United States Government Accountability Office

GAO

Testimony

Before the Committee on Consumer Affairs and Protection and Committee on Governmental Operations, New York State Assembly

For Release on Delivery
Expected at 10:30 a.m. EST
Thursday, September 15, 2005

SOCIAL SECURITY NUMBERS

Federal and State Laws Restrict Use of SSNs, yet Gaps Remain

Statement of Barbara D. Bovbjerg, Director
Education, Workforce, and Income Security Issues

September 15, 2005

SOCIAL SECURITY NUMBERS

Federal and State Laws Restrict Use of SSNs, yet Gaps Remain

GAO Accountability·Integrity·Reliability

Highlights

Highlights of GAO-05-1016T, a report to the Committee on Consumer Affairs and Protection and the Committee on Governmental Operations, New York State Assembly

Why GAO Did This Study

In 1936, the Social Security Administration established the Social Security number (SSN) to track worker's earnings for Social Security benefit purposes. Despite its narrowly intended purpose, the SSN is now used for a myriad of non-Social Security purposes. Today, SSNs are used, in part, as identity verification tools for services such as child support collections, law enforcement enhancements, and issuing credit to individuals. Although these uses can be beneficial to the public, the SSN is now a key piece of information in creating false identities. The aggregation of personal information, such as SSNs, in large corporate databases and the increased availability of information via the Internet may provide criminals the opportunities to commit identity theft.

Although Congress and the states have enacted a number of laws to protect consumers' privacy, the public and private sectors' continued use of and reliance on SSNs, and the potential for misuse, underscore the importance of strengthening protections where possible. Accordingly, this testimony focuses on describing (1) the public use of SSNs (2) the use of SSNs by certain private sector entities, and (3) certain federal and state laws regulating the use of SSNs and identity theft.

www.gao.gov/cgi-bin/getrpt?GAO-05-1016T.

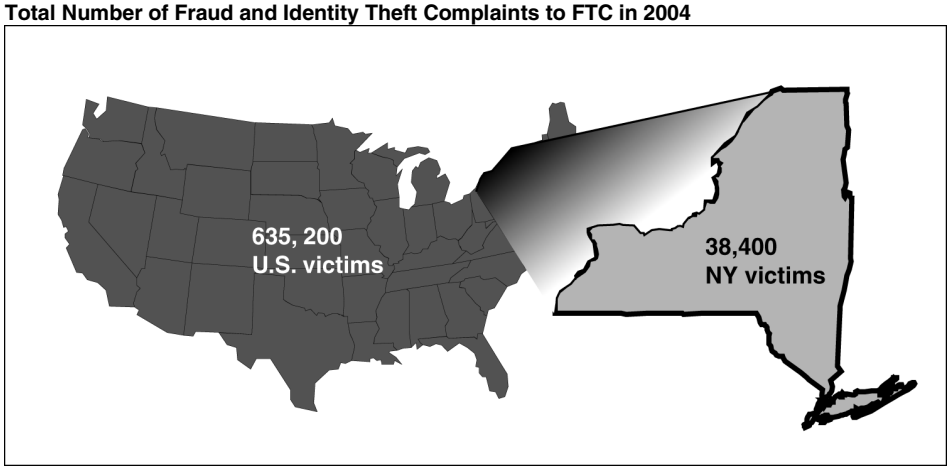
To view the full product, including the scope and methodology, click on the link above. For more information, contact Barbara Bovbjerg at (202) 512-7215 or bovbjergb@gao.gov.

What GAO Found

The public and private sector use of SSNs is widespread. Agencies at all levels of government frequently collect and use SSNs to administer their programs, verify applicants' eligibility for services and benefits, and conduct research and evaluations of their programs. Although some government agencies are taking steps to limit the use and display of SSNs, these numbers are still widely available in a variety of public records held by states, local jurisdictions, and courts. In addition, certain private sector entities that we have reviewed, such as information resellers, credit reporting agencies (CRAs), and health care organizations, also routinely obtain and use SSNs. These entities often obtain SSNs from various public sources or their clients and use SSNs for various purposes, such as building tools that aid in verifying an individual's identity or matching records from various sources.

Given the extent to which government and private sector entities use SSNs, Congress has enacted federal laws to restrict the use and disclosure of consumers' personal information, including SSNs. Many states have also enacted their own legislation to restrict the use and display of SSNs, focusing on public display restrictions, SSN solicitation, and customer notifications when SSNs are compromised. Furthermore, Congress has recently introduced consumer privacy legislation similar to enacted state legislation, which in some cases includes SSN restrictions. Although there is some consistency in the various proposed and enacted federal and state laws, gaps remain in protecting individuals' personal information from fraud and identity theft. Some federal agencies are beginning to collect statistics on identity theft crime, which appears to be growing. For example, recent statistics show that identity theft is increasing in New York. In 2004, Federal Trade Commission (FTC) statistics indicated that over 17,600 New Yorkers reported being a victim of identity theft, which is up from roughly 7,000 in 2001.

Total Number of Fraud and Identity Theft Complaints to FTC in 2004



Source: GAO, FTC analysis and Art Explosion.

Madam Chairwomen and Members of the Committees:

I am pleased to be here today to discuss ways to better protect the Social Security number (SSN). Although the SSN was created as a means to track workers' earnings and eligibility for Social Security benefits, it is now also a vital piece of information needed to function in American society. Because of its unique nature and broad applicability, the SSN has become the identifier of choice for public and private sector entities, and it is used for numerous non-Social Security purposes. Today, U.S. citizens need an SSN to pay taxes, obtain a driver's license, or open a bank account, among other things. For these reasons, the SSN is highly sought by individuals seeking to create false identities for purposes such as fraudulently obtaining credit, violating immigration laws, or fleeing the criminal justice system.

Recent statistics suggest that the incidence of identity theft is rapidly growing.[1] The Federal Trade Commission (FTC) estimated that over a one-year period nearly 10 million people—or 4.6 percent of the U.S. adult population—discovered that they were victims of some form of identity theft, translating into reported losses exceeding $50 billion. Identity theft also appears to be a serious and growing crime in New York. In 2004, FTC statistics indicated that over 17,600 New Yorkers reported being victims of identity theft, up from roughly 7,000 in 2001. However, an FTC survey found that most victims of identity theft do not report the crime. Therefore, the total of number of identity thefts is unknown.

