

Privacy and Federal Agencies:

**Government Exchange and Merger
of Citizens' Personal Information is
Systematic and Routine**

A Special Report Issued by Privacilla.org
<http://www.privacilla.org>

March, 2001

Introduction

More than once every other week, a federal government agency quietly announces a new plan to exchange and merge databases of personal information about American citizens. Under the “Computer Matching and Privacy Protection Act,” they do this routinely, systematically — and legally. Currently:

- The Internal Revenue Service and the Social Security Administration share personal information about American citizens.
- The Social Security Administration and the Health Care Financing Administration share personal information about American citizens.
- The Postal Service and the Department of Labor share personal information about American citizens.
- The Department of Justice and the Department of Veterans Affairs share personal information about American citizens.
- The Internal Revenue Service and state social services agencies share personal information about American citizens.
- The Department of Health and Human Services and the Department of Education share personal information about American citizens.
- The Social Security Administration and the state courts share personal information about American citizens.

And the list goes on.

For the 18-month period from September 1999 to February 2001, federal agencies announced 47 times that they would exchange and merge personal information from databases about American citizens. And these programs are only the tip of an information-trading iceberg. The Computer Matching and Privacy Protection Act, which causes agencies to report these activities in *the Federal Register*, applies only to a small subset of the federal agency programs that exchange and merge databases of personal information.

While these computer matching programs are invariably intended for beneficial purposes, they do not serve Americans’ privacy interests. They demonstrate, instead, that privacy is a cost of the federal government’s numerous tax, law enforcement, and benefit

programs. Despite its name, the Computer Matching and Privacy Protection Act does not protect privacy.

As the Federal Trade Commission, the Department of Health and Human Services, and other agencies review merger and exchange of personal information in the private sector, they conveniently ignore the government's own, more significant role in threatening privacy. The federal government is in fact the largest collector, user, and sometime abuser of citizens' personal and private information. Governments are fundamentally *not* in the business of protecting privacy.

Federal agencies and the Congress should not look outward for opportunities to protect privacy. They should look inward at the privacy threats the government creates through the merger and exchange of personal information it has collected about American citizens.

The federal government is the largest collector, user, and sometime abuser of citizens' personal and private information. Governments are fundamentally *not* in the business of protecting privacy.

In this report, Privacilla describes the Computer Matching and Privacy Protection Act, then briefly analyzes merger and exchange of citizens' personal information by the federal government. We shine on government the light that the Federal Trade Commission is currently turning on the private sector. An appendix lists the 47 instances in the last 18 months where a federal agency has announced a computer matching program. As should be clear, government poses a greater threat to privacy than the private sector.

It is important, however, not to draw too broad a conclusion from privacy-threatening government data practices. There are legitimate interests served by government data-sharing, and there are some protections for citizens. However, because governments have a unique power to write and rewrite the rules about what can be done with personal information — a power no private-sector entity has — governments should be the first to give up data merger practices that threaten privacy.

The United States Congress should take a sweeping look at the federal government's information practices.

The United States Congress — not any limited-jurisdiction agency — should take a sweeping look at the federal government's information practices. It is likely to find a breathtaking amount of personal data exchange and surveillance. The extent of it assuredly offends Americans' powerful sense that they should have some way to protect their privacy by controlling how government uses information about them.

The “Computer Matching and Privacy Protection Act”

The Computer Matching and Privacy Protection Act of 1988 (Public Law 100-503) amended the Privacy Act of 1974. Invoking “privacy,” it regularized and systematized the merger and exchange of Americans’ personal information among federal agencies.

The Act covers only two kinds of programs that match databases of personal information about American citizens: matches involving federal benefits programs, and matches using records from Federal personnel or payroll records. Other programs under which federal agencies exchange and merge personal information about citizens — and there are many — are not covered by the Act or by this study.

