Chapter 4

Computer-Assisted Front-End Verification

Contents

Tables

Figures

Chapter 4

Computer-Assisted Front-End Verification

SUMMARY

Whereas computer matching involves comparing records after an individual is already receiving government benefits or services, front-end verification is used to certify the accuracy and completeness of personal information at the time an individual applies for government benefits, employment, or services. Like computer matching, any large-scale application of front-end verification is dependent on computers and telecommunication systems.

OTA found that:

- The use of front-end verification is creating a de *facto* national database covering nearly all Americans. The technological requisites for front-end verification lead to the establishment of individual databases for verification purposes and to the connection of these databases through on-line telecommunication linkages.
- There is no comprehensive information on the use of front-end verification by Federal agencies. Front-end verification is used by many States, mostly in federally funded programs, and is initiated or required by the Federal Government. Legislation, either recently enacted and/or proposed, will expand the use of front-end verification at the Federal as well as the State level.
- Front-end verification raises due process and privacy issues that have not been systematically studied.
- There has been no comprehensive study of how to conduct front-end verification in the most cost-effective manner and with the highest possible data quality.
- There are no general Federal regulations, either statutory or administrative, guiding the use of front-end verification. In designing guidelines, a number of factors warrant consideration, including:
  —the responsibility for determining access to and record quality of the databases used for verification purposes;
  —the frequency of front-end verification, i.e., routine or selective;
  –the rights of individuals;
  –the types of information used; and
  —the possible requirement of a cost-benefit analysis.

INTRODUCTION AND BACKGROUND

Computer-assisted front-end verification is used to certify the accuracy and completeness of personal information by checking it against similar information held in a computerized database, generally of a third party. It may involve certifying information that the individual has supplied, checking a database to determine if there is additional relevant information, or both. Front-end verification is used when an individual initially applies for government benefits, employment, credit, contracts, or some other government program or service. In the past, such verification was done manually on a random basis or when the accuracy of information provided was suspect. Today, the number of applications and details to be verified makes manual verification prohibitive in terms of cost and time; however, computerized databases and on-line networking make it possible to carry out such verification routinely.

Front-end verification is similar to computer matching in that it involves an electronic search for the purpose of ensuring the accuracy and completeness of information to maintain

the integrity of government programs. However, front-end verification differs from computer matching in four ways: 1) information is verified on an individual basis, rather than for a category or class of people; 2) information is verified before an individual receives any government benefits or employment; 3) its purpose is to prevent and deter, rather than to detect and punish; and 4) it is done most effectively at the time of the initial transaction, and thus accelerates the trend to on-line data linkages. For these reasons, some of the policy issues (e.g., data quality, cost-effectiveness, and administrative discretion) are essentially the same for both front-end verification and computer matching. However, other issues, such as due process and privacy concerns, are different for front-end verification than for matching.

Computer-assisted front-end verification can be done in two ways–by batch processing or by a direct on-line inquiry. If batch processing is used, the agency compiles (usually on magnetic tape) all information needing a specific type of verification, either at the end of the day or week, and sends it to the relevant source for verification. A tape-to-tape match reveals inconsistencies in the data. The second method is a direct on-line inquiry from an agency terminal to the computerized source database as each individual case is considered. An immediate on-line response reveals inconsistencies in the data. Because of its speed and efficiency, the trend is toward more direct on-line verification. For example, the Department of Health and Human Services found that 73 percent of front-end verification in the Aid to Families With Dependent Children (AFDC), food stamp, and Medicaid programs at the State level was conducted on-1ine.[1]

[1]U.S. Department of Health and Human Services, Office of inspector General, Catalog *of Automated Front-End Eligibility Verification Techniques: A Project of the President Council on Integrity and Efficiency, OAI-85-H-51,* September 1985, p. 13.

FINDINGS

Finding 1

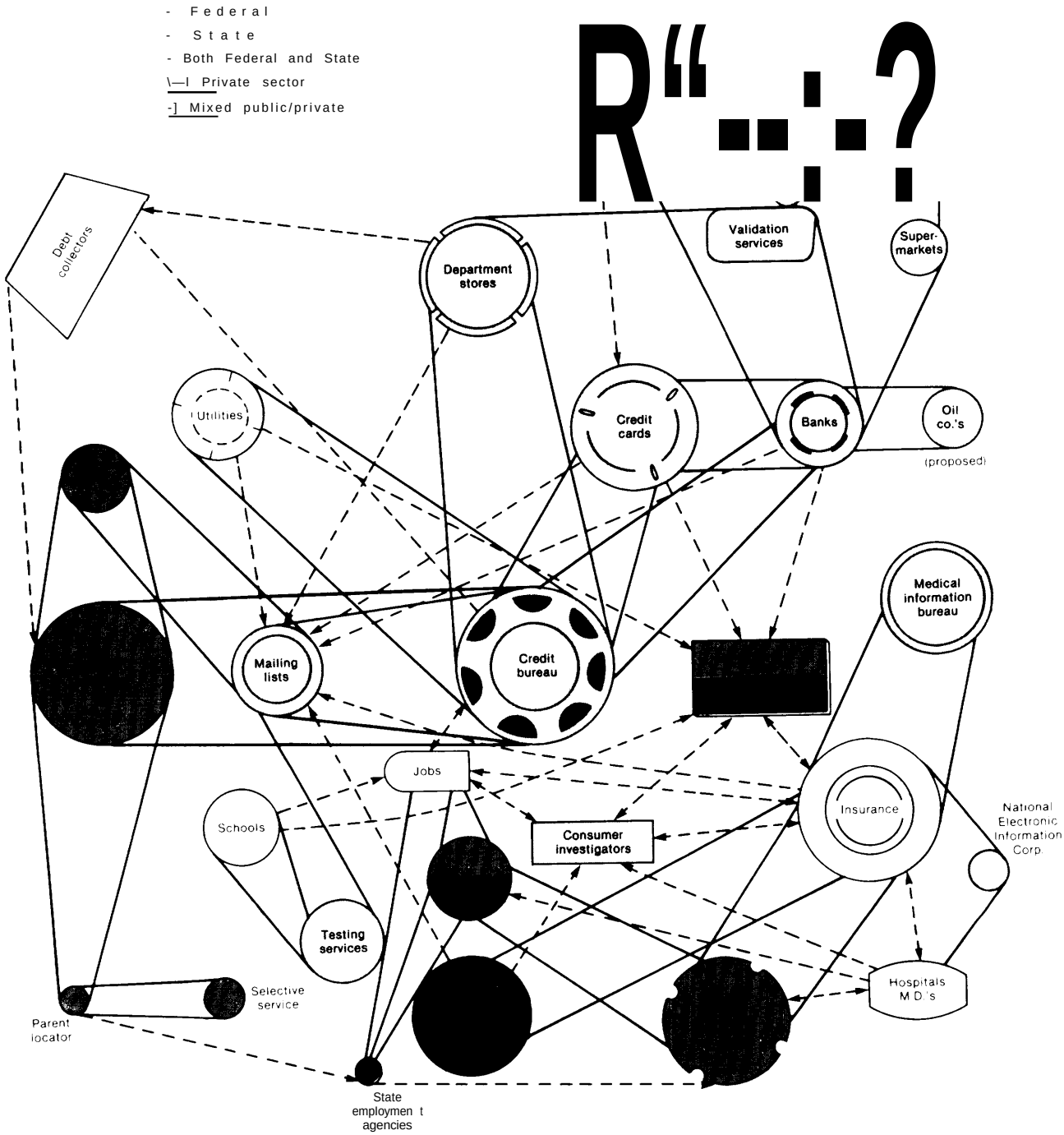
The use of front-end verification is creating a de ***facto*** national database covering nearly all Americans. The technological requisites for front-end verification lead to the establishment of individual databases for verification purposes and to the connection of these databases through on-line telecommunication linkages.