Although there are enacted laws to protect the security of personal information, the continued use of and reliance on SSNs by public and private sector entities and the potential for misuse underscore the importance of identifying areas that can be further strengthened. Accordingly, you asked us to speak about the use of SSNs and the federal and state laws that regulate such use. My remarks today will focus on describing the (1) public use of SSNs, (2) the use of SSNs by certain private sector entities, and (3) federal and state laws regulating the use of SSNs and identity theft. My testimony is based on reports GAO has done for multiple congressional committees over the last several years.

[1] GAO, *Identity Theft: Prevalence and Cost Appear to Be Growing*, GAO-02-363 (Washington, D.C.: March 2002).

In summary, SSN use is widespread. Agencies at all levels of government frequently collect and use SSNs to administer their programs, verify applicants' eligibility for services and benefits, and perform research and evaluations of their programs. Although some government agencies are taking steps to limit the use and display of SSNs, these numbers are still available in a variety of public records held by states, local jurisdictions, and courts.

Certain private sector entities that we have reviewed, such as information resellers, credit reporting agencies (CRAs), and health care organizations also routinely obtain and use SSNs.[2] These entities often obtain SSNs from various public sources or their clients wishing to use their services. We found that these entities used SSNs for various purposes, such as to build tools that verify an individual's identity or match existing records.

A number of federal laws have been enacted to restrict the use and disclosure of consumers' personal information, including SSNs. In addition, many states have enacted their own legislation to restrict the use and display of SSNs on items such as identification cards, and require entities to notify customers of unauthorized access or use of their personal information. In the last year, Congress also has introduced consumer privacy legislation similar to enacted state legislation, which in some cases includes SSN restrictions. To date, enacted federal and state laws provide various ways to protect individual's personal information and prevent identity theft. However, while there is some consistency in the various laws protecting consumer personal information, no single law comprehensively regulates SSN use and protections, and no agency has primary jurisdiction over consumer protections and identity theft.

Background

The Social Security Act of 1935 authorized the Social Security Administration (SSA) to establish a record-keeping system to manage the Social Security program, which resulted in the creation of the SSN.[3]

[2] Information resellers, sometimes referred to as information brokers, are businesses that specialize in amassing consumer information, such as SSNs, for informational services. CRAs, also known as credit bureaus, are agencies that collect and sell information about the creditworthiness of individuals. Health care organizations or health care insurers generally deliver services through a coordinated system that includes health care providers and health care plans.

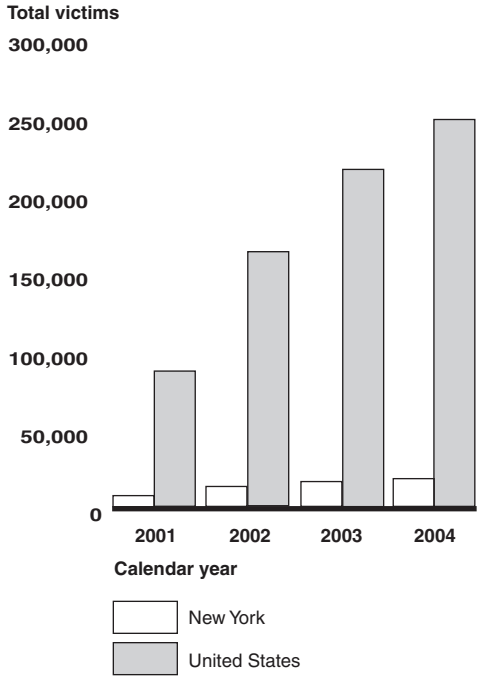
[3] The Social Security Act of 1935 created the Social Security Board, which was renamed the Social Security Administration in 1946.

Through a process known as enumeration, unique numbers are created for every person as a work and retirement benefit record. Today, SSA issues SSNs to most U.S. citizens, but they are also available to noncitizens lawfully admitted to the United States with permission to work. Lawfully admitted noncitizens may also qualify for a SSN for nonwork purposes when a federal, state, or local law requires that they have a SSN to obtain a particular welfare benefit or service. SSA staff collect and verify information from such applicants regarding their age, identity, citizenship, and immigration status.

Since its creation, the SSN has evolved beyond its original intended purpose. This is significant, because these numbers, along with a name and birth date, are the three pieces of information most often sought by identity thieves. Once a SSN is obtained fraudulently, it can then be used as "breeder" information to create additional false identification documents, such as driver's licenses.[4] As shown in figure 1, reported cases of identity theft are on the rise. In addition, the reported incidents of identity theft in New York have also risen, in an increase similar to the overall rise reported in the United States.

[4] United States Sentencing Commission, *Identity Theft Final Alert* (Washington, D.C.: Dec. 15, 1999).

Figure 1: Comparison between Reported New York Identity Theft Complaints and Overall United States Complaints



Source: FTC, Identity Theft Data Clearinghouse.

In 1998, Congress made identity theft a federal crime when it enacted the Identity Theft and Assumption Deterrence Act (Identity Theft Act).[5] The act made it a criminal offense for a person to "knowingly transfer, possess, or use without lawful authority," another person's means of identification "with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of federal law, or that constitutes a felony under any applicable state or local law." Under the act, a name or SSN is considered a "means of identification," and a number of cases have been prosecuted under this law.

The Identity Theft Act mandated a specific role for FTC in combating identity theft. To fulfill the mandate, FTC is collecting identity theft complaints and assisting victims through a telephone hotline and a dedicated Web site; maintaining and promoting the Identity Theft Data Clearinghouse, a centralized database of victim complaints that serves as

[5] Pub. L. No. 105-318, codified in part at 18 U.S.C. §1028.

an investigative tool for law enforcement; and providing outreach and education to consumers, law enforcement, and industry. According to FTC, it receives roughly 15,000 to 20,000 contacts per week on the hotline, via its Web site, or through the mail from victims and consumers who want to avoid becoming victims. FTC has said that the callers to its hotline receive counseling from trained personnel who provide information on prevention of identity theft and also inform victims of the steps to take to resolve the problems resulting from the misuse of their identities.

The increased availability and aggregation of personal information, including SSNs, has exposed SSNs to potential misuse, and in some cases, identity theft. Over the last year, several large companies' databases containing personal information were compromised, but the extent to which identity theft resulted from these reported security breaches is unknown. However, the identity theft crimes that have occurred illustrate how aggregated personal information can be vulnerable. For example, a help desk employee at a New York-based software company, which provided software to its clients to access consumer credit reports, stole the identities of up to 30,000 individuals by using confidential passwords and subscriber codes of the company's customers. The former employee reportedly sold these identities for $60 each. Furthermore, given the explosion of Internet use and the ease with which personally identifiable information is accessible, individuals looking to steal someone's identity are increasingly able to do so. In our work, we identified a case where an individual obtained the names and SSNs of high-ranking U.S. military officers from a public Web site, and used those identities to apply online for credit cards and bank credit.