In fact, the list of programs *not* subject to the Computer Matching and Privacy Protection Act is longer than the list of programs that are. Exclusions from the Act include:

- Statistical matches whose purpose is solely to produce aggregate data stripped of personal identifiers;
- Statistical matches whose purpose is in support of any research or statistical project;
- “Pilot matches” whose purpose is to gather benefit/cost data about full-scale matching programs;
- Law enforcement investigative matches whose purpose is to gather evidence against a named person or persons in an existing investigation;
- “Tax administration matches,” including 1) disclosure of taxpayer information to state tax officials; 2) matches for administration, management, conduct, direction, and supervision of the execution and application of the internal revenue laws, as well as assessment, collection, enforcement, litigation, publication, and statistical gathering functions; and 3) tax refund offset matches;
- Routine administrative matches using Federal personnel records;
- Internal agency matches using only records from the agency’s systems of records; and
- Background investigation and foreign counter-intelligence matches.

The Privacy Act allows disclosures of records if the agency decides that disclosures are “routine.” In such cases, the agency need only publish a *Federal Register* announcement that personal information will be disclosed.

Federal agencies engaging in computer matching programs must enter into “matching agreements” that are approved by the agencies’ “Data Integrity Boards.” Such

agreements must include “procedures for the retention and timely destruction of identifiable records” and “prohibitions on duplication and redisclosure of records.” They also must provide that the Comptroller General may have access to all necessary records to monitor or verify compliance with the agreement.

The Computer Matching and Privacy Protection Act includes important due process protections when a matching program reveals that adverse action may need to be taken against a citizen. The agency must verify the adverse information, and give the individual notice and an opportunity to contest any adverse action. Important though these protections are, they do not go to protecting privacy. Fundamentally, privacy is at odds with much of what modern governments do.

Government Data Exchange and Privacy

The Computer Matching and Privacy Protection Act does not meaningfully contribute to the privacy that American citizens enjoy. By regularizing transfer of citizen data among federal agencies, in fact, the Act sanctions and contributes to the federal government’s threat to privacy. The reason for this is a set of misunderstandings about privacy that befuddled policy-makers in 1988 and that still do today. To unravel them, we turn to some basic principles.

Privacy, that quixotic concept that has frustrated and confounded so many, is best regarded as a *condition*. It is a state of affairs in which knowledge of information about a person is tailored to that person’s interests in revealing or holding that information close. These interests express themselves through the actions of individuals under the infinite circumstances presented throughout daily life. Privacy, the condition, reflects deeply complex and personal values held by individuals.

Privacy, that quixotic concept that has frustrated and confounded so many, is best regarded as a *condition* that reflects deeply complex and personal values held by individuals.

Government cannot protect privacy. It can only foster or destroy people’s ability to protect their own privacy. Privacy is maintained by people having authority and responsibility for what information about them is shared, and on what terms.

When government has collected information from people under the authority of law, people’s ability to protect privacy in that information is taken away. Rules about how government handles data, complex and onerous as they may be, cannot “protect privacy” of information that is already out of individuals’ control. Such rules are really

only guesses by politicians and bureaucrats at what people might choose if they still could. Rules to protect the “privacy” of information held by governments are little more than tardy apologies for stepping between people and their ability to protect privacy in the first place.

In the case of the Computer Matching and Privacy Protection Act, citizens’ data is not made private by sharing it among agencies under strict rules requiring security and accuracy. The information is already wrested from the control of the data subjects. Other than through destruction of the information, which would return control to citizens, no amount of rules can recreate privacy in that information.

The only way truly to protect privacy is through systems that give consumers and citizens the choice, coupled with the responsibility, to protect privacy as they see fit. This is why privacy is inconsistent with so much of what government does. Even the best-intended government programs have as part of their design the removal of citizens’ power over information about themselves. In the private sector, by contrast, privacy can be protected through a combination of educated consumer choice and the freedom to contract, backed up by the privacy torts.

The only way truly to protect privacy is through systems that give consumers and citizens the choice, coupled with the responsibility, to protect privacy as they see fit.

Like modern government, the modern commercial world thrives on information, and it is sometimes very difficult for consumers to know how to protect their privacy. Even when they do, protecting privacy can be very inconvenient. But when dealing with government, it is often outright *illegal* for citizens to protect their privacy. Privacy is a cost of government, one that must be acknowledged forthrightly by serious thinkers.