This de *facto* national database is not a centralized database in the sense that all information is contained in one mainframe computer housed in one building. Instead, the present dominant approach is to create a "virtual" central databank by electronically (via direct on-line linkages[2] or exchange of computer tapes) combining and comparing information from several separate, usually remote, record systems. If enough separate record systems are queried, the result can be the creation of a *de facto* electronic dossier on specific individuals. See figures 5 and 6 for attempts to portray the current state of computerized linkages among separate databases.

Part of the explanation for this decentralized approach to databanks and dossiers, rather than a centralized approach, is that advances in computer and data communication technology have reduced the technical and cost barriers to such interconnections. However, part of the explanation is also political in nature. The decentralized approach reflects the fragmented and complex structure of the executive branch of the Federal Government. Although Federal agencies may collect and use similar information on individuals, they also collect information that is specific to their missions and would prefer to maintain their own

[2]On-1ine telecommunication linkages involve data communications, the contents of which are not protected by existing statutory (e.g., Title III of the Omnibus Crime Control and Safe Streets Act) and constitutional prohibitions on the interception of phone calls. See U.S. Congress, Office of Technology Assessment, *Federal Government Information Technology: Electronic Surveillance and Civil Liberties, OTA-CIT-293* (Washington, DC: U.S. Government Printing Office, October 1985).

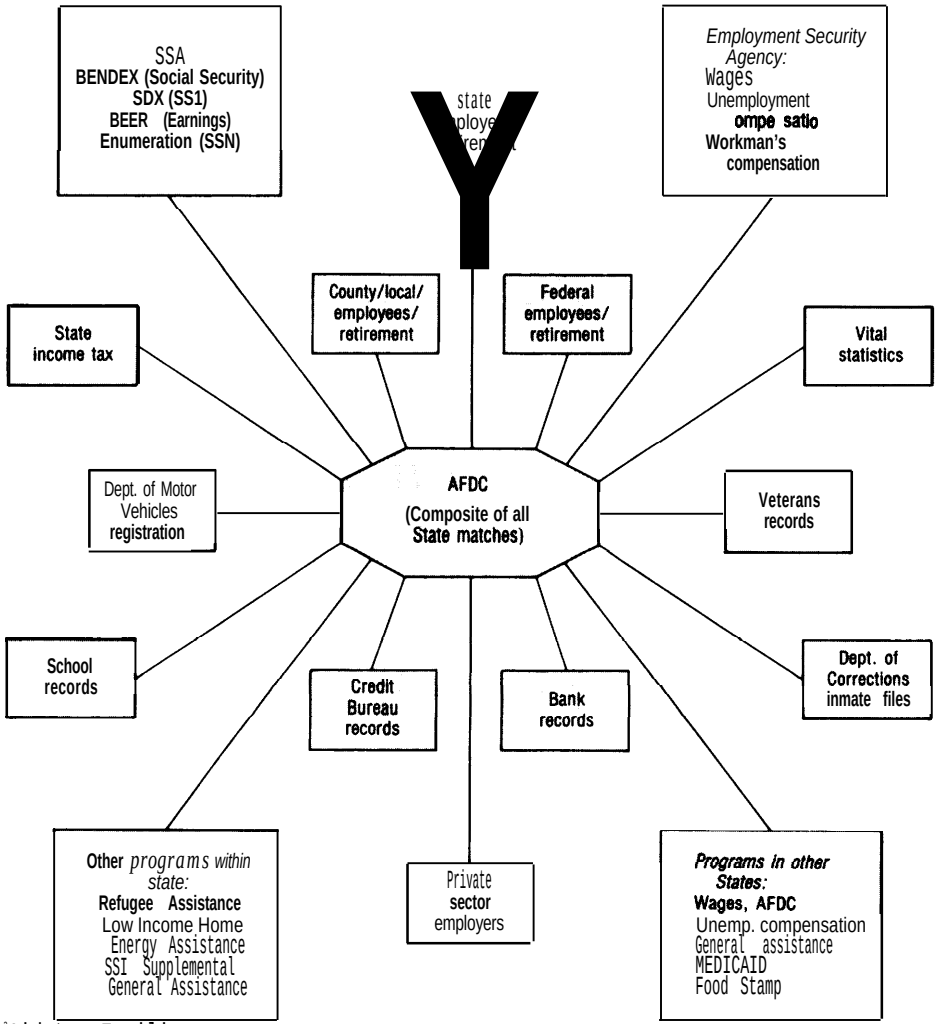
Figure 5.—Current Database Linkages



NOTES Solid lines=automated exchanges, dotted lines=manual exchanges

SOURCE *The Privacy Journal,* April 1984, p 5

Figure 6.–Composite of Data Linkages Through Computer Matches by AFDC[a] Programs in Various-States



[a]Aid to Families With Dependent Children.

NOTE" No single State has all of these links, but each link occurs in at least one State. With a few exceptions, however, these types of sources could be available in every State

SOURCE U S Department of Health and Human Services, Office of Inspector General, Inventory of State Computer Matching Technology, and GAO observation.

databases for their clients or employees. Additionally, the decentralized approach reflects incremental responses to policy problems. Databases usually are created to deal with a specific problem as seen at a particular time. Rarely is the opportunity taken to review related problems and look for a common solution.

The decentralized approach also reflects political concerns frequently expressed about centralized databanks and dossiexs. Indeed, when proposals for various national databanks were first made 15 to 20 years ago, the reaction was quite negative. Concern was expressed that, even if central databanks were technically fea-

sible, they might be more open to abuse, and might consolidate power and control in the Federal Government.[3] Since that time, few proposals for national databanks of personal information have been made or seriously considered. In cases where there has been a serious debate, the common result has been a decentralized approach. Two cases in point are the Interstate Identification Index (known as Triple I), run by the Federal Bureau of Investigation (FBI), and the National Drivers Register (NDR) run by the Department of Transportation's National Highway Traffic Safety Administration (NHTSA).