Public Sector Entities Use SSNs, and Some Agencies Limit Their Display

As required by a number of federal laws and regulations, agencies at all levels of government frequently collect and use SSNs to administer their programs, to link data for verifying applicants' eligibility for services and benefits, and to conduct program evaluations. We have also found that SSNs are widely available in a variety of public records held by states, local jurisdictions, and courts. However, some government agencies are taking steps to limit the use and display of SSNs in hopes of preventing the proliferation of false identities.

Public Sector Entities Are Required by Laws and Regulations to Collect SSNs, and They Use Them for Various Purposes

As required by a number of federal laws and regulations, SSNs are widely used by federal, state, and county government agencies when they provide services and benefits to the public.[6] For example, the Personal Responsibility and Work Opportunity Reconciliation Act of 1996 mandates that, among other things, states have laws in place to require the collection of SSNs on driver's license applications. Such laws and regulations have contributed to the widespread use of SSNs by government agencies, because these numbers serve as a unique identifier for such government-related activities like paying taxes.

Government agencies use SSNs for a variety of reasons. We have found that agencies typically used the SSN to manage their records and to facilitate data sharing to verify an applicant's eligibility for services and benefits.[7] For example, agency officials at all levels of government we surveyed reported using SSNs for internal administrative purposes, which included activities such as identifying, retrieving, and updating records. In addition, agencies reported sharing SSNs and other personal information to collect debts owed the government and conduct or support research and evaluations as well as using employees' SSNs for activities such as payroll, wage reporting, and providing employee benefits.

Government agencies also use SSNs to ensure program integrity. For example, agencies may use SSNs to match records with state and local correctional facilities to identify individuals for whom the agency should terminate benefit payments. In addition, SSNs are sometimes used for statistics, research, and evaluation. For example, the Bureau of the Census prepares annual population estimates for states and counties using individual income tax return data linked over time by SSNs to determine immigration rates between localities.[8] SSNs also provide government agencies and others with an effective mechanism for linking data on

[6] GAO, *Social Security Numbers: Government and Commercial Use of the Social Security Number Is Widespread*, GAO/HEHS-99-28 (Washington, D.C.: February 1999), and GAO, *Social Security Numbers: Government Benefits from SSN Use, but Could Provide Better Safeguards*, GA0-02-352 (Washington, D.C.: May 2002).

[7] GA0-02-352.

[8] The Bureau of the Census is authorized by statute to collect a variety of information and is prohibited from making it available, except in certain circumstances.

program participation with data from other sources to help evaluate the outcomes or effectiveness of government programs.[9]

SSNs Are Widely Available in Public Records Held by States, Local Jurisdictions, and Courts, but Many of These Agencies Are Taking Steps to Limit Display

SSNs are publicly available throughout the United States, primarily at the state and local levels of government.[10] On the basis of a survey of federal, state, and local governments, we reported in 2004 that state agencies in 41 states and the District of Columbia were displaying SSNs in public records; this was also true in 75 percent of U.S. counties.[11] We also found that while the number and type of records in which SSNs were displayed varied greatly across states and counties, SSNs were most often found in court and property records. According to our survey, only four New York state agencies reported collecting SSNs for their operations, and none made them available to the general public.

Public records displaying SSNs are stored in multiple formats that vary by different levels of government. State government offices tended to store such records electronically, while most local government records were stored on microfiche or microfilm. However, our survey found that public access to such records was often limited to inspection of the individual paper copy or request by mail.[12]

According to our survey, few state agencies make public records available on the Internet, but as many as several hundred counties do so. However, few state or local offices reported any plans to significantly expand Internet access to public records that display SSNs. Judging from our

[9] The statistical and research communities refer to the process of matching records containing SSNs for statistical or research purposes as "record linkage." See GAO, *Record Linkage and Privacy: Issues in Creating New Federal Research and Statistical Information*, GAO-01-126SP (Washington, D.C.: April 2001).

[10] Not all records held by government or public agents are "public" in terms of their availability to any inquiring person. For example, adoption records are generally sealed. Personnel records are often not readily available to the public, although newspapers may publish the salaries of high elected officials. There is no common definition of public records. However, we define public records as those records generally made available to the public in their entirety for inspection by a federal, state, or local government agency. Such documents are typically accessed in a public reading room or clerk's office or on the Internet.

[11] GAO, *Social Security Numbers: Governments Could Do More To Reduce Display in Public Records and on Identity Cards*, GAO-05-59 (Washington, D.C.: November 2004).

[12] GAO-05-59.

survey results, only four state agencies indicated plans to make such records available on the Internet, and one agency planned to remove records displaying SSNs from Internet access.

Our survey results also showed that state offices were taking measures to change the way in which they displayed or shared SSNs in public records. For example, we found that many state agencies had restricted access to or redacted—covered or otherwise hidden from view—SSNs from public versions of records. Specific restrictions and other actions state agencies reported taking included blocking or removing SSNs from electronic versions of records, allowing individuals identified in the record to request removing their SSN from the publicly available version, replacing SSNs with alternative identifiers, and restricting access only to individuals identified in the records.

Certain Private Sector Entities Routinely Obtain and Use SSNs

Private sector entities such as information resellers, credit reporting agencies, and health care organizations routinely obtain and use SSNs. Such entities obtain the SSNs from various public sources and their clients wishing to use their services. However, given the varied nature of SSN data found in public records, some reseller officials told us that they are more likely to rely on receiving SSNs from their business clients than they are on obtaining SSNs from public records. Because the SSN is a unique identifier, we found that these entities use SSNs for various purposes, such as building tools to aid in verifying an individual's identity or matching existing data.

Private Sector Entities Obtain SSNs from Public and Private Sources

Private sector entities such as information resellers, CRAs, and health care organizations generally obtain SSNs from various public and private sources. Large information resellers have told us they obtain SSNs from various public records, such as records of bankruptcies, tax liens, civil judgments, criminal histories, deaths, real estate transactions, voter registrations, and professional licenses. To gather SSNs from these records, resellers told us that they send employees to courthouses or other repositories to obtain hard copies of public records, if not easily obtainable on the Internet or public record publications. They also said that they sometimes obtain batch files of electronic copies of jurisdictional public records where available. However, given the varied nature of SSN data found in public records, some reseller officials said they are more

likely to rely on SSNs obtained directly from their clients, who would voluntarily provide such information for a specific service or product, than those found in public records.[13]

Like information resellers, CRAs also obtain SSNs from public and private sources. CRA officials have told us that they obtained SSNs from public sources, such as bankruptcy records. We also found that these companies obtained SSNs from other information resellers, especially those that specialized in obtaining information from public records. However, CRAs are more likely to obtain SSNs from businesses that subscribe to their services, such as banks, insurance companies, mortgage companies, debt collection agencies, child support enforcement agencies, credit grantors, and employment screening companies. Therefore, individuals who provide these businesses with their SSNs for reasons such as applying for credit would subsequently have their charges and payment transactions, accompanied by the SSN, reported to the CRAs.