Turning the FTC Spotlight on Government

Yet the commercial world is today regarded as the greater threat to privacy. Needless to say, many politicians and bureaucrats see opportunities for making hay with the issue. In announcing a “public workshop” on merger and exchange of consumer data in the private sector, the Federal Trade Commission recently posed several questions about current business practices.¹ These questions should be rewritten and addressed to current government practices. The answers reveal how government programs threaten privacy and possibly even violate Fourth Amendment rights.

¹ The announcement can be found at <<http://www.ftc.gov/os/2001/02/mergingfrn.htm>>.

What kinds of citizen information do agencies exchange and what are the sources of that information?

The government sector thrives on information about people. Personal information allows governments to collect taxes, serve up entitlements and benefits, and enforce laws and regulations.

Taxation requires massive collections of information without regard to whether it is personal or private. The list of information required by tax laws and held by the Internal Revenue Service is incredibly long because the government sector is addicted to using taxation as a tool of social policy. The information collected by the IRS includes name, address, phone number, income, occupation, marital status, parental status, investment transactions, home ownership, medical expenses, purchases, foreign assets, charitable gifts, and much more. It is collected both directly from the taxpayer and from “information returns” that must be filed by businesses. Importantly, the law requires people to submit this information. At no point do citizens have an option to withhold information.

The federal government uses copious amounts of information to deliver various entitlements and benefits as well. Any program that doles money out based on condition or status must know what people’s condition or status is, often in comparison to the condition or status of the population at large. Health programs, for example, require beneficiaries’ names, addresses, telephone numbers, genders, ages, income levels, medical conditions, medical histories, providers’ names, and much more. This information is collected both directly from the beneficiary and from health care providers. Collection is also required by law, or as a condition of receiving benefits. Citizens do not have a practical option of withholding it.

A third use the government sector makes of personal information is to investigate crime and enforce laws and regulations. Law enforcers’ ability to do these things correlates directly to the amount of information they can collect about where people go, what they do, what they say, to whom they say it, what they own, what they think, and so on. We rely on government to investigate wrongdoing by examining information that is often regarded as private in the hands of the innocent. It is a serious and legitimate concern of civil libertarians that government collects too much information about the innocent in order to reach the guilty. Though it is unlikely that information collected in investigations is matched under the Computer Matching and Privacy Protection Act, government entities like the Financial Crimes Enforcement Network collect information from a variety of sources and share it widely. Again, no citizen can practically and legally prevent this information from being collected.

Are there new technologies or technical standards that may increase the sharing of detailed citizen information and do they include or facilitate privacy protections?

It is important to focus away from technologies in privacy debates. Nearly all technologies can be used for good purposes and bad purposes alike. Information technology can be used both to improve efficiency and to threaten or invade privacy. As a matter of privacy policy, nearly all technologies should be treated with neutrality or indifference. It is different *uses* of technology that should be addressed.

Increased digitization of records and record-keeping means that agencies can work with information more quickly and ably. More efficient government is sorely needed, and, to the extent technology can be used to lower the cost of government while improving the delivery of services, it benefits the public.

On the other hand, technology increases the power of agencies and individual bureaucrats to do harm. The Internal Revenue Service, for example, is aggressively pushing electronic filing. While this will undoubtedly improve its operations as our nation's tax collector, e-filing will also make Americans' tax information more accessible for both good and bad purposes. Paper IRS filings are today protected to some extent by "practical obscurity." Anyone wanting information has to go and dig them out of a physical file. The IRS has had problems in the past with employees snooping into citizens' files. These could recur on a wider scale thanks to technology.

On balance — and provided security controls are put in place — technologies should be regarded at worst with indifference, and more often as improvements over former practice. The rules that apply to use and control of information are what matter to privacy.

How does the merger and exchange of detailed citizen data between federal agencies affect citizens?

Merger and exchange of citizen data by federal agencies inherently harm citizens by eroding their ability to protect their privacy.

The Fourth Amendment to the Constitution is the primary, essential limit on the power of governments in the U.S. to inquire into people's lives, arrest them, and take their property. The Framers of the Constitution recognized the unique powers of government

— powers that no private-sector entities have. They sought to curtail them by preventing governments from collecting information about citizens without substantial justifications.