In both of these situations, proposals to maintain central databanks (on criminal history records and motor vehicle operator records, respectively) run by the Federal Government were strongly opposed by various States and civil liberty groups and ultimately defeated, even after partial implementation. In both cases, a decentralized index approach was adopted (with support from the States and civil liberty groups) as an alternative to the central databank approach. In the index approach, the Federal Government (in these examples, the FBI and NHTSA) maintains, in effect, an index to records in State record systems. Only names and identifiers are contained in the index–it does not include information about specific offenses, charges, and dispositions (for criminal history records indexed by the Triple I) or about specific driver violations and license suspensions (for vehicle operator records indexed by NDR).

The NDR contains 10 million records with information on drivers' licenses that have been revoked or suspended in various States. NDR is a voluntary Federal/State cooperative program to aid States in exchanging information about the driving records of certain individuals. Currently all States participate in reporting license withdrawals, submitting names to be checked against the NDR file, or both. NDR has been in operation since 1961 under the authority of Public Law 86-660, which directed the Secretary of Commerce to establish a register of all names of individuals reported by the States for revocation of a driver's license because of driving while intoxicated or violation of a highway safety code involving loss of life. Until 1982, reports on license withdrawals and denials contained descriptive information about the individual and details of the adverse action taken. The National Drivers Register Act of 1982 (Public Law 97-364) requires that the content of the Federal NDR file be limited to minimal, personal, identifying information with case-specific information being maintained only by the State instituting the adverse action. The 1982 law also converted NDR to a fully automated system.

The FBI's Triple I, which became operational on February 7, 1983, contained 9,268,332 records as of May 1, 1985.[4] Triple I is essentially an index of persons with criminal history records on file at the FBI and/or in State criminal history record repositories. For each person listed, Triple I includes only information on personal descriptors, identifying numbers, and the location(s) of the criminal history record(s). At present, use of Triple I is limited to criminal justice and criminal justice employment purposes, although the question of noncriminal justice use (primarily for employment and licensing checks) has not been resolved (see app. A at the end of this report for further dis-

[3] See U.S. Congress, House Committee on (government Operations, Special Subcommittee on Invasion of Privacy, *The Computer and Invasion of Privacy*, hearings, 89th Cong., 2d sess., July 25, 27, 28, 1966 (Washington, DC: U.S. Government Printing Office, 1966); and U.S. Congress, Senate Committee on the Judiciary, Subcommittee on Administrative practice and Procedure, *Invasion of Privacy*, hearings, 89th Cong., February 1965 to June 1966 (Washington, DC: (1. S. Government Printing Office, 1 965-67).

[4] FBI response to OTA Federal Agency Data Request. Also see U.S. Department of Justice, Federal Bureau of Investigation, Technical Services Division, *Statement of Work for NCIC 2000 (2K) Project—PHASE I: A Comprehensive Study To Define: System Requirements, Functioned Design and System Specs (Consistent With a Rigorous En \ ironmental Analysis Evaluation)*, January 1985, p. A9; and David F. Nemecek, "The Interstate Identification Index (1 I I)," *Interface*, SEARCH Group, Inc., 101.9, No. 1, summer 1984, pp. 1011.

cussion). If authorized criminal justice agencies obtain a "hit" or match on Triple I, the agencies obtain the actual criminal history record information from the FBI (for Federal offenders and offenders from States not yet participating in Triple I) or from State criminal record repositories (for Triple I participants). Triple I inquiries are made electronically via the National Crime Information Center's (NCIC) communication lines and, if a hit occurs, are referred or switched automatically to the appropriate holder of the original criminal history record. Records are provided by one or a combination of the following: on-line via NCIC, electronically from a State via the National Law Enforcement Telecommunications System, or by mail from the FBI or State repository.

Triple I represents an alternative to the now-defunct Computerized Criminal History (CCH) file previously maintained in NCIC. By including index entries for computerized criminal history records maintained by the FBI's Identification Division, as well as records from participating States, Triple I has been able to facilitate access to and exchange of over 9 million criminal history records, compared to the roughly 2 million records contained in the old NCIC/CCH file. However, there still are several unresolved issues concerning Triple I—noncriminal justice use, record quality, and policy oversight. These are discussed in further detail in appendix A to this report.

The decentralized approach in these instances is generally perceived as minimizing adverse impacts on Federal-State relations, since the States retain primary control over the source records. Also, the risk of abuse or misuse by the Federal Government is thought to be lessened, since there is no central file. However, authorized Federal, State, and local agencies can determine, via the index, the location of records of interest and request such records directly from the State record repositories. Thus, a dossier on any given individual can be compiled by consolidating various records from separate State agencies. It is also possible for Federal agencies to run a longer list of persons against the index to see if there are any matches, or "hits," and then follow up to obtain more detailed information.

Agencies may also maintain a centralized index of individuals whose records are maintained in their computerized databases. For example, the OTA survey revealed that the Immigration and Naturalization Service (INS) has a Central Index System (CIS) of 152 million records that contains file location, immigration status, and biographical data on individuals of interest to INS. On-line access to CIS is provided at ports of entry, file control offices, border patrol headquarters, and other agencies involved in intelligence or law enforcement. On an average, 600 users generate 100,000 file accesses per day.

Although electronically linked, on-line databases are distributed in a physical sense, they constitute a centralized database in a practical sense. As more and more systems automate and have on-line communication capability, this virtual database will grow. There are a number of computerized databases that are accessible by selected government agencies for computer-assisted verifications—for example, the computer files of the FBI's NCIC and those of the Bureau of the Customs' Treasury Enforcement Communication System. INS maintains a number of computerized record systems —the Anti-Smuggling Information System, the Central Index System, the Non-Immigrant Information System, the Student School System, and the National Automated Immigration Lookout System. The Social Security Administration (SSA) also maintains a number of databases for verification purposes—the State Data Exchange, the Beneficiary and Earnings Data Exchange, the Third Party Query, and the Enumeration Search and Verification Response System. Additionally, private sector firms, such as credit bureaus and medical insurers, maintain a number of centralized databases that are accessible by government agencies. See table 13 for a description of these databases.

Centralized databases are also created from existing decentralized databases. One example is the IRS's Debtor Master File, which was

Table 13.—Computerized Databases Used for Front-End Verification

National Crime Information Center (A/C/C) .-There are 12 files containing a total of 16,395,662 files (as of 5/1/85) that can be accessed through the NCIC system.[a] The 12 files include: the Interstate Identification Index (III) File, the Stolen Securities File, the Stolen Guns File, the Stolen Articles File, the Stolen Vehicles File, the Stolen License Plates File, the Wanted Persons File, the Missing Persons File, the Stolen Boats File, the Canadian Warrant File, the U.S. Secret Service Protective File, and the Unidentified Persons File. NCIC functions as a nationwide computerized Information service for Federal, State, and local criminal justice agencies.