Health care organizations, including health care insurance plans and providers, are less likely to obtain SSN data from public sources. Health care organizations typically obtained SSNs from either individuals themselves or from companies that offer health care plans. For example, subscribers or policyholders enrolled in a health care plan, provide their SSNs as part of their health care plan applications to their company or employer group. In addition to health care plans, health care organizations also included health care providers, such as hospitals. Such entities often collected SSNs as part of the process of obtaining information on insured people. However, health care provider officials told us that, particularly with hospitals, the medical record number is the primary identifier, rather than the SSN.

Private Sector Entities Use SSNs Mainly for Linking Data for Identity Verifications

Information resellers, CRAs, and health care organization officials all said that their companies used SSNs to link data for identity verifications. Most of the officials we spoke to said that the SSN is the single most important identifier available, because it is truly unique to an individual, unlike a name or address, which can change over an individual's lifetime. For example, we found that one large information reseller that specialized in information technology solutions had developed a customer verification data model that used SSNs to help financial institutions comply with

[13] GAO-04-11.

federal laws regarding "knowing your customer."[14] Most of the large information resellers' officials we spoke to said that although they obtained the SSN from their clients, they rarely provided SSNs to their customers. Furthermore, almost all of the officials said that they provided their clients a truncated SSN (e.g., xxx-xx-6789).

We also found that Internet-based information resellers—which provide investigative or background checks to anyone willing to pay a fee—used the SSN as a means to collect other information about an individual to verify their identity. These types of resellers were more dependent on SSNs than the large information resellers. In 2003, in an effort to determine what type of information we could obtain from these Internet-based resellers, our investigators accessed these sites, paid the fee, and supplied several Internet-based resellers with legitimate SSNs. Our investigators found that these resellers provided them with corresponding information based on the supplied SSNs, such as a name, address, telephone number, and on two occasions, a truncated SSN. Also, all but one reseller required our investigators to provide both the name and SSN of the person who was the subject of our inquiry. During our investigation, not one of the reviewed Internet-based resellers in any apparent way attempted to audit us, determine who we were, or verify that we were using the information for the permissible purpose we had indicated.[15]

CRAs used SSNs as the primary identifier of individuals, which enabled them to match the information they received from their clients with the information stored in their databases.[16] Because these companies had various commercial, financial, and government agencies furnishing data to them, the SSN was the primary factor that ensured that incoming data were matched correctly with an individual's information on file. For example, CRA officials said they used several factors to match incoming data with existing data, such as name, address, and financial account

[14] Under Section 326 of the USA PATRIOT Act, financial institutions must verify each new account holder's identity after opening an account in an effort to curtail money laundering and terrorist financing.

[15] GAO-04-11.

[16] We found that CRAs and information resellers can sometimes be the same entity, a fact that blurs the distinctions between the two types of businesses but does not affect the use of SSNs by these entities. Five of the six large information resellers we spoke to said they were also CRAs. Some CRA officials said that information reselling constituted as much as 40 percent of CRAs' business.

information. However, because of its uniqueness, they said that they use the SSN as a primary means to match data.

We also found that health care organizations used the SSN to help verify identities. These organizations used SSNs, along with other information, such as name, address, and date of birth, to determine a member's identity. Health care officials said that health care plans, in particular, used the SSN as the primary identifier, and it often became the customer's insurance number. Health care officials said that they used SSNs for identification purposes, such as linking an individual's name to an SSN to determine if premium payments have been made. They also used the SSN as an online services identifier, as an alternative policy identifier, and for phone-in identity verification. Health care organizations also used SSNs to tie family members together where family coverage is used,[17] to coordinate member benefits, and as a crosscheck for pharmacy transactions. Health care industry association officials also said that SSNs are used for claims processing, especially with regard to Medicare.

Federal and State Laws Limit Disclosure of Personal Information and Address Identity Theft

Certain federal laws have been enacted to restrict the use and disclosure of consumers' personal information, including SSNs. In addition to these federal laws, many states have enacted their own legislation to restrict the use and display of SSNs, focusing on public display restrictions, such as the display of SSNs on identification cards, SSN solicitation, and customer notifications when SSNs are compromised. In the last year, Congress has also introduced consumer privacy legislation similar to enacted state legislation, which in some cases includes SSN restrictions. In 1998, Congress enacted legislation that made identity theft a crime, and state legislatures have also enacted such legislation.

Federal and State Laws Limit the Use and Disclosure of Personal Information, Including SSNs

Certain federal and state laws have placed restrictions on entities' use and disclosure of consumers' personal information, including SSNs. At the federal level, such laws include the Fair Credit Reporting Act (FCRA), the Fair and Accurate Credit Transaction Act (FACTA), the Gramm-Leach-Bliley Act (GLBA), the Drivers Privacy Protection Act (DPPA), and the Health Insurance Portability and Accountability Act (HIPAA). As shown in

[17] During the enrollment process, subscribers have a number of options, one of which is deciding whether they would like single or family coverage. In cases where family coverage is chosen, the SSNs is the key piece of information generally allowing the family members to be linked.

table 1, these federal laws either restrict certain public and private sector entities from disclosing personally identifiable information to specific purposes or with whom the information is shared. See appendix II for more information on these laws.

Table 1: Aspects of Federal Laws That Affect Private Sector Disclosure of Personal Information

Federal laws	Restrictions
Fair Credit Reporting Act	Limits access to credit data that includes SSNs to those who have a permissible purpose under the law.
Fair and Accurate Credit Transactions Act	Amends FCRA to allow, among others things, consumers who request a copy of their credit report to also request that the first five digits of their SSN (or similar identification number) not be included in the file; requires consumer reporting agencies and any business that use a consumer report to adopt procedures for proper disposal.
Gramm-Leach-Bliley Act	Creates a new definition of personal information that includes SSNs and limits when financial institutions may disclose the information to nonaffiliated third parties.
Drivers Privacy Protection Act	Prohibits obtaining and disclosing SSNs and other personal information from a motor vehicle record except as expressly permitted under the law.
Health Insurance Portability and Accountability Act	Protects the privacy of health information that identifies an individual (including by SSNs) and restricts health care organizations from disclosing such information to others without the patient's consent.

