United States General Accounting Office

GAO

Report to the Committee on Governmental Affairs, U.S. Senate

October 2000

THE CHALLENGE OF DATA SHARING

Results of a GAO-Sponsored Symposium on Benefit and Loan Programs

GAO

Accountability * Integrity * Reliability

GAO-01-67

Contents

Abbreviations

DMDC	Defense Manpower Data Center
DOD	Department of Defense
GSA	General Services Administration
IRS	Internal Revenue Service
NDNH	National Directory of New Hires
OASDI	Old-Age, Survivors, and Disability Insurance
OCSE	Office of Child Support Enforcement
OMB	Office of Management and Budget
PARIS	Public Assistance Report Information System
PKI	public key infrastructure
SSA	Social Security Administration
SSI	Supplemental Security Income
TANF	Temporary Assistance for Needy Families
UI	unemployment insurance

GAO
Accountability * Integrity * Reliability

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

October 20, 2000

The Honorable Fred Thompson
Chairman
The Honorable Joseph I. Lieberman
Ranking Minority Member
Committee on Governmental Affairs
United States Senate

Many federal benefit and loan programs have common data needs, such as the need for accurate information on the income and assets of applicants and recipients. Such information can be subject to error or abuse when applicants and recipients are the sole source of it. Past work has shown, for example, that some individuals misrepresent their financial condition by under- or overstating their income and assets when applying for programs or during subsequent determinations of eligibility. [1] As a result, agencies can make payments or loan funds to individuals who are not entitled to them, or over- or underpay individuals who are entitled. These inaccuracies can be expensive—costing the government billions of dollars each year.

Data sharing across government agencies has been an important and successful tool for identifying improper payments. The Social Security Administration (SSA), for example, identifies improper payments to Supplemental Security Income (SSI) recipients in part by obtaining wage data from state agencies to verify self-reported earnings. Similarly, some state human services departments use data from various federal and state agencies to verify the income and assets of their applicants and recipients.

Because improper payments are a continuing problem among benefit and loan programs, you asked us to review whether expanded and improved data sharing among these programs could contribute to more accurate initial and continuing eligibility decisions. In response, we conducted two projects. The first was a study that focused primarily on the data-sharing

[1]Such work has been done by both GAO and agency inspectors general. For example, see *Financial Management: Increased Attention Needed to Prevent Billions in Improper Payments* (GAO/AIMD-00-10, Oct. 29, 1999) and *U.S. Department of Housing and Urban Development: Attempt to Audit the Fiscal Year 1999 Financial Statements*, HUD Inspector General (00-FO-177-0003).

efforts of three programs as case examples.[2] The second project, designed to provide a broader, governmentwide perspective, involved presenting a 2-day symposium on data sharing among benefit and loan programs.

This report discusses the results of the symposium held June seventh and eighth, 2000, in Washington, D.C. The symposium focused on (1) how data sharing has improved the payment controls of benefit and loan programs, (2) how technologies are expanding data-sharing opportunities, (3) why privacy is a concern in a data-sharing environment, and (4) how data sharing can be advanced among benefit and loan programs governmentwide. Audience participants included representatives of federal, state, and local benefit and loan programs and oversight agencies; congressional staff; members of federal and state government boards focusing on data sharing; and individuals from the private sector interested in public/private data sharing or concerned about privacy and security issues.

Summary of Proceedings

Sally Katzen, then Counselor to the Director of the Office of Management and Budget (OMB) and now OMB's Deputy Director for Management, kicked off the symposium by highlighting the importance of data sharing in achieving one of the priority management objectives in the 2001 budget: verifying that the right person is getting the right benefit at the right time. Other symposium speakers highlighted the number of program dollars saved through detecting improper benefit and loan payments. For example, Pete Monaghan, an SSA official responsible for data exchanges, estimated that SSA saves a total of $675 million annually in its retirement, disability, and SSI programs by matching its recipient rolls against data from other agencies. These matches detect such things as undisclosed income and assets, which can either reduce the benefit payments of some recipients or make them ineligible for benefits altogether. Welfare agencies participating in multistate matches to identify recipients who receive benefits in more than one state also report significant savings. Elliot Markovitz from Pennsylvania's Department of Public Welfare's Bureau of Program

[2]See *Benefit and Loan Programs: Improved Data Sharing Could Enhance Program Integrity* (GAO/HEHS-00-119, Sept. 13, 2000). This report focused on public housing programs administered by local agencies with the help of the Department of Housing and Urban Development, student financial assistance programs administered by the Department of Education, and Temporary Assistance for Needy Families programs administered by the states.

Evaluation estimated, for example, that Pennsylvania saves $2.8 million each year that it participates in such matches. Finally, child support payments have increased substantially because of two legally mandated data-sharing projects that identify the earnings, financial accounts, and addresses of individuals who are obligated to make child support payments. For example, Donna Bonar, Acting Associate Commissioner at the Office of Child Support Enforcement (OCSE), reported that child support collections in Virginia increased an estimated $13 million in 1 year as a result of using a national database that contains quarterly wage and other information on U.S. workers.