Treasury Enforcement Communication System (TECS).– Includes a range of information on persons suspected of, or wanted for, violations of U.S. Customs or related laws —e. g., persons suspected of or wanted for thefts from international commerce, and persons with outstanding Federal or State warrants, The Border Enforcement System is the major component and is used to: assist Customs and the Immigration and Naturalization Service (INS) personnel screen persons and property entering and exiting the United States; provide investigative data to Customs or other agency law enforcement or intelligence officers; and aid i n the exchange of data with other Federal, State, or local law enforcement agencies. As of May 1, 1985, the Border Enforcement System included computerized records on over 2 million persons.

Nonimmigrarft /formation System (N//S), —Contains over 32 million records on foreign visitors, diplomats, and students for purposes of tracking their movements, The system has been operational since January 1983, The student/schools subsystem became operational in August 1984 and tracks 500,000 students at 15,000 schools,

Anti-Smuggling Inforrnation System (AS/S). —Incorporates 750,000 records containing information relating to alien smugglers, including names (and aliases), addresses, phone numbers, and license plates.

National Automated Immigration Lookout System (NAILS).— Provides on-line information for the detection of inadmissible persons and others of particular interest to INS and other law enforcement agencies. Presently contains 40,000 records.

State Data Exchange (SDX—Social Security Administration [SSA]).–Contains 7.5 million records with title XVI information extracted from the supplemental security record, as well as Medicaid eligibility data for specified States. SDX has been in operation since December 1973 and is accessible by State Welfare/Human Resources Departments for use in adminitration of income maintenance and Medicaid programs.

Beneficiary and Earnings Data Exchange (BENDEX–SSA), – Contains *64* million records with information on title II eligibility, Medicare entitlement, wage data, and eligibility entitlement to other SSA-administered programs. BENDEX has been in operation since 1968 and is accessible by State Welfare/Human Resources Departments for use In administration of income maintenance programs.

Third Party Query (TPQY—SSA). —Contains the 7.5 million SDX records and the 64 million BENDEX records. TPQY has been in operation since November 1984 and is accessible for purposes of speeding up the SSA-administered benefit verification process by all State, local, and Federal agencies that administer a health and/or income maintenance program (including commercial vendors).

Enumeration Search Verification and Response System (ESVARS—SSA). –Contains identification data for every social security number that has been issued. There are 280 million base records, which are expanded to 420 million iterations because of name changes, duplicate cards, and such, ESVARS has been in operation since Apr. 1, 1985 and is accessible by all SSA employees who need to verify social security numbers and Federal, State, local, and private agencies that justify their need to verify social security numbers.

[a]For further discussion see app A at the end of this report Also see US Congress Office of Technology Assessment, *An Assessment of Alternatives for a National Computerized Criminal History* System OTA CIT-161 (Springfield VA National Technical Information Service October 1982)

SOURCE Office of Technology Assessment

created in 1986 using information from the databases of a number of agencies. The Debtor Master File was authorized in the Deficit Reduction Act. The purpose of the Debtor Master File is to aid in administering the offset of tax refunds to collect on delinquent Federal debts, such as student loans.[5] The 1986 Debtor Master File contains the names of 750,000 individuals who are indebted to at least one of the following agencies: the Departments of Education, Housing and Urban Development, or Agriculture; the Veterans Administration; and the Small Business Administration. Preoffset notices were sent to these individuals and resulted in payments from 41,000 persons totaling $14 million.[6]

As the exchange of information becomes faster and easier, there will be pressure to increase computer connections and on-line processing. The Deficit Reduction Act and the establishment of Income Eligibility Verification Systems (IEVS) is a good example (see app. E of this report). Under the rules issued by the De-

[5]U.S. Department of the Treasury, Internal Revenue Service, "Privacy Act of 1974: System of Records," *Federal Register*, vol. 50, No. 195, Oct. 8, 1985, p. 41085.

[6]See David Bumham, "I.R.S. To Withhold Tax Refunds Owed Loan Defaulters," *New York Times,* Jan. 10, 1986, pp. Al, Al 1; Keith B. Richburg, "Agencies Give Defaulters' Names to IRS," *Washington Post,* Jan. 10, 1986, p. A21; and Judith A. Sullivan, "IRS To Collect Agencies' Debts," *Government Computer News,* Sept. 13, 1985, pp. 1, 16.

partments of Labor, Agriculture, and Health and Human Services,[7] IEVS would contain wage and benefit data from State Wage Information Collection Agencies; wage, benefit, and other income data from SSA; and unearned income data from the Internal Revenue Service (IRS). The Deficit Reduction Act requires each State to establish an Income Eligibility Verification System. The rules do not interpret this as mandating a physical system, but a logical process that would assure timely and efficient exchange of data. Compatibility to allow exchanges of data among various IEVS is a possibility. The Deficit Reduction Act also requires each State to collect quarterly wage reports from all employers and to establish a State Wage Information Collection Agency that will maintain records of social security numbers; full name; quarterly wages; and employer's name, address, and identifier. As of 1982, 12 States did not collect wage information on a quarterly basis.[8]

The result of IEVS will be uniformity among State systems. The Department of Agriculture has agreed that State Wage Information Collection Agencies should collect the following information: social security number; full name; quarterly wages; and employer's name, address, and identifier. Additionally, the need to follow specific guidelines in accessing IRS-and SSA information will also create more uniform systems throughout the States, and is tantamount to the establishment of a de *facto* wage and eligibility recipient system. In the congressional debates on the Deficit Reduction Act there was no explicit discussion of such a system.

[7]Departments of Labor, Agriculture, and Health and Human Services, "Income & Eligibility Verification Procedures for Food Stamps, Aid to Families With Dependent Children, State Administered Adult Assistance, Medicaid and Unemployment Compensation Programs: Final Rule, " *Federal Register,* vol. 51, No. 40, Feb. 28, 1986, pp. 7178-7217.

[8]U.S. Congress, Hearings Before the Senate Committee on Governmental Affairs, Subcommittee on Oversight of Government Management, *Oversight of Computer Matching To Detect Fraud and Mismanagement in Government Programs,* Dec. 15-16, 1982 (Washington, DC: U.S. Government Printing Office, 1982), p. 14.

Finding 2

There is no comprehensive information on the use of front-end verification by Federal agencies, although the Federal Government is increasingly requiring front-end verification in many federally funded programs administered by the States. Recently enacted legislation will expand the use of front-end verification at the Federal as well as the State level.

Because the personal information provided by applicants for government programs is often inaccurate or incomplete, front-end verification is useful for checking eligibility for Federal benefit programs, checking on current debts and earnings for loan applicants, and checking financial and criminal histories for employment applicants.

