection Board (DIB) for the linkage of files that contain "personal data procured from any other personal file, unless the data are recorded or disseminated by virtue of a statute, a decision of the Data Inspection Board, or by permission of the person registered. " DIB evaluates all proposals for record linkages and has approved an estimated 80 to 90 percent of the proposed record linkages. In reviewing proposals, DIB looks especially at the purpose of the match and the quality, e.g., timeliness, accuracy, and completeness, of the data to be used. In general, DIB is opposed to linkages of very sensitive personal information, e.g., alcoholism and drug addiction records, and linkages where the users do not know why personal information was originally collected.

DIB has not always been successful at preventing record linkages. For example, when the tax authorities sought information on income from interest and dividends from the banks, DIB said that the banks were not licensed to divulge such information to the tax authorities. Regardless, the banks gave the information to the tax authorities. DIB sought to prosecute the banks under the Data Act and the case is still under appeal.

France

The National Commission on Informatics and Freedoms (CNIL) has to authorize record linkages. In general, CNIL is opposed to linkages because of the principle that data should be used only for the purposes for which they were collected. In contrast to other countries, there are few plans for record linkages.

Federal Republic of Germany

The Republic's Federal Data Protection Act contains a general prohibition against the dissemination of personal data from one public body to another, unless the release of the information "is necessary for the legitimate accomplishment of the tasks for which the dissemination unit or the recipient is competent. "

---

[56] "Information for this section is derived from David H. Flaherty, "Data Protection and Privacy: Comparative Policies, " OTA contractor report, January 1985.

"Privacy Commissioner, *Annual Report, 1983-84,* p. 3.

Computer linkages among social services occur frequently and do not have to be reported to the Data Protection Commissioners. Most linkages of social service data outside the social service administrations are prohibited by the Social Code unless the information is necessary to prevent premeditated crimes, to protect public health under certain circumstances, to implement specific stages of the taxation process, and to assist the registered alien authorities.

Finding 11

Computer matching raises a number of policy questions that warrant congressional attention, including availability of records for matching, approval before matches, notice for individuals, requirement of cost-benefit analysis, and verification of hits.

In designing policy for computer matching, consideration of the following factors is important:

Records to be made available for computer matches and for what purposes. —Currently, there are few restrictions on the systems of records that can be used. If a "routine use" can be crafted to justify the match, then almost any Federal system can be made available. The primary exception to this is IRS information, but this restriction can be circumvented somewhat by matching with a system of records that has already been matched against IRS information. Another long-standing exception has been private sector information; however, a number of new Federal and State laws now allow for such access.

In determining what records should be available, several possibilities exist. One is to make all records available for all matches. Another is to prohibit the use of some systems of records, e.g., health information, bank records, or IRS records. A third is to make the availability of records dependent on the purpose of the match. The difficulty with this alternative, which may be otherwise attractive because it allows flexibility, is that it could easily evolve into a system similar to what currently exists where routine use exceptions are not carefully scrutinized. If the use of records is to depend on the purpose of the match, then the purposes that would legitimate the use of particular systems of records need to be specifically established in advance of proposals to match.

Another issue in determining what records are to be available is the quality of records used in computer matching. Inaccurate records detract from the effectiveness of computer matching and increase the problems individuals experience as a result of a match. Record systems could be required to meet specific data quality standards prior to being used in a computer match.

Approval required before a match takes place. —Both a process for approving matches and a substantive review of the purpose of the match must be considered. In terms of process, one task is to check on and oversee program managers' decisions to match. This check could be carried out within an agency, as often appears to be the case at present, by a formal executive branch review process, or by review by a legislative body. In addition to the process, criteria need to be developed to determine the appropriateness of matching under the circumstances. Such criteria could be based on both the privacy interests involved and the management interests.

Notice to individuals. –This depends in part on the purposes of notification. Originally, notice as part of due process was viewed as a means of empowering the individual. If an individual knew what was to take place, he or she could take measures to try to stop the action. This original goal seems to have been replaced with a more passive view of notice. In part this may be attributed to the lack of options available to an individual who is dependent on government benefits or employment. If this is indeed the case, i.e., that individuals could be told of an action with no recourse, its implications need to be acknowledged.

There are limitations to the present system of placing notices in the *Federal Register*. Other alternatives include placing a notice on the original application form, having an indi-

vidual sign a consent form at the time of application, writing all individuals prior to the match, and writing to obtain signed consent prior to the match.

An additional question is when to notify individuals–before they become part of the program, before the match, after matching has produced a hit, or after the hit has been verified?

Requiring cost-benefit analysis. –Originally, cost-benefit analyses were required prior to a match. Currently, cost-benefit analyses are to be filed with OMB following a match. Agencies have not welcomed the requirement of doing cost-benefit analyses. In part, this is because there are many qualitative costs that are difficult to measure. In part, it is because many of the quantitative costs are difficult to separate from other administrative costs. In determining what kind of a cost-benefit analysis to require, questions of time of submission, review, and components to be addressed need to be answered.

Verification of hits. -Other than for matches conducted under DEFRA, there are no requirements on verifying hits. Again, this involves two issues—the process of verification and the substance of what is to be verified. Specific questions include: do all hits have to be verified or only some predetermined percentage; what sources are to be used in verifying hits; if there is a discrepancy in information received, how is it resolved; and what is the role of the individual in the verification process?

Appropriate action to be taken against an individual who has submitted false in formation.—Presently, the individual is given an administrative hearing and can then be subject to criminal charges. If the purpose of the hearing is indeed to refine evidence for criminal proceedings, then it may be more appropriate to conduct the hearing in a formal judicial setting. Alternatively, the use of evidence from a computer match could be prohibited from criminal proceedings, allowing its use only in civil proceedings.