Symposium speakers discussed technologies that are expanding data-sharing opportunities and offering new possibilities for securing information, including technology that makes direct communication among computer systems possible. These endeavors consist of requesting and receiving information from different computer systems over the Internet or other network, with software translating the information into formats that each computer and end user can understand. In one presentation, an official responsible for SSA payment and recovery policy and a government liaison with NACHA—The Electronic Payments Association described how a network could be created so that benefit and loan programs could obtain financial account information on program applicants and recipients electronically from financial institutions. In another talk, William Boggess, an official responsible for computer systems at the Defense Manpower Data Center (DMDC), described how the internal network of computers that the Department of Defense (DOD) uses to deliver military benefits to personnel could be a model for creating a nationwide network of public assistance databases that could be accessed and shared by various programs. In a third talk, David Temoshok, responsible for developing applications to enhance government electronic services at the General Services Administration (GSA), described how the Internet is being used to facilitate sharing information among federal, state, and private-sector entities with common program missions and data needs, such as student financial aid programs. All three of these applications offer numerous advantages to the government and the public, including the ability to verify program participant information and thereby detect improper payments sooner, or perhaps even prevent them altogether. Integral to these discussions was how access to, and use of, shared information could be appropriately limited to authorized personnel for official reasons. David Mintie, an automated systems manager with the Connecticut Department of Social Services, discussed another technological advancement: biometric identification systems. These

automated systems scan parts of the human body and, through a comparison with a previous scan, verify a person's identity. Biometrics is being used by human services departments to scan the fingerprints of welfare participants to prevent individuals from receiving multiple benefits for the same time period. These departments are also beginning to develop standard formats to facilitate sharing fingerprint files among states to detect and deter the receipt of duplicate benefits.

Perhaps the single most important concern about sharing personal information among government programs is whether it can be done without sacrificing an individual's right to privacy. Although all the symposium speakers and audience participants who discussed privacy issues agreed that it is important to protect this right, they disagreed about the extent to which data sharing threatens it. Some believed, for example, that data sharing is a risk to personal privacy for two reasons:

- it increases the chances that personal information will be wrongfully disclosed and perhaps misused and
- it can hinder the public's ability to monitor what the government is doing with personal information that its citizens provide to specific agencies for specific reasons.

Other symposium speakers and audience participants believed that the right to privacy has been, and will continue to be, protected by security technologies, the nation's privacy laws, and congressional oversight and legislative authority over data sharing. Opinions also varied about the extent to which the nation's privacy laws should be changed. Privacy advocates believed that society needs to revisit fundamental concepts regarding what information should be shared and with whom. For example, a key concern was the extent to which personal financial information that individuals provide to a government agency should be allowed to be shared with other agencies. The revisions that others mentioned were more limited, such as lengthening the time periods that computer-matching agreements can remain in effect.

Another topic addressed during the symposium was how data sharing could be advanced among benefit and loan agencies. Central to these discussions was the idea that any enhancements to data sharing should be weighed against the need to protect personal privacy. Those who talked about such enhancements advocated that they include the necessary technological and legal protections to safeguard personal privacy. Some of the discussions focused on methods for facilitating data sharing

nationwide, such as forming a governmentwide group to discuss, manage, and fund data-sharing projects and creating incentives for agencies to take on more projects. Other suggestions focused on specific data-sharing initiatives, such as increasing access to OCSE's database of information on U.S. workers and advocating that agencies obtain information electronically from other government programs and private entities during the application process to prevent improper payments from ever being made. Some of these suggestions, however, may require changes to existing law.

Background

Benefit and loan programs provide cash or in-kind assistance to individuals who meet specified eligibility criteria. Temporary Assistance for Needy Families (TANF), SSI, Food Stamps, housing assistance, and student loans are representative of such programs. Some programs are administered centrally by federal agencies (such as SSI), while others are administered by states and localities (such as TANF). Benefit and loan programs often have difficulty making accurate eligibility and payment amount decisions because applicants and recipients provide much of the information needed to make these decisions, and the programs do not always have effective ways to verify that these individuals are fully disclosing all relevant information.

The symposium, entitled "Data Sharing: Initiatives and Challenges Among Benefit and Loan Programs," was sponsored by GAO and the Chairman and Ranking Minority Member of the Senate Committee on Governmental Affairs. It was an impartial and balanced forum to explore the successes, problems, and possible future directions of data sharing among benefit and loan programs. The symposium consisted of an opening address by Sally Katzen, Deputy Director for Management of OMB, and four panels composed of four to six speakers each. Ms. Katzen's talk highlighted both the importance of data sharing and the need to protect individual privacy in the course of such sharing. Panel speakers then discussed how data sharing has benefited their programs, how technology offers new data-sharing possibilities, the privacy and security concerns that arise in a data-sharing environment, and how data sharing can be advanced among benefit and loan programs governmentwide. Panel speakers, who came from a variety of federal and state benefit and loan programs and the private sector, included officials from SSA, the Department of Labor, OCSE, the Department of the Treasury, and state human services departments, as well as representatives from the financial services industry and privacy

advocates. Appendix I contains the symposium agenda, including the names and complete titles of the speakers.

Many of the symposium speakers and audience participants referred to the National Directory of New Hires (NDNH). The Congress mandated that OCSE create this database as part of welfare reform primarily to aid in collection of interstate child support payments. The NDNH is maintained by OCSE and, to a large extent, is derived from reports that private employers and states are required to file containing information on newly hired employees, quarterly wage information, and quarterly unemployment insurance (UI) information. In addition, this database contains information on newly hired federal employees and quarterly wage information on all federal employees. OCSE matches these data against information it has on parents who are involved in child support cases and forwards the matched results to the state child support offices responsible for collecting the payments. The Social Security Act limits access to the NDNH to specific agencies for specific purposes. For example, Treasury (including the Internal Revenue Service [IRS]) has access to the NDNH to administer federal tax laws and to verify claims for the Earned Income Tax Credit. SSA also has access to help it administer the SSI and Old-Age, Survivors, and Disability Insurance (OASDI) programs. More recently, the Department of Education was granted access for purposes of obtaining the addresses of individuals who have defaulted on student loans or who owe grant repayments to Education.