The existence of the numerous computerized databases discussed above would seem to indicate that many agencies use front-end verification. However, only two agencies–the Bureau of Indian Affairs in the Department of the Interior and the Veterans Administration—responded affirmatively to the OTA survey's question on front-end verification. In part, the small number of affirmative responses to the question may be attributed to a lack of understanding of what would be termed "front-end verification. "

Until recently, there was almost no information on State use of front-end verification. However, the Department of Health and Human Services has recently completed a survey of automated front-end eligibility y verification applications currently used or being developed at the State level for use in AFDC, food stamp, Medicaid, and unemployment insurance programs. With a 92 percent response rate from the States, the survey found 75 front-end verification applications being used in AFDC, food stamp, and Medicaid programs in 36 States, and 53 front-end verification applications being used in unemployment insurance programs

in 36 States.[9] The primary data checked in these front-end verifications include duplicate benefits, earned income, and work history. Examples of some front-end verification programs appear in table 14.

There has been a marked increase in State use of front-end verification in Federal welfare programs. Federal statutes, most notably the Deficit Reduction Act, now require front-end verification in certain programs. The Deficit Reduction Act requires States to use front-end verification in administering the food stamp, AFDC, unemployment compensation, Medicaid, and SSA'S adult assistance programs (titles I, X, XIV, XVI). The sources that will be used most frequently for verifying information are: the agency's own data sources, as a check on duplicate benefits; SSA'S State Data Exchange System (SDX), which contains a listing of all supplemental security income recipients in the State; the SSA'S Beneficiary and Earnings Data Exchange (BENDEX), which contains wage data and eligibility entitlements to SSA programs; SSA'S Enumeration Verification System (EVS), which contains information on social security numbers; IRS files for earned and unearned income; INS files for immigration status; and State wage data systems (see fig. 7).

Under the rules developed by the Departments of Labor, Agriculture, and Health and Human Services, States are required to develop a statewide IEVS, and to use SSA and IRS systems for verifying additional information. Examples of front-end verification required under the Deficit Reduction Act include verification of: social security numbers through BENDEX, SDX, or EVS; unearned income through IRS with subsequent verification from the individual or source of unearned income; and income/wages through IEVS.[10]

[9] U.S. Department of Health and Human Services. *Catalog of Automated Front-End Eligibility Verification Techniques,* op. cit.

[10] See app. E of this report.

Table 14.— Examples of State Front-End Verification Programs

Nevada. —The Welfare Referral System under development will provide the caseworker with information about the applicant's receipt of income assistance benefits, wages, and unemployment compensation benefits (UC B). When an applicant comes into the local office, the worker will enter the applicant's name, social security number, and other data into the "key file. " This information will be matched on-line against welfare and wage and UCB data (welfare refers to Aid to Families With Dependent Children (A FDC), food stamps, Medicaid, child support, and social services). A hardcopy of the match WIII be generated and transmitted to the worker.

Georgia.—At the time of application, the eligibility worker does an on-line check of the current recipient database to detect any duplicate benefits. In addition, this match is also run during the batch processing of the application that occurs immediately prior to payment. Results are received prior to eligibility certification. This batch match also accesses statewide records of closed benefit cases. The duplicate benefit check is part of Georgia's larger Public Assistance Reporting System (PARIS) designed to collect, store, and generate information utilized by the AFDC. food stamp, and Medicaid programs.

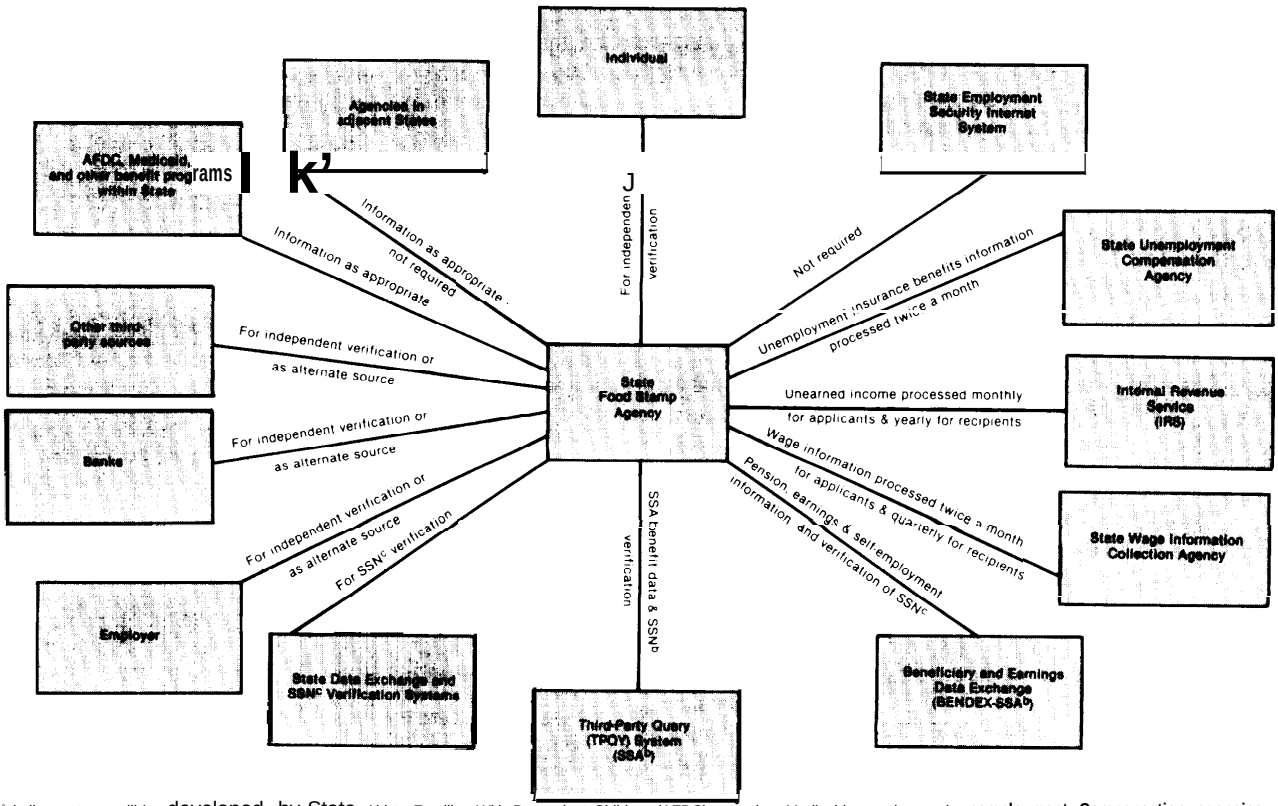
New York.—As a new subsystem of the Welfare Management System, the Resource File Integration automatically provides front-end matching of all applicants for public assistance against the State wage file. The wage data is available on-line to eligibility workers. To assure that local workers take action on the information, a resolution code indicating the action is required before any further processing can take place. Future plans call for adding State UCB data to the resource file. This system is used statewide except in New York City, which has a slightly different system providing the same information by overnight batch processing.

Florida. —Information on individuals who are known to have been involved in labor disputes and who have committed benefit fraud is stored in the claim history file When an individual applies for unemployment compensation benefits, employees automatically perform an on-line match between this data and applicant data when they enter data from a new application. Positive hits generate flags that prevent any payments from being made until the issue is resolved.