Source: GAO analysis.

Many states have enacted their own legislation to restrict the use and display of SSNs by public and private sector entities. Similar to some of New York's proposed bills, several state statutes include provisions related to restricting the display of SSNs, the unnecessary collection of SSNs, and the disclosure of individual's SSN without their consent. See appendix III for some examples of states that have enacted such legislation.

Notably, in 2001, California enacted a law to restrict the use and display of SSNs.[18] The law generally prohibits companies and persons from engaging in certain activities, such as

- posting or publicly displaying SSNs,
- printing SSNs on cards required to access the company's products or
- services,
- requiring people to transmit an SSN over the Internet unless the connection is secure or the number is encrypted,

[18] Cal. Civ. Code § 1798.85 (2001).

- requiring people to log onto a Web site using an SSN without a password, or
- printing SSNs on anything mailed to a customer unless required by law or the document is a form or application.

After its enactment, California's Office of Privacy Protection published recommended practices for protecting the confidentiality of the SSN, which included reducing its collection, controlling institutional access to it, instituting safeguards to protect it, and holding employees accountable for protecting it. These recommendations applied to both public and private sector entities.

Subsequently, several states have enacted laws restricting the use or display of SSNs. Specifically, we have identified 11 states—Arkansas, Arizona, Connecticut, Illinois, Maryland, Michigan, Minnesota, Missouri, Oklahoma, Texas, and Virginia—that have each passed laws similar to California's.[19] While some states, such as Arizona, have enacted virtually identical SSN use and display restrictions, other states have modified the restrictions in various ways. For example, unlike the California law, which prohibits the use of the full SSN, the Michigan statute prohibits the use of more than four sequential digits of the SSN. The Michigan law also contains a prohibition against the use of SSNs on identification and membership cards, permits, and licenses. Missouri's law includes a prohibition against requiring an individual to use his or her SSN as an employee number. Oklahoma's law is unique in that it only limits the ways in which employers may use their employees' SSNs, and does not apply more generally to other types of transactions and activities.

Some states have recently enacted other types of restrictions on the uses of SSNs as well. Both Arkansas and Colorado prohibit the use of a student's SSN as a student identification number.[20] New Mexico requires businesses that have acquired consumer SSNs to adopt internal policies to

[19] See Arkansas (Ark. Code Ann. § 4-86-107 (2005)); Arizona (Ariz. Rev. Stat. § 44-1373 (2004)); Connecticut (Conn. Gen. Stat. § 42-470 (2003)); Illinois (815 Ill. Comp. Stat. 505/2QQ (2004)); Maryland (Md. Code Ann., Com. Law § 14-3301 et seq. (2005)); Michigan (Mich. Comp. Laws § 445.81 et seq. (2004)); Minnesota (Minn. Stat. § 325E.59 (2005)); Missouri (Mo. Rev. Stat. § 407.1355 (2003)); Oklahoma (Okla. Stat. tit. 40, § 173.1 (2004)); Texas (Tex. Bus. & Com. Code Ann. 35.58 (2003)); and Virginia (Va. Code Ann. § 59.1-443.2 (2005)).

[20] Ark. Code Ann. § 6-18-208 (2005) and Colo. Rev. Stat. § 23-5-127 (2003).

limit access to authorized employees.[21] Texas recently enacted a law requiring businesses to properly dispose of business records that contain a customer's personal identifying information, which is defined to include SSNs.[22]

Other recent state legislation includes new restrictions on state and local government agencies. For example, South Dakota law prohibits the display of SSNs on all driver's licenses and nondriver's identification cards,[23] while Indiana law prohibits a state agency from releasing a SSN unless otherwise required by law.[24] In addition, a Nevada law requires governmental agencies, except in certain circumstances, to ensure that the SSNs recorded in their books and on their records are maintained in a confidential manner.[25]

We also identified three states that have passed legislation containing notification requirements in the event of a security breach, similar to the recently enacted New York law requiring such notifications. California requires a business or a California state agency to notify any California resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.[26] In the last year, this law forced several large companies to notify individuals that their information was compromised because of certain circumstances. Under a Nevada law, government agencies and certain persons who do business in the state must notify individuals if their personal information is reasonably believed to have been compromised.[27] Similarly, Georgia requires certain private sector entities to notify their customers if a security breach occurred that compromised their customers' personal information, such as their SSNs.[28]

[21] N.M. Stat. Ann. § 57-12B-1 et seq. (2003).

[22] Tex. Bus. & Com. Code Ann. 35.48 (2005).

[23] S.D. Codified Laws § 32-12-17.10 (2005); § 32-12-17.13 (2005).

[24] Ind. Code § 4-1-10-1 et seq. (2005).

[25] Nev. Rev. Stat. Chapter 239 (2005).

[26] Cal. Civ. Code § 1798.29 (2002); 1798.82 (2002).

[27] Nev. Rev. Stat. Chapter 239B; Chapter 603 (2005).

[28] Ga. Code Ann. § 10-1-910 et seq. (2005).

At the time of this writing, Congress is also considering consumer privacy legislation, which in some cases includes SSN restrictions. As of August 18, 2005, there were approximately 22 proposed bills pending before the U.S. House and Senate. In many cases, the provisions being considered mirrored provisions in enacted state laws. For example, some of the proposed legislation included prohibitions on the display of SSNs, similar to the concept of Colorado's law prohibiting the display of a person's SSN on a license, pass, or certificate, issued by a public entity, except under certain circumstances.[29] Several other pieces of proposed federal legislation address the solicitation of SSNs by public and private sector entities. For example, one proposed bill prohibits business entities from denying an individual goods or services for refusing to give an SSN for account record purposes. Some states, such as Texas, Maine, and Colorado, have also enacted SSN solicitation prohibitions or restrictions.[30]

In addition, some federal privacy legislation also proposed consumer safeguards, such as security freezes and prohibitions on the sale and purchase of SSNs. For example, some proposed federal legislation included provisions that allow consumers to place a security "credit" freeze on their information to bar lenders and others from reviewing their credit history.[31] Five proposed bills also introduced a prohibition on the sale or purchase of individual's SSNs by both public and private sector entities. In one instance, legislative provisions prohibit the sale of customer information to a nonaffiliated third party, unless customer consent is given. Additionally, roughly nine proposed pieces of federal legislation contain security breach notification requirements, and two proposed federal bills required the disposal of sensitive personal data, such as SSNs.