Data Sharing Has Enhanced the Payment Controls of Programs

Sally Katzen, Deputy Director for Management of OMB, kicked off the data-sharing symposium by highlighting the importance of data sharing in achieving one of the top objectives contained in the administration's 2001 budget proposal: verifying that the right person is getting the right benefit at the right time. This objective is being accomplished in part by data sharing among agencies to identify when improper benefit and loan payments have been made to program recipients. Several symposium participants representing major benefit and other programs reported that shared information is predominantly used in computer matches. That is, an agency compares the information it has on its program recipients against a file from another agency containing similar information to detect discrepancies, such as undisclosed income or assets. Once such discrepancies are detected, the agency investigates to determine if improper payments have been made and, if so, takes action to collect any overpayments and, sometimes, to remove the individual in question from the program. Agencies find such computer matches cost-effective because

computers do most of the work. According to one symposium speaker, Pete Monaghan, an SSA official, the cost-benefit ratios of matches range from $20 to $40 of savings for every $1 spent to perform the match.

Symposium speakers estimated that substantial savings accrue to programs that use computer matches to detect improper payments. According to Mr. Monaghan, SSA saves about $675 million annually by matching its OASDI and SSI program rolls against data from 10 to 12 federal agencies and 4,000 state and local jails to identify ineligible or overpaid individuals. (See table 1.) Mr. Monaghan also explained that SSA provides data that it maintains on U.S. workers and SSA program recipients to 10 to 12 federal agencies and all states and U.S. territories, and that the use of these data results in annual savings of $1.5 billion. Finally, many states have begun to participate in multistate matches, known as Public Assistance Report Information System (PARIS) matches, to identify welfare recipients who receive simultaneous benefits in more than one state. At the time of the symposium, two PARIS matches had been conducted, and 13 states and the District of Columbia had participated in the most recent one. Although comparable match results among participating states do not exist, Elliot Markovitz, from the Pennsylvania Department of Public Welfare, provided indications of the matches' effectiveness by reporting the results for the District of Columbia and selected states, including Pennsylvania. Pennsylvania and the District of Columbia determine results by estimating their annual savings for such public assistance programs as TANF and Food Stamps as a result of removing individuals from their rolls because they were found to be receiving benefits in another state. Pennsylvania estimated its annual savings at $2.8 million and removed 566 individuals from the rolls. These individuals accounted for nearly 16 percent of all cases that Pennsylvania county workers investigated as a result of the two matches. The District of Columbia put its annual savings at about $1 million and the number of individuals removed from the rolls as a result of one match at 382. These individuals accounted for about 18 percent of all PARIS cases investigated by the District of Columbia.

Table 1: Estimated Program Dollars Saved Annually Through Computer Matching

Program type	Dollars saved annually (in millions)
SSA programs	
OASDI	$350
SSI	325
Programs using SSA data[a]	
Federal programs[b]	900
State programs[c]	600
Selected participants in PARIS matches	
Pennsylvania	2.8
District of Columbia	1.0

[a]SSA estimates may be understated because they include only data-sharing initiatives that are subject to the Computer Matching and Privacy Protection Act, but SSA also provides data that result in savings under initiatives that are not covered by the act.

[b]Federal programs include those within the Office of Personnel Management, Railroad Retirement Board, Department of Veterans Affairs, Health Care Financing Administration, and Department of Education.

[c]State programs are mainly TANF and Medicaid but to a lesser extent also include UI agencies.

Another agency that obtains a substantial amount of data from outside sources, OCSE, also made a presentation at the symposium. Although OCSE does not make benefit or loan payments, it is responsible for helping state child support offices collect child support payments from parents who are obligated to make such payments. In some cases, the law requires that these payments be used to offset public assistance benefits that the custodial parents received during periods when their ex-partners owed them child support.

OCSE has data from two sources that are instrumental in collecting child support payments: the NDNH and financial account information on individuals from financial institutions. Donna Bonar, Acting Associate Commissioner at OCSE, reported that

- in Texas, the amount of child support payments collected increased $4 million (32.6 percent) the month after that state automated wage withholding and began using the results from the NDNH match and

- in Virginia, child support collections increased by an estimated $13 million (33 percent[3]) in 1 year as a result of the NDNH match.

For the financial institution match, OCSE submits electronic files containing the names of individuals who are delinquent in their child support payments to about 3,000 financial institutions, and these institutions respond to OCSE when such individuals have accounts with them. Over a three-quarter period (July 1999 through March 2000), OCSE received information pertaining to more than 879,000 individuals with accounts totaling approximately $3 billion. Child support offices are able to collect lump-sum payments from delinquent child support obligators on the basis of these accounts. Ms. Bonar reported that

- the highest lump-sum payment collected was $74,000, of which $34,000 went to the state to reimburse the TANF program and $40,000 went to the custodial parent, and
- lump-sum payments commonly range from $20,000 to $30,000.