SOURCE U S Department *of* Health a-rid Human Services, Office of Inspector General, Catalog of *Automated Front-End Eligibility* Verification Techniques, OAI-85-H-51 September 1985

The Debt Collection Act requires applicants for Federal loans to supply their taxpayer identification number (for individuals, their social security numbers), and requires agencies to screen credit applicants against IRS files to check for tax delinquency. Circular A-70 of the Office of Management and Budget (OMB)

Figure 7.—A Representative Income and Eligibility Verification System (IEVS) for a State Food Stamp Agency as Required by the Deficit Reduction Act of 1984[a]



[a]similar systems will be developed by State Aid to Families With Dependent Children (AFDC) agencies, Medicaid agencies, and unemployment Compensation agencies. as well as for the Adult Assistance Program in the Territories,
[b]Social Security Administration.
[c]Social securit, number.

SOURCE: Office of Technology Assessment.

mandates that Federal agencies must conduct a credit screen on a potential candidate before issuing a contract, grant, loan, or loan guarantee.

With debt collection and with credit screening, the Federal Government is relying on private sector databases for verifying the information. As presently planned, five companies, including TRW Information Services, will develop databanks on individuals' credit and debt information from private and governmental sources, and two companies, TRW and Dun & Bradstreet, will do likewise for commercial firms.11 Dun & Bradstreet's Director of Corporate Government Services was quoted as saying:

> Private lenders, banks, etc., who are Dun & Bradstreet subscribers can get this data, too. So, if you don't pay the Feds, from now on it'll affect your commercial credit rating, too.[12]

There has also been an increased effort to require criminal history record checks for job applicants in sensitive categories, e.g., day-care providers for children. Congress included a pro vision in the Continuing Appropriation Act of 1985 (Public Law 98-473) requiring that States establish procedures to provide for nationwide criminal history checks for all operators and

[11]"Front-End Credit Screening: How an Ounce of Prevention Could Avoid Billions in Cure," *Government Executive,* January 1985, pp. 34-35.

[12]*Ibid, p, 35.

employees of child-care facilities.[13] States were to have such procedures in place by September 30, 1985. '4 According to the Office of the Inspector General, U.S. Department of Health and Human Services, as of November 1984, 3 States (California Georgia Minnesota) had statutes requiring FBI criminal record checks on day-care providers, 24 States conducted statewide criminal record checks on day-care providers, and 20 States were anticipating new legislation authorizing such criminal record checks.[15] There has also been growing interest in implementing criminal record checks for teachers, youth group leaders, and elder-care providers. 'G

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

Additionally, Section 6103(1) allows for the disclosure of return information for purposes other than tax administration. The list has grown considerably since 1976, and includes disclosures to: SSA and the Railroad Retirement Board (Public Law 94-455, 1976); Federal loan agencies regarding tax delinquent accounts (Public Law 97-365, 1982); the Department of Treasury for use in personnel or claimant representative matters (Public Law 98-369, 1984); Federal, State, and local child support enforcement agencies (Public Law 94-455, 1976); and Federal, State, and local agencies ad-ministering certain programs under the Social Security Act or Food Stamp Act of 1977 (Public Law 98-369, 1984). Section 2651 of the Deficit Reduction Act also amends Section 6103(1) of the Tax Reform Act and allows return information from W-2S and unearned income reported on 1099s to be divulged 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. Section 6103(m) of the Tax Reform Act also provides for disclosure of taxpayer identity information to a number of agencies, including the National Institute for Occupational Safety and Health and the Secretary of Education.

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

The potential for expanding the use of front-end verification for government programs, loans, and employment is enormous, as evidenced by the Reagan Administration's proposed Payment Integrity Act that would require front-end verification in 12 new programs, including Pen Grants, guaranteed student loans, school lunches, health education loans, veterans' programs, Department of Housing and Urban Development housing programs, and railroad retirement. Additionally, the Administration would expand the types of data

[13] U.S. Department of Health and Human Services, *Model Child Care Standards Act- Guidance to States To Prevent Child Abuse in Day Care Facilities*, Washington, DC, January 1985, p. 2.
[14] 1 bid., p. 3.
[15] 1 bid., p. 27.
[16] See, for example, Adrian Higgins, "Day Care Worker Checks Getting Mixed Reviews, *Arlington Journal*, Sept. 6, 1985, p. A7; Linda Lantor, "Fairfax Schools To Tighten Employee Screening, " *Arlington Journal*, Sept. 10, 1985; p. A4; and Andee Hochman, "Youth Workers Face Additional Screening; Change Follows Spate of Sex Abuse Cases, *The Washington Post*, Sept. 23, 1985, pp. D1-D2.

available for verification beyond those specified in the Deficit Reduction Act to include alien status, government wages and pensions, veterans' benefits, and railroad retirement.

Another section of the proposed Payment Integrity Act would set up a Health Insurance Verification System that would enable federally funded health care programs to access third-party insurance files to verify information supplied by the person applying for insurance payments. The Federal programs include Medicaid, Medicare, Veterans, Indian Health, Black Lung, and Maternal and Child Health. The third-party insurance files to be accessed include private insurance companies, health maintenance organizations, self-insured employer-based plans, State and local employee health plans, Federal health insurance programs, and Federal and State workers' compensation.

There are presently a number of front-end verification pilot projects being conducted at the Federal level or at the State level with Federal funds. One is the Systematic Alien Verification for Entitlements (SAVE) system operated by the Immigration and Naturalization Service. State welfare agencies can access SAVE to determine if an applicant is a legal alien. Such information was previously verified by sending individual forms to INS. SAVE in this way saves time for the applicant, although State laws generally require welfare agencies to act on an application within 10 days. However, INS also regards it as a "policing tool, as indicated by this statement in an INS memo about SAVE:

> Success will be measured by the number of criminal prosecutions resulting from these efforts; the dollars of cost avoidance; and the number of unentitled aliens identified and removed or barred from benefit rolls .17

Another pilot project is Project Checkmate in the District of Columbia. In this project, AFDC applicants are screened against credit bureau records providing information on income, resources, bank accounts, credit balances, and employment.[18]

Finding 3

Front-end verification raises due process and privacy issues that have not been systematically studied.

Under traditional due process principles, it is arguable that individuals should be notified that information they provide will be verified by third-party sources.[19] In many of the front-end verification programs currently being used, individuals are not informed or are only informed indirectly, i.e., they are told that information may be verified, but not when or how. They are often left with the impression that they will be responsible for bringing proof to verify information, not that the agency will verify information from other sources (see box B).

The Deficit Reduction Act and the Debt Collection Act include requirements that agencies give some notice to individuals. The Deficit Reduction Act requires agencies to notify applicants at the time of application and periodically thereafter that information about them will be exchanged and used to verify income and eligibility. Under the proposed rules, it is not clear how this will be done ("in writing at application, but not necessarily on the application form' or how specific will be the information that is provided to the individual.

"As quoted in American Civil Liberties Union, "computer Matching-Focus Paper, " September 1985, p. 5.