Finally, some of the proposed federal legislation would preempt state law and supersede some of the states' consumer protection statutes.[32]

[29] Colo. Rev. Stat. § 24-72.3-102 (2004).

[30] Texas (Tex. Bus. & Com. Code Ann. § 35.581 (2005)); Maine (Me. Rev. Stat. Ann. tit. 10, §1272-B (2003)); and Colorado (Colo. Rev. Stat. § 24-33-110 (2004)).

[31] Because few lenders will issue credit without first seeing a credit report, it has been argued that this may help thwart identity thieves from opening fraudulent accounts using the name of someone who has frozen his or her credit reports.

[32] Federal preemption may arise whenever Congress enacts a statute in an area in which state legislatures have acted or have the authority to act. Determining whether a federal law preempts state law may require judicial resolution and turns on whether Congress intended that the federal law override state law.

According to some privacy advocates, historically, federal privacy laws have not preempted stronger state protections or enforcement efforts, and they have said that the proposed preemption would reduce some consumer privacy protections. However, some private sector entities have noted the difficulty of doing business within the framework of many different state laws and have advocated a uniform federal standard. See appendix IV for a list of proposed federal legislation we identified.

Federal and State Legislation Exist to Address Identity Theft

The Identity Theft Act of 1998, the primary federal statute, criminalizes fraud in connection with the theft and unlawful misuse of personal identifiable information. The Identity Theft Act establishes the person whose identity is stolen as a "true" victim and enables that victim to seek restitution if there is a conviction. Previously, only the credit grantors who suffered monetary losses were considered victims. Additionally, Congress enacted FACTA in 2003, which amended FCRA and added several provisions that were aimed at identity theft prevention and victim assistance. For example, Congress enacted provisions that allow an individual to obtain a free copy of his or her credit report annually for self-monitoring.

Many states have laws prohibiting the theft of identity information, and where specific identity theft laws do not exist, the practices may be prohibited under other state laws or the states may be considering such legislation. For example, New York law makes identity theft a crime.[33] In other states, identity theft statutes also address specific crimes committed under a false identity. For example, Arizona law prohibits any person from using deceptive means to alter certain computer functions or use software to collect bank information, take control of another person's computer, or prevent the operator from blocking the installation of specific software.[34] In addition, Idaho law makes it unlawful to impersonate any state official to seek, demand, or obtain personally identifiable information of another person.[35] Furthermore, some states have also included identity theft victim assistance provisions in their laws. For example, Washington law requires police and sheriff's departments to provide a police report or original

[33] N.Y. Penal Law § 190.77-190.84 (2002).

[34] Ariz. Rev. Stat. § 44-7301 et seq. (2005).

[35] Idaho Code § 18-3126A (2005).

incident report at the request of any consumer claiming to be a victim of identity theft.[36]

Because identity theft is typically not a stand-alone crime, but rather a component of one or more complex crimes, such as computer fraud, credit card fraud, or mail fraud, the federal laws that apply vary.[37] For example, with the theft of identity information, a perpetrator may commit computer fraud when using a stolen identity to fraudulently obtain credit on the Internet. Computer fraud may also be the primary vehicle used to obtain identity information when the offender obtains unauthorized access to another computer or Web site to obtain such information. As a result, the offender may be charged with both identity theft and computer fraud.

According to a Department of Justice official, the investigation of identity theft is labor intensive and individual cases are usually considered to be too small for federal prosecution. Moreover, perpetrators usually prey on multiple victims in multiple jurisdictions. Consequently, a number of federal law enforcement agencies can have a role in investigating identity theft crimes. How the thief uses an individual's identity usually dictates which federal agency has jurisdiction in the case. For example, if an individual finds that an identity thief has stolen the individual's mail to obtain credit cards, bank statements, or tax information, the victim should report the crime to the U.S. Postal Inspection Service, the law enforcement arm of the U.S. Postal Service. In addition, violations are investigated by other federal agencies, such as the Social Security Administration Office of the Inspector General, the U.S. Secret Service, the Federal Bureau of Investigation (FBI), the U.S. Securities and Exchange Commission, the U.S. Department of State, the U.S. Department of Education Office of Inspector General, and the Internal Revenue Service. The Department of Justice prosecutes federal identity theft cases. Table 2 highlights some of the jurisdictional responsibilities of some federal agencies.

[36] Wash. Rev. Code § 19.182.160 (2005) [not yet codified].

[37] 18 U.S.C. §1028(a)(1)-(6); 18 U.S.C. §1029; 18 U.S.C. §1341.

Table 2: List of Federal Agencies with Some Identity Theft Jurisdiction

Federal agency	Jurisdictional identity theft highlights
Social Security Administration's Office of the Inspector General	Investigates SSN misuse involving the buying and selling of SSN cards.
U.S. Secret Service	Investigates crimes associated with financial institutions; investigations include bank fraud, access device fraud involving credit and debit cards, telecommunications and computer crimes, fraudulent identification, fraudulent government and commercial securities, and electronic funds transfer fraud.
Federal Bureau of Investigation	Investigates cases of identity theft; investigations can include bank fraud, mail fraud, wire fraud, bankruptcy fraud, insurance fraud, and fraud against the government. In addition, FBI sponsors a national Identity Theft Working Group, where participants from law enforcement, federal regulatory bodies, and the financial services industry meet regularly to discuss identity theft-related issues.
U.S. Securities and Exchange Commission	Investigates investment fraud in instances where an identity thief has tampered with securities investments or brokerage accounts.
U.S. Department of State	Investigates passport fraud in instances where a passport is used fraudulently.
U.S. Department of Education Office of Inspector General	Investigates fraudulent student loan activity.
Internal Revenue Service	Investigates tax fraud where identity theft may relate directly to tax records.

Source: GAO analysis.

Conclusions

SSNs are still widely used and publicly available, although they have become less so in the last year. Given the significance of the SSN in committing fraud or stealing a person's identity, it is imperative that steps be taken to protect this number. This is especially true as information technology makes it easier to access individuals' personal information. The increased availability and aggregation of personal information in public and private sector databases and via the Internet has provided new opportunities for individuals to engage in fraudulent activities. Without proper regulations or safeguards in place, SSNs will remain vulnerable to misuse, thus adding to the growing number of identity theft victims.