Technologies Are Expanding Data-Sharing Opportunities

Symposium speakers also discussed technologies that are expanding data-sharing opportunities and that offer new possibilities for data security. Three of the data-sharing applications discussed involve computer applications that make direct communication among computer systems possible. All three of these applications offer benefits to the government and the public, including the ability to verify program participant information and thereby detect improper payments sooner, or perhaps prevent them altogether. Integral to these discussions was how access to, and use of, shared information could be appropriately limited to official personnel for authorized reasons related to program administration. Another technological advancement discussed at the symposium was biometric identification systems, which are used to help ensure data security and prevent improper payments. These automated systems scan parts of the human body and, through a comparison with a previous scan, verify a person's identity.

[3]This percentage increase was provided by the Virginia Child Support Enforcement Agency.

Internet-Based Technology Promotes the Interoperability of Computer Systems

Three presentations focused on how technology has enabled government agencies to request information from and transmit it among different types of computer systems via the Internet or other network. These exchanges are possible because new types of software can facilitate communications between computers, translating information from one system into a format that is understandable by another system and end user, a capability known as interoperability. With interoperability, clusters of related computer systems can be linked, allowing information to be accessed and shared by many programs with similar purposes.

In one presentation, Marty Hansen, with SSA, and Ian Macoy, with NACHA—The Electronic Payments Association, focused on how agencies might access financial account information electronically from financial institutions. For benefit programs whose payments are based on need, agencies must know about the assets of applicants and recipients to determine what payment, if any, individuals are entitled to receive. In 1999 alone, according to SSA quality assurance reviews, unreported bank account balances resulted in approximately $240 million in overpayments in the SSI program. Historically, obtaining timely and accurate bank account information from the 20,000 financial institutions in the United States has not been cost-effective for agencies administering needs-based benefit programs; thus, such checks have been done only under certain circumstances. However, automating the process would greatly reduce the burden of requesting and retrieving such information for both the agencies and the financial institutions. A network that provided secure access, delivery, and storage for financial account information could enable benefit programs to prevent hundreds of millions of dollars in overpayments. The speakers proposed two technological alternatives for devising such a system. One possibility would be to "piggyback" on the previously discussed matching being done by financial institutions with OCSE. Another would be to set up a centralized list of beneficiaries and ask financial institutions to match their account holders against the list via network connections. This alternative could be made more attractive to financial institutions in two ways. First, if the information was shared by all the agencies needing account information, the financial institutions could avoid responding repeatedly to similar inquiries communicated through different avenues. Second, if financial institutions could also use the network to exchange information among themselves for commercial purposes, they would be motivated to participate. In presenting these alternatives, the speakers acknowledged that privacy is an issue that must be addressed.

A second presentation focused on how the model for DOD's health care benefit delivery system could be adapted to meet the data-sharing needs of benefit programs. According to William Boggess, an official with the DMDC, the DOD system provides a broad range of information on the 23 million beneficiaries of the military health care system. The system consists of a central computer system containing identifying information on beneficiaries linked to a network of "satellite" computer systems containing databases of other information about the beneficiaries, including medical, dental, immunization, and pharmaceutical records; benefit entitlement; and security clearances, among others. With this network of databases, Mr. Boggess said that DOD is able to respond, on average, within 4 seconds to over a million information requests each day from more than 1,400 locations in 13 countries.

Mr. Boggess then described how government agencies might improve their payment accuracy and program integrity if they created a nationwide network of benefit programs based on the DOD approach. A central database containing identifying information about the individual could be linked to the computer systems used by such programs as TANF, Food Stamps, SSI, Medicaid, and Medicare. Each agency could access the information it needed from any of the databases in the network, and each agency would have responsibility for maintaining the data in its own database. If agencies shared their data in this manner, individuals applying for or receiving benefits from multiple agencies could provide much of the information that these agencies needed only one time, to one agency. In addition, access to the databases of other agencies would make it possible for an agency to verify information provided by applicants and recipients to help ensure that benefits are provided only to those who are entitled to them.

David Temoshok, with GSA's Office of Governmentwide Policy,[4] explained how GSA is helping the Department of Education pilot a project involving a system of linked databases containing information on postsecondary educational and financial opportunities. These databases contain information on scholarships, loans, and grants; admission; registration; and student financial aid accounts. The pilot project uses interoperability technology to provide a Web-based exchange of the information among

[4]One of the responsibilities of GSA's Office of Governmentwide Policy is to develop policy and guidelines for electronic services. The education pilot project is being carried out as part of this responsibility.

many different computer systems. This system is intended to help student and financial aid administrators by presenting useful information in one place. In particular, agencies and lenders should be able to make better decisions because they will be able to access integrated student accounts via this system.

Guaranteeing the Security of Data in an Interoperable Environment

A number of speakers pointed out that while interoperability technology has improved the ease and efficiency of broad-based data sharing, it has also greatly increased the need for security in data sharing.[5] When information can be accessed or exchanged at numerous locations by many users, it is critical to have security measures in place that can control and track access. Mr. Temoshok described four basic elements that the federal government requires for the secure electronic exchange of information over networks: user identification and validation, secure transmission of data, assurance that the data are not changed in transmission, and assurance that parties to a transaction cannot later repudiate the transaction. To provide these elements, the federal government, under the leadership of OMB, is encouraging federal agencies to incorporate public key infrastructure (PKI) into their computer environments when warranted.

Richard Guida, Chairman of the Federal PKI Steering Committee, explained that PKI is a method whereby an individual generates a pair of digital keys, which are very large numbers, about 150 digits in length. One of these keys is called the private key because the individual keeps it to him- or herself. The other key is called the public key, and it is provided to anyone with whom the individual wishes to interact electronically. This latter key is made publicly available in the form of a digital certificate, which is an electronic credential that binds an individual's identity to the public key. Using these public and private keys, it is possible to electronically place and then verify a person's identity and ensure that electronic files do not get changed before, during, or after electronic transmissions. It is also possible to encrypt the information to ensure its privacy.