The growth of the federal government during the 20th century vastly increased the amount of personal information about citizens that governments in the United States collect. As noted above, more and more information is collected for increasingly complex taxation and benefits programs.

When information is collected for these “administrative” purposes, the government does not have to face Fourth Amendment limitations, and it can collect information at will. The upshot is that governments can effectively search citizens without cause by going back to them again and again for personal information under myriad tax and benefit programs.

Law-abiding Americans have a reasonable expectation that information collected by governments will not be amassed into dossiers or held in databases that are easily and quickly combined for whatever purposes capture the government’s interest. The merger and exchange of detailed personal information among federal agencies violates citizens’ expectations under the Fourth Amendment to be free of warrantless government snooping into their affairs.

Because the United States’ special constitutional rules are supposed to limit governments’ power to collect information about citizens, widespread exchange and merger of personal information by federal agencies may violate the Fourth Amendment. These practices certainly prevent people from maintaining privacy at the levels they desire.

What types of notice have federal agencies provided consumers regarding various kinds of data merger and exchange activities?

Though some federal agencies may provide notice that there will be merger and exchange of information at the time information is collected, this notice is usually not sufficient because agencies routinely alter the uses they make of personal information.

Notices of new merger and exchange programs are usually given through announcements in the *Federal Register*. This daily publication is perfectly obscure to the clear majority of Americans about whom federal agencies exchange personal information. *Federal Register* notice is technical, legal notice. It is an unsatisfactory way to keep the public meaningfully informed about uses that are being made of personal information.

Of course, notice is worth even less if nothing can be done about information collection and sharing in the first place. As mentioned above, personal information is collected by governments under the authority of law or as a condition of receiving benefits. Citizens have no effective power to withhold information at any point in the process.

Citizens also have little power to stop merger and exchange of information being undertaken by federal agencies. To attempt it, they must contact their political leaders and be lucky enough to do so in sufficient numbers to make a federal political issue out of it. Even highly objectionable government collection of citizens' personal financial information continues today under the Bank Secrecy Act, while private-sector firms like DoubleClick and N2H2 have terminated information collection and merger proposals in the face of public concern.

The notice federal agencies give of their data merger and exchange plans are technical and legal. They serve only to emphasize the powerlessness of citizens in the face of their government.

What governmental purposes are served through the merger of an agency's internal information about citizens with information obtained from other agencies?

There should be no mistake about it. Merger and exchange of personal information among federal agencies serves many useful purposes.

Judging by the stated purposes of the computer matches identified in this survey, one of the primary uses of personal information by federal agencies is for debt collection and assessment of credit risk. There are many delinquencies in the numerous federal loan and loan guarantee programs. Merger and exchange of personal information about Americans helps agencies locate debtors and collect money owed. Many computer matches also assess whether applicants for loans or benefits are in compliance with the law. This serves law enforcement goals, and also helps ensure that the federal government makes or guarantees loans to law-abiding citizens.

A second major purpose of the computer matching programs identified in this survey is avoiding waste and overpayment in federal programs. By comparing income and annuity information from one agency, for example, another agency can check the accuracy of information that has been submitted by beneficiaries. Agencies use health care utilization records, for example, to identify program beneficiaries who may be deceased so that their benefits can be terminated. Though it is assuredly quite concerning

that health care records should be transferred throughout the federal government for this purpose, it does serve laudable goals.

Finally, a major beneficial use of merger and exchange of personal information is to catch criminals. By comparing information collected by, and submitted to different agencies, law enforcement can catch people who are defrauding the government, underpaying taxes, receiving benefits for which they are not eligible, and so on.

Though privacy interests are assuredly sacrificed, there can be no mistake that important governmental purposes are served by agencies' merger and exchange of personal information.

Conclusion

Federal government agencies are exchanging and merging personal information about citizens constantly and increasingly. On average, a new program for comparing databases of personal information is announced every two weeks. Over the 18-month period September 1999 to February 2001, announcements of these programs were issued at least 47 times.

It is more than ironic that federal government agencies should look askance at information practices in the commercial sector. Governments — unlike any private-sector entities — have the power to inquire by force of law into people's lives, arrest them, and take their property. Governments alone can write and rewrite the rules about how information may be used.