Current federal restrictions on SSNs and other personal information are industry specific and do not apply broadly. Certain industries, such as the financial services industry, are required to protect individuals' personal information while others are not. In addition, given the industry specific nature of federal laws, no single federal agency has responsibility for ensuring the protection of individuals' personal information. Consequently, gaps remain at the federal level in protecting individuals' personal information.

State legislatures have also placed restrictions on SSNs by enacting laws that restrict the use and display of SSNs and prohibit the theft of

individuals' personal information. However, gaps also remain at the state level because not all states have enacted laws to protect individuals' personal information. In addition, while there is some consistency among enacted state laws, privacy protections and identity theft prevention varies with the focus of each state's legislature.

As legislatures at both the federal and state level continue to enact laws to protect individuals' personal information, gaps in protections will need to be determined and addressed in order to prevent SSNs and other personal information from being misused. We are pleased that the Assembly is concentrating on this important policy issue, and we hope our work will be helpful to you. That concludes my testimony, and I would be pleased to respond to any questions.

Contacts and Acknowledgments

For further information regarding this testimony, please contact Barbara D. Bovbjerg, Director or Tamara Cross, Assistant Director, Education, Workforce, and Income Security at (202) 512-7215. Individuals making key contributions to this testimony include Margaret Armen, Pat Bernard, Mindy Bowman, Richard Burkard, Rachael Chamberlin, Amber Edwards, Jason Holsclaw, Joel Marus, and Sheila McCoy.

Appendix I: Federal Statutes That Authorize or Mandate the Collection and Use of SSNs by Government Entities

Federal statute	General purpose for collecting or using the Social Security number (SSN)	Government entity and authorized or required use
Tax Reform Act of 1976 42 U.S.C. 405(c)(2)(c)	General public assistance programs, tax administration, driver's license, motor vehicle registration	Authorizes states to collect and use SSNs in administering any tax, general public assistance, driver's license, or motor vehicle registration law
Food Stamp Act of 1977 as amended 7 U.S.C. 2025(e)(1)	Food Stamp Program	Mandates the Secretary of Agriculture and state agencies to require SSNs for program participation
Deficit Reduction Act of 1984 42 U.S.C. 1320b-7(a) and (b)	Eligibility for federal benefits under state administered program	Requires that, as a condition of eligibility for Medicaid benefits and other federal benefit programs, applicants for and recipients of these benefits furnish their SSNs to the state administering program
Comprehensive Omnibus Budget Reconciliation Act of 1986 20 U.S.C. 1091(a)(4)	Financial Assistance	Requires students to provide their SSNs when applying for federal student financial aid
Housing and Community Development Act of 1987 42 U.S.C. 3543(a)	Eligibility for the Department of Housing and Urban Development programs	Authorizes the Secretary of the Department of Housing and Urban Development to require program applicants and participants to submit their SSNs as a condition of eligibility
Family Support Act of 1988 42 U.S.C. 405(c)(2)(C)(ii)	Issuance of birth certificates	Requires states to obtain parents' SSNs before issuing a birth certificate unless there is good cause for not requiring the number
Technical and Miscellaneous Revenue Act of 1988 42 U.S.C. 405(c)(2)(D)(i)	Blood donation	Authorizes states and political subdivisions to require that blood donors provide their SSNs
Food, Agriculture, Conservation, and Trade Act of 1990 42 U.S.C. 405(c)(2)(C)(iii)	Retail and wholesale businesses participation in food stamp program	Authorizes the Secretary of Agriculture to require the SSNs of officers or owners of retail and wholesale food concerns that accept and redeem food stamps
Omnibus Budget Reconciliation Act of 1990 38 U.S.C. 5101(c)	Eligibility for Veterans Affairs compensation or pension benefits programs	Authorizes the Secretary of Veterans Affairs to require individuals to provide their SSNs to be eligible for Department of Veterans Affairs' compensation or pension benefits programs
Social Security Independence and Program Improvements Act of 1994 42 U.S.C. 405(c)(2)(E)(ii)	Eligibility of potential jurors	Authorizes states and political subdivisions of states to use SSNs to determine eligibility of potential jurors

Federal statute	General purpose for collecting or using the Social Security number (SSN)	Government entity and authorized or required use
Personal Responsibility and Work Opportunity Reconciliation Act of 1996 42 U.S.C. 666(a)(13)	Various license applications, divorce and child support documents, death certificates	Mandates that states have laws in effect that require collection of SSNs on applications for driver's licenses and other licenses; requires placement in the pertinent records of the SSN of the person subject to a divorce decree, child support order, paternity determination; requires SSNs on death certificates
Higher Education Act Amendments of 1998 20 U.S.C. 1090(a)(7)	Financial assistance	Authorizes the Secretary of Education to request SSNs of parents of dependent students applying for federal student financial aid
Internal Revenue Code (various amendments) 26 U.S.C. 6109	Tax returns	Authorizes the Commissioner of the Internal Revenue Service to require that individuals include their SSNs on tax returns

Source: GAO review of applicable federal laws.

Appendix II: Federal Laws Affecting Information Resellers, CRAs, and Health Care Organizations

Fair Credit Reporting Act (FCRA)

Congress has limited the use of consumer reports to protect consumers' privacy. All users must have a permissible purpose under FCRA to obtain a consumer report. Some of these permissible purposes are

- for the extension of credit as a result of an application from a consumer or the review or collection of a consumer's account, for employment purposes, including hiring and promotion decisions, where the consumer has given written permission;
- for the underwriting of insurance as a result of an application from a consumer;
- when there is a legitimate business need, in connection with a business transaction that is initiated by the consumer; and
- to review a consumer's account to determine whether the consumer continues to meet the terms of the account.

Fair and Accurate Credit Transaction Act (FACTA)

FACTA added new sections to FCRA intended primarily to help consumers prevent and combat identity theft. Some of the provisions include

- allowing consumers to obtain a free copy of their credit report,
- the truncation of credit and debit card account numbers and the truncation of SSNs if requested,
- requirements for the disposal of consumer report information or records,
- obligations for furnishers of information to investigate and correct inaccurate information recorded in a consumer's credit report.