[5]For a general discussion about computer security at government agencies, see *Computer Security: Critical Federal Operations and Assets Remain at Risk* (GAO/T-AIMD-00-314, Sept. 11, 2000).

Biometric identification, which can be used both to prevent unlawful access to government records and to help identify improper benefit and loan payments, was also discussed at the symposium. Biometric identification systems scan unique physical features, such as fingers, eyes, faces, or hands, and convert the information to a digital format that can be stored in a computer or on an identification card. That information can be compared to earlier scans to verify a person's identity. The symposium speaker on this subject, David Mintie, an automated systems manager with the Connecticut Department of Social Services, said that human services departments around the country have begun using this technology (primarily finger imaging) as it has become affordable and practical to reduce and deter fraud and abuse. Mr. Mintie explained that when the identity of an individual can be readily established and verified, benefit recipients are much less likely to obtain benefits under false or duplicate identities in more than one city or state. Moreover, because the individual's identity can be verified before benefits are paid out, biometric identification can prevent improper payments from being made, not merely identify instances in which improper payments have already been made. In 3 years of operation, one type of biometric identification, finger imaging, prevented $23 million in improper payments in Connecticut and $297 million in New York. Texas estimates that the Food Stamp program avoided over $5 million in improper payments in that state in fiscal year 1999 as a result of finger imaging, and California estimates having saved $86 million in seven counties in the first 2 years of using finger imaging.

At the time of Mr. Mintie's presentation, 8 states were using biometric identification systems, and 21 others were either planning biometric systems or pursuing legislation to use biometrics. As a "next step," some of these states are working on developing standards for sharing and matching biometric fingerprint files among states. Such sharing, according to Mr. Mintie, could be a valuable tool for identifying individuals who receive duplicate welfare benefits in more than one state and for enforcing the nationwide 5-year time limit for receipt of welfare benefits. This sharing would enable welfare agencies not only to verify an individual's identity, but also to check an individual's welfare history when that person applied for benefits. In the absence of a nationwide system to track receipt of benefits, a welfare recipient nearing the end of the 5-year eligibility could simply relocate to another state and make a new application for benefits.

Privacy Is a Concern in a Data-Sharing Environment

Perhaps the single most important concern about sharing personal information among government programs is whether it can be done without sacrificing an individual's right to personal privacy. Although symposium speakers and audience participants who discussed privacy issues agreed that it is important to protect this right, they disagreed about the extent to which data sharing threatens it. Opinions also varied among symposium speakers and audience participants on how the nation's privacy laws should be changed.

Data Sharing Can Be a Risk to Personal Privacy

According to symposium speakers who discussed risks to privacy, the first risk to individuals is that their personal information may be wrongfully disclosed and perhaps misused. Such disclosure and misuse can occur when agency staff access data obtained from outside sources either without authorization to do so or, if authorized, for purposes unrelated to that authorization. Although this same type of abuse can occur with an agency's own data, the unease about data sharing is that, as the number of agencies and individuals who have access to personal information increases, so do the chances of wrongful disclosure and misuse of that information.

Although privacy advocates acknowledged that technologies exist that make wrongful disclosure and misuse of information somewhat more difficult and less likely, they believed that such tools have not, and cannot, always prevent such abuses. Others believed, however, that existing and new technologies have successfully managed this risk and will continue to do so. They cited such techniques as sending electronic data to other agencies over dedicated, secure computer lines; installing software that authenticates users and gives them access to only data that they are authorized to examine; establishing anomaly detection that notifies officials when a user has accessed something out of the ordinary; and using PKI.

The second risk to privacy that symposium speakers and audience participants described is that it is becoming more difficult for the public to know what personal information government agencies are maintaining in databases and how they are using it. The speakers viewed this limited public awareness as important because it inhibits society's ability to monitor what the government is doing with personal information. It also means that society's views about how the government is using such information are not being factored into political and public policy

decisions. Finally, the speakers characterized the limited public awareness about the wealth of information contained in databases as an increasing problem, given that technology has made it much easier to amass large amounts of information and to share it with others.

The NDNH was frequently used to illustrate these concerns during the symposium. Section 453 of the Social Security Act specifies the agencies that may use this database for purposes unrelated to the collection of child support payments and the purposes for which this use is permissible.[6] Privacy advocates were concerned about these "secondary" uses of the NDNH because they saw them as conflicting with a fundamental privacy principle, embodied in the Privacy Act, that data acquired for one purpose should not be used for a different purpose without the consent of the data subject. The Privacy Act provides 12 exceptions to this prohibition against disclosure without written consent, 1 of which benefit and loan agencies use to justify most of their data-sharing activities. This exception is called "routine use." Under routine use, an agency may not disclose data unless the use of the data is compatible with the purpose for which the data were collected. Privacy advocates said that it is hard to see how using the NDNH data for such secondary purposes as the administration of SSA, IRS, and Education programs is compatible with the original purpose of the NDNH: helping collect child support payments. Moreover, because the NDNH database is the most comprehensive and centralized information source that exists on the earnings of U.S. workers, privacy advocates fear that it will be sought by many other agencies for uses that the database subjects never contemplated.