[18]U.S. Department of Health and Human Services, *Catalog of Automated Front-End Eligibility Verification Techniques,* op. cit., p. 44.

[19]"Procedural due process traditionally means that an official government action must meet certain standards of fairness to an individual. This generally includes the rights of adequate notice and of a meaningful opportunity to be heard prior to a decision. In deterrnining the level of procedural due process that is appropriate, three issues are considered: 1) is there a threat to life, liberty, or property interests; 2) what are the interests of the government and of the individual; and 3) what procedures are cost-justified. See Kenneth C. Davis, *Administrative* Law *Treatise,* 2d ed. (San Diego, CA: K.C. Davis Publishing, 1979); Kenneth C. Davis, *Discretionary Justice: A Preliminary Inquiry* (Urbana: University of Illinois Press, 1969); and Ernest Gellhorn and Barry B. Boyer, *Administrative Law and Process* (St. Paul, MN: West Publishing, 1981).

Box B.—Example of Front-End Verification Notice

Penalty Warning

THE INFORMATION PROVIDED ON THIS FORM WILL BE SUBJECT TO VERIFICATION BY FEDERAL, STATE AND LOCAL OFFICIALS. IF ANY IS FOUND INACCURATE, YOU MAY BE DENIED FOOD STAMPS AND/OR BE SUBJECT TO CRIMINAL PROSECUTION FOR KNOWINGLY PROVIDING FALSE INFORMATION.

ANY MEMBER OF YOUR HOUSEHOLD WHO INTENTIONALLY BREAKS ANY OF THE FOLLOWING RULES CAN BE BARRED FROM THE FOOD STAMP PROGRAM FOR 6 MONTHS AFTER THE FIRST VIOLATION, 12 MONTHS AFTER THE SECOND VIOLATION, AND PERMANENTLY FOR THE THIRD VIOLATION. THE INDIVIDUAL CAN ALSO BE FINED UP TO $10,000, IMPRISONED UP TO 5 YEARS, OR BOTH. A COURT CAN ALSO BAR AN INDIVIDUAL FOR AN ADDITIONAL 18 MONTHS FROM THE FOOD STAMP PROGRAM. THE INDIVIDUAL MAY ALSO BE SUBJECT TO FURTHER PROSECUTION UNDER OTHER APPLICABLE FEDERAL LAWS.

DO NOT give false information, or hide information, to get or continue to get food stamps.

DO NOT trade or sell food stamps or authorization cards.

DO NOT alter authorization cards to get food stamps you're not entitled to receive.

DO NOT use food stamps to buy ineligible items, such as alcoholic drinks and tobacco.

DO NOT use someone else's food stamps or authorization cards for your household.

Your Signature

I understand the questions on this application and the penalty for hiding or giving false information or breaking any of the rules listed in the Penalty Warning. My answers are correct and complete to the best of my knowledge.

I understand that I my have to provide documents to prove what I've said. I agree to do this. If documents are not available, I agree to give the Food Stamp office the name of a person or organization they may contact to obtain the necessary proof.

Your signature

Today's date

Witness if you signed with an X

You or your representative may request a fair hearing either orally or in writing if you disagree with any action taken on your case. Your case may be presented at the hearing by any person you choose.

We will consider this application without regard to race, color, sex, age, handicap, religion, national origin or political belief.

FORM FNS-385 (7-83) *Previous Editions Obsolete*

Page 5

From prototype of food stamp application approved by the Office of Management and Budget. Actual forms vary by State.

In 1983, OMB issued its Guidelines *on the Relationship of the Debt Collection Act of 1982 to the Privacy Act of 1974.*[20] The guidelines specify that before an agency discloses information to a consumer reporting agency, the agency head or designee must review and validate the disclosure, must have given notice to the debtor of the overdue debt and its intention to disclose, must have given the individual time to file for review, and must have published

[20] Apr. 11, 1983 (effective Mar. 30, 1982) (43 FR 15556).

a notice in the *Federal Register* identifying those systems of records from which they intend to disclose. Disclosure should be limited to that information directly related to the identity of the debtor and the history of the claim. Although under the act the consumer reporting agencies receiving records are exempt from criminal liability for misuse of information, the guidelines indicate that it would be appropriate to incorporate assurances to this effect in service contracts between Federal and consumer reporting agencies. The guidelines also clarify that nothing in the wording of the Debt Collection Act authorizes agencies to share information among themselves or to use information obtained under this act for any other purpose.

In general, it can be a simple process to notify applicants that information they provide will be verified before benefits are granted and which databases will be searched for verification of which data elements. Some even envision verification being completed while the individual waits. However, there is some question whether notice is useful for the individual under these circumstances. The purpose of notice is to give the individual information so he or she can act.[21] In the case of front-end verification, notice generally leaves the individual only one recourse if he or she does not want the information verified, and that is to withdraw the application.

The exchanges of personal information necessitated by front-end verification may conflict with the Privacy Act principles that information should be collected directly from the individual and that information collected for one purpose should not be used for another purpose without the consent of the individual. Although in front-end verification information may originally be collected directly from the individual, additional information is provided from outside sources. Moreover, the information being used to verify information provided by the individual is being used for a purpose other than that for which it was originally collected.

[21] Davis, op. cit., 1979.

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

An additional due process question that is raised by verifying information from governmental or private sector (e.g., TRW or Dun & Bradstreet) databanks is: what recourse does the individual have if the information is false? Specifically, can the individual sue the databank owner or operator? The Privacy Act provides means by which individuals can take action against a Federal agency. The Fair Credit Reporting Act may provide a vehicle by which an individual could take action against a credit reporting agency. However, in other circumstances, statutes may not provide a legal means by which individuals can challenge false information and individuals would need to rely on common law defamation suits.

Finding 4

There has been no comprehensive study of how to conduct front-end verification in the most cost-effective manner and with the highest possible data quality.

The high costs of computer matching (e.g., verifying large numbers of hits, holding hearings, and prosecuting wrongdoers) are not incurred in front-end verification. However, front-end verification has its own costs. It may add to the caseworker's time in processing an application, although it may save somewhat in subsequent administrative time. Front-end verification will increase budgets devoted to automated data processing and telecommunications. There are also some high initial overhead costs in terms of developing the databases used for verification (e.g., State Income

Verification Eligibility Systems) and getting them on-line, and ongoing costs of keeping them up to date.

The Department of Health and Human Services' survey of front-end eligibility verification techniques at the State level asked respondents about both developmental and operating costs. Most States were not able to provide the information as they were not keeping track of the administrative time devoted to verification. [22]

The major savings associated with front-end verification result from the avoidance of payments. The General Accounting Office reported that a New York State program that matched welfare applications with tax records to verify income avoided paying over $27.5 million, and that front-end verification in AFDC and food stamp programs in Arkansas saved $5 to $8 million.[23] In neither case was a detailed cost-benefit analysis available.