The Computer Matching and Privacy Protection Act is poorly named. The privacy of personal information in the hands of government cannot be protected, because privacy is a condition people maintain by the exercise of control over their information and themselves. Privacy can not be a product of government functions and programs, which rely on eroding citizens' privacy. Indeed, privacy is a direct and substantial cost of government.

The government can do its most fruitful work to restore privacy by correcting its own practices.

Congress should examine anew the federal government's information practices and its massive use of citizens' personal information. It should consider the costs to privacy of the many government programs and functions that rely on reducing citizens' control over personal information. The government can do its most fruitful work to restore privacy by correcting its own practices. The American people expect and deserve no less.

APPENDIX

Survey of Merger and Exchange of Citizen Data (Sept. 1, 1999 – Feb. 28, 2001)

The table below draws from *Federal Register* notices under the Computer Matching and Privacy Protection Act. It includes date of *Federal Register* notice, agency giving notice, list of other participating agencies, and excerpts from the stated purpose of the computer matching program.

Notice Date	Agency	Participating Agencies	Purpose of Matching Program
2/20/2001	Social Security Administration	Railroad Retirement Board	“ . . . to disclose RRB annuity payment data . . . ” “ . . . to verify Supplemental Security Income (SSI) program and Special Veterans Benefits (SVB) eligibility and benefit payment amounts.”
2/16/2001	Social Security Administration	Health Care Financing Administration, Department of Health and Human Services	“ . . . to identify Supplemental Security Income (SSI) recipients and Special Veterans’ Benefits beneficiaries who have been admitted to certain public institutions.”
2/13/2001	Social Security Administration	Health Care Financing Administration, Department of Health and Human Services	“ . . . to disclose Medicare non-utilization data to SSA.”
2/12/2001	Department of Education	Social Security Administration	“ . . . to assist the Secretary of Education in his obligation to ‘verify immigration status and social security numbers [SSN] provided by a student to an eligible institution’”
1/8/2001	Defense Manpower Data Center, Defense	Office of Personnel Management	“ . . . to identify individuals who are improperly receiving credit for military service in their civil service annuities or annuities based on the

	Logistics Agency, Department of Defense		‘guaranteed minimum’ disability formula.”
12/7/2000	Office of Personnel Management	Social Security Administration	“ . . . SSA records are used in redetermining and recomputing certain annuitants’ benefits . . .”
12/1/2000	Office of Inspector General, Postal Service	Office of Workers’ Compensation Programs, Department of Labor	“ . . . to determine whether the current Postal Service automated and manual procedures for monitoring FECA benefits payments made to employees returning to work are operating effectively.” “ . . . to identify those Postal Service employees who may have received dual benefits in violation of section 8116(a) of the FECA.”
11/29/2000	Office of the Chief Information Officer, Department of Housing and Urban Development	Social Security Administration; Internal Revenue Service, Department of Treasury	“ . . . to increase the availability of rental assistance to individuals who meet the requirements of the rental assistance programs.” “ . . . determining the appropriate level of rental assistance, and deterring and correcting abuses in assisted housing programs.”
11/16/2000	Social Security Administration	Internal Revenue Service	“ . . . to disclose to SSA certain return information for use in verifying eligibility for, and/or the correct amount of, benefits . . .”
11/7/2000	Immigration and	Minnesota Department of Economic Security	“ . . . to confirm the immigration status, and therefore eligibility status, of alien applicants for,