Other symposium participants also saw the NDNH database as a valuable source of information for benefit and loan programs but did not see sharing this information as a threat to personal privacy. One audience participant mentioned, for example, that this information already exists in each of the states and that collecting it in a single federal file does not necessarily violate an individual's privacy. Some participants also believe that the public does have an opportunity to learn about, and comment on, new data-sharing initiatives involving NDNH data. For example, the Privacy Act requires that such initiatives be posted in the *Federal Register* for the

[6]SSA may use NDNH for the administration of its OASDI and SSI programs; Treasury, including the IRS, for the administration of federal tax laws and verification of claims for the Earned Income Tax Credit; and, more recently, Education, to obtain the addresses of individuals who have defaulted on their student loans.

purpose of public review and comment. Moreover, the public can learn about proposals for expanded access to NDNH data because such access is controlled to a large extent by legislation.

Symposium Participants Suggest That Privacy Laws May Need to Be Revisited

Symposium speakers discussed two key privacy laws that govern data sharing among benefit and loan agencies: section 6103 of the Internal Revenue Code and the Privacy Act, which includes the Computer Matching and Privacy Protection Act amendment. These laws were enacted in part to control whether and how tax return and personal information maintained by federal agencies could be shared. The laws describe situations in which an agency may disclose personal data. Section 6103 does this by specifically naming agencies that may have access to certain items of tax return information and specifying the conditions under which such access may be granted. The Privacy Act does this in part through the routine use provision described above. The Privacy Act also requires that agencies enter into written agreements when they share information that is protected by the Privacy Act for the purpose of conducting computer matches. These agreements, referred to as matching agreements, detail the information that will be exchanged, how the exchanges will occur, and how the receiving agency will verify the results of the match and keep the data secure.[7]

The Privacy Act and section 6103 were written in the 1970s, when many of today's advanced data-sharing capabilities did not exist. For example, according to Robert Veeder, a former OMB official who was responsible for overseeing the implementation of the Privacy Act, much of the data that were covered by this act existed on paper; thus, electronically sharing this information was relatively difficult. Mr. Veeder also said that it was much harder for agencies to share information electronically in those few cases in which there were electronic files of data because interoperability among computer systems did not yet exist. Privacy advocates believe that the technological changes that have occurred since the 1970s warrant that we as a society reexamine the type of data that we would like shared among government agencies and the extent to which such sharing should occur. In the absence of such a debate, these individuals believe that data sharing on the scale of the NDNH database will become the norm.

[7]For more information on the nation's privacy laws, see GAO/HEHS-00-119, Sept. 13, 2000.

Although other symposium speakers and audience participants also felt that the privacy laws should be changed, their comments focused on amending specific provisions that they felt make data sharing overly cumbersome yet do little to ensure that personal privacy is protected. One frequently cited provision that benefit and loan officials would like to see changed concerns the time limits on computer-matching agreements. Currently, under the Privacy Act, an initial computer-matching agreement between two agencies may remain in effect for only 18 months. After that, an extension must be negotiated between the agencies, and this extension may remain in effect for only 12 months. Once this 12-month period expires, the agencies must negotiate an entirely new agreement.

The time limits on computer-matching agreements were intended to cause agencies to periodically reassess the matches they conduct. Although officials believe that having time limits is valuable, they also argue that the limits are too short. Officials believe, for example, that the renegotiations can be time-consuming and burdensome and that the newly negotiated agreements often add no value to the data-sharing efforts because substantive changes are not often made to the computer matches themselves. Mr. Monaghan reported, for example, that most of the time of his staff is spent renegotiating these agreements, but that in reality this work is little more than a paper exercise. He also stated that SSA is drafting proposed legislation that would increase the time limit on new agreements to 5 years with a 3-year extension. We also suggested in a recent report on data sharing that the time limits on computer matching agreements be extended.[8] We reported that the appropriate time periods for new and renewed agreements are subject to debate, but that they range from 3 to 5 years for new agreements and 2 to 3 years for existing agreements.

Participants Made Various Suggestions for Advancing Data Sharing

Another topic discussed during the symposium was how data sharing should be advanced among benefit and loan agencies. An integral part of these discussions was the concern that any enhancements to data sharing be weighed against the need to protect personal privacy. Many of those who discussed such enhancements advocated that they include the necessary technological and legal protections to safeguard personal privacy. Some of these discussions focused on methods for facilitating data

[8]For more information, see GAO/HEHS-00-119, Sept. 13, 2000.

sharing governmentwide, while others addressed specific data-sharing initiatives.

Some Participants Suggested Methods for Facilitating Data Sharing Governmentwide

Data sharing is not always an agency priority because program officials feel they do not have enough staff and resources to handle additional data-sharing projects while still handling the work of their programs. Two speakers mentioned, for example, that some state human services departments might not be participating in interstate computer matches designed to detect recipients receiving benefits in more than one state because their current priority is to seek out potentially eligible recipients. Another speaker, Mr. Monaghan of SSA, mentioned that his agency would need additional resources to respond to every outside request for information because it is fully occupied with managing and operating its programs and enhancing its own matching activities.

Given that agencies are not always willing or able to take on data-sharing projects, some symposium speakers felt a need for an oversight body with authority to initiate and manage such projects. Thomas Stack, Director of Human Resources with Maximus Incorporated and until recently the Senior Advisor for Credit and Cash Management at OMB, described his vision of a board or committee composed of officials from various levels of government and the private sector. Such a group could be headed by OMB and include an equal number of members from key federal and state benefit and loan programs. It could develop a working group to support data sharing and establish software and hardware standards for agencies wishing to participate in data exchanges. The board could evaluate data-sharing proposals, addressing issues such as financing, management, timing, assigning the work, and examining the privacy implications. The board could also have some authority to decide which agencies should have access to the data of other agencies, and to what extent, and establish the required security controls for agencies wishing to access the data.