Another projected saving is a reduction in efforts to detect fraud, waste, and abuse for those already enrolled in government programs, as these individuals would have been initially screened by front-end verification. However, front-end verification would not eliminate the need to use other techniques (e.g., computer matching) because even when information is verified initially, frequent status changes (e.g., address and income) may necessitate later verification.

The President's Council on Integrity and Efficiency has projected that the eligibility verification required by the Deficit Reduction Act will save $1 billion over 5 years. The Congressional Budget Office did a gross estimate that confirmed this figure, but did not specify categories or figures for costs and savings.[24]

The costs of front-end verification are directly tied to data quality. The timeliness of data used is an especially critical issue; for example, wage data are often between 3 and 6 months out of date by the time they are available from State wage reporting agencies. Unearned income from the IRS is not reported until a month after the end of the tax year and would not be processed and available for verification purposes until many months later. Other income data can likewise be stale. Some front-end verification systems, such as those required in the Deficit Reduction Act, require workers to manually check information that appears false. However, the costs associated with front-end verification will increase with each subsequent verification.

Finding 5

At the present time, there are no policy guidelines for use of computer-assisted front-end verification.

There are no general Federal guidelines, statutory or administrative, guiding the use of front-end verification. The OMB computer matching guidelines specifically exclude from their purview record searches that are conducted at the application stage. The Deficit Reduction Act due process requirements for notice, verification, and hearings may provide a model for more general guidelines. In designing policy guidelines, the following factors warrant consideration:

1. *The responsibility for determining access to and record quality of the databases used for verification purposes.*

It is noteworthy that the FBI has taken the position that it has a responsibility only for the quality of the Triple I index entries, and not for the State criminal history records on which the index entries are largely based. Likewise, NHTSA officials have stated that the quality of driver's license records maintained by the States (and indexed in the NDR) is not the responsibility of NHTSA.

When records are maintained in a central Federal records repository, access and dissem-

[22] Interview with Liz Handley, Project Director, Department of Health and Human Services Front-End Eligibility Project, Apr. 9, 1985.

[23] U.S. General Accounting Office, *Eligibility Verification and Privacy in Federal Benefits Programs: A Delicate Balance,* HRD-85-22, Mar. 1, 1985.

[24] U.S. Department of Health and Human Services, Office of the Inspector General, Semiannual *Report to the Congress,* Apr. 1, 1985 -Sept. 30, 1985.

ination generally follow applicable Federal laws and regulations. However, under a decentralized index approach, record access and dissemination are much more complicated. There are wide differences in State laws and regulations on record access and dissemination, ranging all the way from so-called "open record" States such as Florida, where many personal records maintained in State files are open to public access at a modest fee, to very restrictive States like Massachusetts, where access and dissemination are tightly controlled.

This wide disparity in approach is especially true with respect to criminal history records, but also affects many other kinds of personal records maintained in State repositories. This contributes to inconsistent and incomplete exchange of record information. In some of the Federal social service and welfare programs, Congress has addressed this problem by requiring States to collect and exchange information as a condition of Federal funding, as discussed earlier. But in other areas such as criminal history records, while Congress previously has taken action to encourage enactment of State laws, there are wide differences among the many State laws that have been enacted.

2. *The frequency of use of front-end verification, i.e., routine or selective.*

If it is conducted routinely (e.g., for all benefit programs and Federal employment, loans, and contracts), the societal implications of subjecting to scrutiny all information submitted to the government by individuals would need to be considered. Any possible long-term societal effects, such as increased distrust between citizens and government, loss of individual responsibility, and a sophisticated governmental information infrastructure would need to be weighed against the significant budgetary savings that may be achieved by routine verification.

If front-end verification is used selectively (e.g., by law, OMB regulations, or court decisions) rather than routinely, then consideration must be given to the criteria for selecting Federal programs that may use it, the approval process for each use, and the societal groups that will be most affected. Another alternative for doing selective verification would be to select particular individuals rather than particular programs. The individuals selected for front-end verification could be chosen by a computer profile. However, profiling raises additional policy issues, as will be discussed in chapter 5.

3. *The rights of individuals.*

Based on due process principles, as well as traditional information privacy principles, individuals should be given some notice of verification and some means to challenge information if discrepancies should appear as a result of verification. There are a number of ways in which compliance with these principles could be achieved. Individuals could be informed in writing or verbally at the time they submit an application that the information supplied will be verified. Additionally, they could be given a range of details concerning the sources to be accessed in the process. Individuals wanting more details on the process or wishing to contest verification could be advised by the caseworker whom they should consult within the agency and when.

If front-end verification reveals problems with the information provided by the individual, then a process of further checking the validity of information and informing the individual of the problems could be started. The degree of individual involvement and the depth of validation may vary based on agency directives or the goodwill of caseworkers, and therefore may need to be specified in the regulations.

Once these principles are recognized in procedural protections, there may also be a need to ensure that agencies are providing the requisite notices and hearings. Some method of enforcement or automatic accounting could also be specified in the regulations. Such oversight could be conducted within the agency or by some outside body.

With respect to involving the individual in the verification of information, the Department of Education is conducting an experimental

program, the Pen Grant Electronic Pilot. [25] Under this project, Pen Grant applicants can correct or verify information on their Student Aid Reports through computer facilities at institutions or financial aid services that participate in the project. Applicants can now make corrections on their Student Aid Reports and mail them back to the Department of Education.

4. *The types of information used.*

This question involves whether the use of some types of information (e.g., medical history or criminal history) should be prohibited because of their sensitivity. The use of such information could be prohibited, or its use could be restricted to particular verifications, for example, use of criminal history information in screening day-care workers.

Additionally, front-end verification raises a separate and potentially more serious issue because the information is being used to make an immediate, or near immediate, decision. In order for front-end verification to be most effective, information should be up to date, accurate, and complete. However, the information in some categories, for example, unearned income and checking accounts, may change so often that the data contained in computerized databanks will rarely be up to date. Additionally, the record quality of many existing databanks that could be used in front-end verification (e.g., computerized criminal history records) is questionable.

5. *The possible requirement of a cost-benefit analysis.*

Because a major purpose of front-end verification is to cut programmatic costs, documentation of how front-end verification will achieve this may be necessary. If a cost-benefit analysis were to be required, the categories of costs and benefits to be included could be specified in regulations. The detail to which costs and benefits should be analyzed could also be specified. The degree of detail may vary depending on the category; for example, administrative costs may be more difficult to compute than telecommunication costs.

Cost-benefit analyses could be used within an agency or program for internal improvements in ongoing front-end verifications. They could also be distributed among agencies or programs for development of new front-end verifications. Additionally, they could be used within an agency or by an outside body as part of a process of approval of new front-end verifications or review of ongoing ones.

[25] U.S. Department of Education, office of Postsecondary Education, "Invitation To Participate and Closing Date for Participation in Pen Grant Electronic Pilot, *Federal Register,* vol. 50, No. 141, Tues., July 23, 1985.