	Naturalization Service, Department of Justice		or recipients of, unemployment compensation.”
10/25/2000	Office of Personnel Management	Social Security Administration	“ . . . to verify earnings data supplied by civil service annuitants.”
10/16/2000	Internal Revenue Service, Department of Treasury	Federal, state, and local agencies, including Department of Housing and Urban Development Albany Financial Operations Center; Debt Collection and Management System, Department of Justice; Accounts Receivable Records, Department of Veterans Affairs; Social Security Administration Master Beneficiary Record and Supplemental Security Income Record and Special Veterans Benefits; Department of Education Student Financial Assistance Collection Files	“ . . . to prevent or reduce fraud or abuse in certain Federally assisted benefit programs and facilitate the settlement of government claims while protecting the privacy interest of the subjects of the match.”
10/13/2000	Department of Veterans Affairs	Bureau of Prisons, Department of Justice	“ . . . to verify continuing eligibility for Federal benefit programs of those who are confined for a period exceeding 60 days due to a conviction for a felony or misdemeanor.”
10/12/2000	Internal Revenue Service, Department of the Treasury	Federal, state, and local agencies, including Real Estate Assessment Center, Department of Housing and Urban Development; Veterans Benefits Administration, Department of Veterans Affairs; Office of Program Benefits Policy, Social Security Administration; Alabama Department of Human Resources;	“ . . . to prevent or reduce fraud and abuse in certain federally assisted benefit programs while protecting the privacy interests of the subjects of the match.”

		<p>Alabama Medicaid Agency; Alaska Department of Health and Social Services; Arizona Department of Economic Security; Arizona Health Care Cost Containment System; Arkansas Department of Human Services; California Department of Social Services; Colorado Department of Human Services; Connecticut Department of Social Services; District of Columbia Department of Human Services; Florida Department of Children and Families; Georgia Department of Human Resources; Guam Department of Public Health and Social Services; Hawaii Department of Human Services; Idaho Department of Health and Welfare; Illinois Department of Human Services; Indiana Family and Social Services Administration; Iowa Department of Human Services; Kansas Department of Social and Rehabilitation Services; Kentucky Cabinet for Families and Children; Louisiana Department of Social Services; Maine Department of Human Services; Maryland Department of Human Resources; Massachusetts Department of Transitional Assistance; Massachusetts Division of Medical Assistance; Michigan Family Independence Agency; Minnesota Department of Human Services; Mississippi Division of Medicaid; Mississippi Department</p>	
--	--	---	--

		<p>of Human Services; Missouri Department of Social Services; Montana Department of Public Health and Human Services; Nebraska Department of Health and Human Services; Nevada Department of Human Resources; New Hampshire Department of Health and Human Services; New Jersey Department of Human Services; New Mexico Human Services Department; New York Office of Temporary and Disability Assistance; North Carolina Department of Health and Human Services; North Dakota Department of Human Services; Ohio Department of Human Services; Oklahoma Department of Human Services; Oregon Department of Human Services; Pennsylvania Department of Public Welfare; Puerto Rico Department of the Family; Puerto Rico Department of Health; Rhode Island Department of Human Services; South Carolina Department of Social Services; South Dakota Department of Social Services; Tennessee Department of Human Services; Texas Department of Human Services; Utah Department of Health; Utah Department of Workforce Services; Vermont Department of Prevention, Assistance, Transition, and Health Access; Virgin Islands Bureau of Health Insurance and Medical Assistance; Virgin Islands Department of Human Services;</p>	
--	--	---	--

		Virginia Department of Social Services; Washington Department of Social and Health Services; West Virginia Department of Human Services; Wisconsin Department of Workforce Development; Wyoming Department of Family Services	
10/12/2000	Social Security Administration	Department of Labor	“ . . . to disclose Black Lung benefit data to SSA.” “ . . . to determine the correct amount of Social Security disability benefits for recipients of Part C Black Lung benefits”
10/6/2000	Railroad Retirement Board	Office of Personnel Management	“ . . . to enable the RRM [sic] to (1) Identify affected RRB annuitants who are in receipt of a Federal public pension benefit but who have not reported receipt of this benefit to the RRB and (2) receive needed Federal public pension benefit information for affected RRB annuitants more timely and accurately.”
9/7/2000	Department of Education	Office of Child Support Enforcement, Administration for Children and Families, Department of Health and Human Services	“ . . . to obtain address information on individuals who owe funds to the Federal Government under defaulted student loans or grant overpayments.”
9/6/2000	Social Security Administration	Office of Personnel Management	“ . . . to verify the accuracy of information furnished by applicants and recipients concerning eligibility factors for the Supplemental Security Income (SSI) and Special Veterans’ Benefits (SVB) programs.” “ . . . to identify disability insurance beneficiaries whose benefits should be reduced” “ . . . to [calculate] a modified benefit computation formula . . . for certain persons who receive both a