In discussing the funding of a network that could support such broad-based data sharing, Mr. Stack pointed out that the federal government made an estimated $19 billion dollars in improper payments in fiscal year 1998. Estimating that such a network would cost about $100 million to create, he proposed funding it with a portion of the program dollars that would be saved as a result of the reduced overpayments achieved through data sharing. Estimated program savings from current data sharing reported by symposium speakers amounts to more than $2 billion annually (see table 1).

A second suggestion for improving data sharing governmentwide was to create incentives for agencies themselves to take on more data-sharing projects. One idea proposed by Mr. Stack and others would be to allow agencies to use some of the program dollars saved through data-sharing efforts to expand such efforts and to pursue cases in which data exchanges have indicated possible overpayments.

Other Participants Focused on Specific Data-Sharing Initiatives

Several officials from benefit and loan programs mentioned that access to the NDNH database maintained by OCSE would greatly aid in the administration of their programs. Patricia Dalton, the Acting Inspector General for the Department of Labor, gave several examples of how access to this database would help improve the payment accuracy and assess the effectiveness of Labor programs. Labor is engaged in a proactive effort to investigate potentially fraudulent cases involving the $32 billion UI program. This program provides partial wage replacement for those who lose their jobs through no fault of their own. Many fraudulent schemes concerning UI payments involve fictitious claimants or claimants with nonexistent employers. In one case investigated by Labor, over $625,000 in fraudulent UI benefits were paid. Ms. Dalton believes that routine and expeditious access to centralized wage databases, such as the NDNH, would enable Labor to more efficiently verify wage data submitted by program applicants and thereby identify potential overpayments before they occur.

Symposium participants from other benefit programs, including TANF, Food Stamps, and Medicaid, also mentioned that NDNH data would be useful in controlling payment accuracy. These programs all depend on knowing the earnings of applicants and recipients to make correct initial and continuing eligibility decisions. In the cases of the Food Stamp, Medicaid, and Labor programs, the Congress would have to pass legislation granting access. The TANF program, however, has legislatively authorized access to the NDNH data, and it was envisioned that OCSE would ask the state agencies administering this program to go through their state child support agencies to get access. However, the state child support agencies often do not respond to TANF requests for information because of staff and resource concerns. According to Donna Bonar, OCSE Acting Associate Commissioner, OCSE intends to remedy this situation by developing a system under which the state TANF programs can obtain the information directly from OCSE.

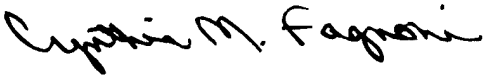
Another commonly suggested enhancement to data sharing frequently mentioned during the symposium was that, when possible, agencies use the data they obtain from outside sources during the application process. For example, agencies might query outside databases at the time of application to verify that applicants have disclosed their earnings accurately. This access to information could help prevent some overpayments from ever being made, as opposed to the current practice of using computer matches to identify such payments after they have occurred. Agencies could take this initiative without slowing down the application process by using electronic connections to outside databases to obtain the information immediately on-line or within a short period of time through a batched process. Several of the symposium participants believe this should be the future of data sharing. They believe that it would not only help ensure proper payments from the start but also enhance customer service, because the agency would obtain official verifications rather than requiring applicants to provide official documents, as is currently the case. While acknowledging these advantages of querying data sources, other participants think their programs need to evaluate it more thoroughly before deciding whether and how to implement it. One concern expressed by officials of various agencies, including OMB, is that querying data sources be done in such a way that individual privacy and data security are protected. Another concern is that the staff who make eligibility decisions are often overextended. Thus, before adding the requirement that they check outside databases, officials want to make sure it is cost-effective for the program as a whole.

Direct connections between government agencies do exist and in certain situations are being used to verify applicant-reported information in an effort to ensure that the correct payments are made at the outset. SSA has a network of dedicated, secure lines to most federal agencies and all 50 states. SSA uses this network to electronically transfer data used in computer matches and to receive and respond to queries at periodic intervals. SSA is also using this network for on-line, direct access. SSA plans to have on-line access to OCSE's NDNH data in January of 2001 and hopes to stop many SSI overpayments stemming from undisclosed wages by requiring its field staff to check the NDNH database for undisclosed wages before issuing the first check to newly eligible SSI recipients. SSA is also providing data on the recipients of its programs' benefits on-line to seven state human services departments that administer TANF benefits. According to an SSA official, some of these states are using SSA's data at the time of application to prevent overpayments to TANF recipients who

failed to disclose that they were also receiving SSA benefits.[9] SSA hopes to eventually expand on-line access to human services departments nationwide.

We are sending copies of this report to relevant congressional committees and other interested parties. We will make copies available to others upon request.

If you have any questions about this report, please contact me on (202) 512-7215. See appendix II for other GAO contacts and staff acknowledgments.



Cynthia M. Fagnoni
Managing Director, Education, Workforce,
and Income Security Issues

[9]Both SSI and OASDI benefits are considered income when determining TANF benefits.

Symposium Agenda—Data Sharing: Initiatives and Challenges Among Benefit and Loan Programs

Wednesday, June 7, 2000

Introductory Remarks—Comptroller General David M. Walker

OMB's Views on Data Sharing and Privacy—Sally Katzen, Deputy Director for Management, Office of Management and Budget

Symposium Overview—Cynthia M. Fagnoni, Managing Director, Education, Workforce, and Income Security Issues, GAO

Panel I—Data Sharing Has Improved Benefit and Loan Programs, but Barriers Remain

Moderator—Sigurd Nilsen, Director, Education, Workforce, and Income Security Issues, GAO

Data Sharing at SSA: Significant Benefits and Lessons Learned—Pete Monaghan, Director, Information Exchange and Computer Matching Staff, Social Security Administration

Multistate Data Sharing Is Improving Public Assistance Programs—Elliot Markovitz, Bureau of Program Evaluation, Pennsylvania Department of Public Welfare

Data Sharing Could Significantly Help DOL Control Benefit Payments and Improve Program Performance—Patricia A. Dalton, Acting Inspector General, Department of Labor

Child Support: A New Era of Data Matching—Donna J. Bonar, Acting Associate Commissioner, Office of Automation and Program Operations, Office of Child Support Enforcement

Panel II—Technology Offers New Data-Sharing Possibilities

Moderator—Lee Holcomb, Co-Chair, Interoperability Committee of the CIO Council, and Chief Information Officer for NASA

Accessing Financial Account Information to Improve Program Stewardship—Marty Hansen, Director, Payment and Recovery Policy Staff, Social Security Administration, and Ian W. Macoy, Senior Director, NACHA—The Electronic Payments Association

State Biometric Identification Projects and Exchanges at Social Service Agencies—David Mintie, Program Manager, Biometric Identification Project, Connecticut Department of Social Services

Interagency Data Exchanges Using the Internet—David M. Temoshok, Electronic Government Program Manager, Office of Governmentwide Policy, General Services Administration

Creating a Relational Data Base to Improve the Administration and Accuracy of Government Benefit Programs—William F. Boggess, Deputy Division Chief, DEERS System, Defense Manpower Data Center

Thursday, June 8, 2000

Panel III—Security and Privacy in a Data-Sharing Environment

Moderator—Barry Bedrick, Associate General Counsel, GAO

Privacy Concerns About Sharing Information on Program Participants—Maya A. Bernstein, Law Clerk, District of Columbia Court of Appeals, and former Principal Privacy Policy Expert, Office of Management and Budget

The Role of Privacy and Security Laws in a Data-Sharing Environment—Robert Veeder, President and Founder of The Privacy Advocates

The Confidentiality of Tax Information: Navigating Section 6103 of the Internal Revenue Code—Elizabeth P. Askey, Attorney-Advisor, Office of Tax Legislative Counsel, Department of the Treasury

New Technologies Designed to Ensure the Security and Privacy of Shared Data—Richard A. Guida, Chairman, Federal Public Key Infrastructure Steering Committee

VA's Pilot of Public Key Infrastructure (PKI) Technology to Guarantee the Security of Data in a Shared Environment—Daniel L. Maloney, Director of Emerging Technologies, Department of Veterans Affairs

Panel IV—Where Do We Go From Here?

Moderator—Sigurd Nilsen, Director, Education, Workforce, and Income Security Issues, GAO

This final session was a series of discussions led by congressional staff and representatives from the states, the private sector, the General Services Administration, and the Department of Agriculture.

Congress' Role in Promoting Data Sharing—Henry Wray and Kevin Landy, Counsels, Senate Committee on Governmental Affairs

State Perspectives on Data Sharing—Bradley Dugger, Chief Information Officer for Tennessee and former Chair of the National Association of State Information Resource Executives

Public/Private Partnerships for Data Sharing—Thomas Stack, Director, Human Resources Division, Maximus Incorporated

Issues in Data Matching Among State Welfare Programs—Abigail C. Nichols, Director, Program Accountability Division, Food Stamp Program, U.S. Department of Agriculture

Strategies for Overcoming Barriers to Data Sharing—Martha A. Dorris, Deputy Director, Office of Intergovernmental Solutions, General Services Administration

GAO Contacts and Staff Acknowledgments

GAO Contacts

Sigurd Nilsen, (202) 512-7003
Nancy Cosentino, (415) 904-2117

Staff Acknowledgments

In addition to those named above, the following individuals made important contributions to this report: Roland Miller III, Jill Yost, Christopher Morehouse, Jeremy Cox, James Lawson, and Inez Azcona.

Ordering Information

The first copy of each GAO report is free. Additional copies of reports are $2 each. A check or money order should be made out to the Superintendent of Documents. VISA and MasterCard credit cards are accepted, also.

Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:
U.S. General Accounting Office
P.O. Box 37050
Washington, DC 20013

Orders by visiting:
Room 1100
700 4th St. NW (corner of 4th and G Sts. NW)
U.S. General Accounting Office
Washington, DC

Orders by phone:
(202) 512-6000
fax: (202) 512-6061
TDD (202) 512-2537

Each day, GAO issues a list of newly available reports and testimony. To receive facsimile copies of the daily list or any list from the past 30 days, please call (202) 512-6000 using a touchtone phone. A recorded menu will provide information on how to obtain these lists.

Orders by Internet:
For information on how to access GAO reports on the Internet, send an e-mail message with "info" in the body to:

info@www.gao.gov

or visit GAO's World Wide Web home page at:

http://www.gao.gov

To Report Fraud, Waste, or Abuse in Federal Programs

Contact one:

- **Web site: http://www.gao.gov/fraudnet/fraudnet.htm**
- **e-mail: fraudnet@gao.gov**
- **1-800-424-5454 (automated answering system)**