			civil service benefit and a Social Security retirement or disability benefit.” “ . . . to verify information provided . . . by the SSA beneficiary at the time of initially applying for Social Security benefits and on a continuing basis . . .”
9/1/2000	Railroad Retirement Board	Health Care Financing Administration, Department of Health and Human Services	“To identify RRB annuitants who are 66 or over and who have not had any Medicare utilization during the past calendar year.”
8/23/2000	Department of Education	Internal Revenue Service, Department of Treasury	“ . . . permits ED to have access to any taxpayer’s mailing address who has defaulted on certain loans . . . for the purpose of locating the taxpayer to collect the loan.” “ . . . provides for redisclosure . . . to any lender, or State or nonprofit guarantee agency”
8/22/2000	Social Security Administration	Texas Workers Compensation Commission	“ . . . to identify Title II and/or Title XVI recipients who are receiving workers compensation benefits.”
8/21/2000	Railroad Retirement Board	Social Security Administration	“The RRB will, on a daily basis, obtain from SSA a record of the wages reported to SSA for persons who have applied for benefits” “ . . . [T]he RRB will receive from SSA the amount of certain social security benefits which the RRB pays on behalf of SSA.” “ . . . [T]he RRB will receive from SSA once a year a copy of SSA’s Master Benefit Record for earmarked annuitants.” “SSA will receive from RRB weekly RRB earnings information for all railroad employees.” “SSA will also receive from RRB on a daily basis

			RRB earnings information on selected individuals.”
8/16/2000	Department of Housing and Urban Development	Department of Education	“ . . . will allow the Department of Education access to a system which permits prescreening of applicants for debts owed or loans guaranteed by the Federal Government to ascertain if the applicant is delinquent in paying a debt owed to or insured by the Government.”
8/15/2000	Department of Veterans Affairs	Department of Defense	“ . . . to identify the eligibility status of veterans, servicemembers, and reservists who have applied for or who are receiving education benefit payments under the Montgomery GI Bill.”
8/14/2000	Department of Education	Postal Service	“ . . . will compare USPS payroll and ED delinquent debtor files for the purpose of identifying postal employees who may owe delinquent debts to the federal government under programs administered by the ED.”
7/28/2000	Department of Veterans Affairs	Postal Service	“ . . . to identify and locate USPS employees who owe delinquent debts to the Federal Government as a result of their participation in benefit programs administered by VA.”
7/28/2000	Department of Veterans Affairs	Internal Revenue Service, Department of Treasury	“ . . . to locate taxpayers who owe delinquent debts to the Federal Government as a result of their participation in benefit programs (including health care) administered by VA.”
7/27/2000	Social Security Administration	State Courts	“To identify individuals who are subject to the title II benefit nonpayment on section 202(x)(1) on the Social Security Act”
6/9/2000	Department of	Department of Veterans Affairs	“ . . . will allow VA access to a system which

	Housing and Urban Development		permits prescreening of applicants for loans or loans guaranteed by the Federal Government to ascertain if the applicant is delinquent in paying a debt owed to or insured by the Government.”
6/5/2000	Defense Manpower Data Center, Defense Logistics Agency, Department of Defense	Small Business Administration	“ . . . to identify and locate any matched Federal personnel, employed, serving, or retired, who owe delinquent debts to the federal government under certain programs administered by SBA.”
4/11/2000	Administration for Children and Families, Department of Health and Human Services (on behalf of itself, the Health Care Financing Administration, and the Food and Nutrition Service)	Department of Veterans Affairs; Connecticut Department of Social Services; District of Columbia Department of Social Services; Florida Division of Public Assistance; Illinois Department of Public Aid; Kansas Department of Social and Rehabilitation Services; Louisiana Department of Social Services; Maryland Department of Human Resources; Massachusetts Department of Transitional Assistance; Nebraska Department of Social Services; New York Department of Social Services; North Carolina Department of Human Resources; Ohio Department of Human Services; Oklahoma Department of Human Services; Pennsylvania Department of Public Welfare; South Dakota Department of Social Services; Tennessee Department of Human Services; Texas Department of Human	“ . . . to provide [state public assistance agencies] with data from the VA benefit and compensation file for the states to determine eligibility and insure fair and equitable treatment”

		Services; Utah Department of Workforce Services and Department of Health; Virginia Department of Social Services	
4/10/2000	Office of Personnel Management	Social Security Administration	“ . . . to offset specific benefits by a percentage of benefits payable under Title II of the Social Security Act.”
3/28/2000	Social Security Administration	State Health / Income Maintenance Agencies	“To identify eligible Supplemental Security Income (SSI) Medicaid enrollees whose records have been inactive”
3/14/2000	Defense Manpower Data Center, Defense Logistics Agency, Department of Defense	National Science Foundation	“ . . . to identify and locate any matched Federal personnel, employed, serving, or retired, who owe delinquent debts to the Federal Government under certain programs administered by NSF.”
3/8/2000	Department of Education	Department of Justice	“ . . . to assist ED in enforcing the sanctions imposed under section 5301 of the Anti-Drug Abuse Act of 1988 (Pub. L. 100-690).”
3/1/2000	Department of Education	Immigration and Naturalization Service, Department of Justice	“ . . . will permit ED to confirm the immigration status of alien applicants for, or recipients of, assistance”
2/8/2000	Defense Manpower Data Center, Defense Logistics Agency, Department of	Department of Veterans Affairs	“ . . . to identify and locate any Federal personnel, employed, serving, or retired, who owe delinquent debts to the Federal Government under certain programs administered by VA.”

	Defense		
1/27/2000	Immigration and Naturalization Service, Department of Justice	District of Columbia Department of Employment Services; New York State Department of Labor; New Jersey Department of Labor; Texas Workforce Commission; Massachusetts Department of Employment and Training; California Department of Social Services; California Department of Health Services; Colorado Department of Human Services	“ . . . to confirm the immigration status of alien applicants for, or recipients or, Federal benefits assistance”
12/29/1999	Department of Education	Social Security Administration	“ . . . will provide an efficient and comprehensive method of identifying incarcerated applicants who are ineligible to received [sic] student financial assistance”
11/29/1999	Social Security Administration	States	“ . . . to facilitate administration of [the required income and eligibility verification system]”
11/15/1999	Selective Service System	Department of Education	“ . . . to ensure that the requirements of section 12(f) of the Military Selective Service Act (50 U.S.C. App. 462(f) are met.”
10/26/1999	Office of the Chief Information Officer, Department of Housing and Urban Development	Small Business Administration	“ . . . will allow SBA access to a system which permits prescreening of applicants for debts owed or loans guaranteed by the Federal Government to ascertain if the applicant is delinquent in paying a debt owed to or insured by the Government. In addition, HUD will be provided access to SBA’s debtor data for prescreening purposes.”
10/13/1999	Social Security	Internal Revenue Service, Department of the	“ . . . to locate certain recipients of Social Security

	Administration	Treasury	benefits . . . in order to aid in the collection or compromise of Federal claims against these individuals”
9/29/1999	Social Security Administration	Compensation and Pension Service, Department of Veterans Affairs	“To identify Supplemental Security Income (SSI) recipients who receive benefits and to update their SSI records to reflect the presence of such income.”
9/29/1999	Office of the Chief Information Officer, Department of Housing and Urban Development	Department of Agriculture	“ . . . will allow USDA access to a system which permits prescreening of applicants for loans owed or guaranteed by the Federal Government to ascertain if the applicant is delinquent in paying a debt owed to or insured by the Government.”
9/16/1999	Office of Personnel Management	Office of Workers’ Compensation Programs, Department of Labor	“ . . . to identify and/or prevent erroneous payments under the Civil Service Retirement Act (CSRA) or the Federal Employees’ Retirement System Act and the Federal Employees’ Compensation Act (FECA).”
9/14/1999	The Real Estate Assessment Center, Department of Housing and Urban Development	Social Security Administration; Internal Revenue Service, Department of Treasury	“ . . . identifying potential income discrepancies, i.e., income that tenants did not report as required when applying for initial or continued rental assistance.”