Gramm-Leach-Bliley Act (GLBA)

GLBA requires companies to give consumers privacy notices that explain the institutions' information-sharing practices. In turn, consumers have the right to limit some, but not all, sharing of their nonpublic personal information. Financial institutions are permitted to disclose consumers' nonpublic personal information without offering them an opt-out right in some of the following circumstances:

- to effect a transaction requested by the consumer in connection with a financial product or service requested by the consumer; maintaining or servicing the consumer's account with the financial institution or another entity as part of a private label credit card program or other extension of credit; or a proposed or actual securitization, secondary market sale, or similar transaction;

- to protect the confidentiality or security of the consumer's records; to prevent actual or potential fraud, for required institutional risk control or for resolving customer disputes or inquiries, to persons holding a legal or beneficial interest relating to the consumer, or to the consumer's fiduciary;

- to the extent specifically permitted or required under other provisions of law and in accordance with the Right to Financial Privacy Act of 1978, to law enforcement agencies, self-regulatory organizations, or for an investigation on a matter related to public safety;

- to a consumer reporting agency in accordance with the Fair Credit Reporting Act or from a consumer report reported by a consumer reporting agency;

- to comply with federal, state, or local laws; an investigation or subpoena; or to respond to judicial process or government regulatory authorities. Financial institutions are required by GLBA to disclose to consumers at the initiation of a customer relationship, and annually thereafter, their privacy policies, including their policies with respect to sharing information with affiliates and non-affiliated third parties.

Drivers Privacy Protection Act (DPPA)

The DPPA specifies a list of exceptions when personal information contained in a state motor vehicle record may be obtained and used. Some of these permissible purposes include

- for use by any government agency in carrying out its functions;

- for use in connection with matters of motor vehicle or driver safety and theft; motor vehicle emissions; motor vehicle product alterations, recalls, or advisories; motor vehicle market research activities, including survey research;

- for use in the normal course of business by a legitimate business, but only to verify the accuracy of personal information submitted by the individual to the business and, if such information is not correct, to

obtain the correct information but only for purposes of preventing fraud by pursuing legal remedies against, or recovering on a debt or security interest against, the individual;

- for use in connection with any civil, criminal, administrative, or arbitral proceeding in any federal, state, or local court or agency;
- for any other use specifically authorized under a state law, if such use is related to the operation of a motor vehicle or public safety.

Health Insurance Portability and Accountability Act (HIPAA)

The HIPAA privacy rule also defines some rights and obligations for both covered entities and individual patients and health plan members. Some of the highlights are

- Individuals must give specific authorization before health care providers can use or disclose protected information in most nonroutine circumstances, such as releasing information to an employer or for use in marketing activities.
- Covered entities will need to provide individuals with written notice of their privacy practices and patients' privacy rights. The notice will contain information that could be useful to individuals choosing a health plan, doctor, or other service provided. Patients will be generally asked to sign or otherwise acknowledge receipt of the privacy notice.

Covered entities must obtain an individual's specific authorization before sending them marketing materials.

Appendix III: Examples of Enacted State SSN Legislation Restricting Use

State (year passed)	Code section	Summary of key provisions
Arizona (2004)	Ariz. Rev. Stat. § 44-1373	Generally prohibits any person or entity from (1) intentionally communicating or otherwise making an individual's SSN available to the general public; (2) printing an individual's SSN on any card required to receive products or services; (3) requiring an individual to transmit his or her SSN over the Internet unless the number is encrypted or the connection is secure; (4) requiring the use of a SSN to access an Internet Web site unless a password or other security device is used; and (5) printing an individual's SSN on any material to be mailed to the individual, unless the inclusion of the SSN is required by law.
Arkansas (2005)	Ark. Code Ann. § 4-86-107	Generally prohibits any person or entity from (1) publicly posting or displaying an individual's SSN in any manner; (2) printing an individual's SSN on any card required to receive products or services; (3) printing an individual's SSN on a postcard or in any other manner by which the SSN is visible from the outside; and (4) requiring an individual to transmit his or her SSN over the Internet unless the number is encrypted or the connection is secure.
Arkansas (2005)	Ark. Code Ann. § 6-18-208	Generally prohibits schools and school districts from using, displaying, releasing, or printing a student's SSN or any part thereof on any report, ID card or badge, or any document that will be made available to the public, a student, or a student's parent or guardian without the express written consent of the parent, if the student is a minor, or the student if the student is 18 years of age or older.
California (2001)	Cal. Civ. Code § 1798.85	Generally prohibits any person or entity from (1) publicly posting or displaying an individual's SSN in any manner; (2) printing an individual's SSN on any card required to receive products or services; (3) requiring an individual to transmit his or her SSN over the Internet unless the number is encrypted or the connection is secure; (4) requiring the use of a SSN to access an Internet Web site unless a password or other security device is used; and (5) printing an individual's SSN on any material to be mailed to the individual, unless the inclusion of the SSN is required by law.
California (2004)	Cal. Fam. Code § 2024.5	Authorizes a petitioner or respondent to redact SSNs from pleadings, attachments, documents, or other material filed with the court pursuant to a petition for dissolution of marriage, annulment, or legal separation, except as specified. Requires that filing forms contain a notice of the right to redact SSNs.
Colorado (2003)	Colo. Rev. Stat. § 23-5-127	Requires each institution of higher education to assign a unique identifying number to each student enrolled at the institution starting. Prohibits the use of a student's SSN as the unique identifying number. Requires institutions of higher learning to take reasonable and prudent steps to ensure the privacy of students' SSNs.
Connecticut (2003)	Conn. Gen. Stat. § 42-470	Generally prohibits any person or entity, except government entities, from (1) publicly posting or displaying an individual's SSN in any manner; (2) printing an individual's SSN on any card required to receive products or services; (3) requiring an individual to transmit his or her SSN over the Internet unless the number is encrypted or the connection is secure; and (4) requiring the use of a SSN to access an Internet Web site unless a password or other security device is used.

State (year passed)	Code section	Summary of key provisions
Connecticut (2004)	Conn. Gen. Stat. § 8-64b	Prohibits entities purchasing all or part of a housing project from a housing authority from disclosing to the public tenant SSNs or bank account numbers contained in lease agreements.
Delaware (2004)	Del. Code Ann., tit. 7 § 503	Insures that SSNs provided by hunting, fishing, and trapping license holders would not be released to the public.
Florida (2005)	Fla. Stat. ch. 97.0585[1]	Exempts a voter's SSN, driver's license number, state identification number, and signature from the public disclosure laws.
Georgia (2004)	Ga. Code Ann. § 50-18-72	Provides that public disclosure shall not be required for records that would reveal the home address or telephone number, SSN, or insurance or medical information of certain state employees.
Hawaii (2005)	Haw. Rev. Stat. § 12-3[2]	Prohibits the use of a registered voter's SSN as identifying information on candidate nomination papers.
Illinois (2004)	815 Ill. Comp. Stat. 505/2QQ[3]	Generally prohibits any person or entity from (1) publicly posting or displaying an individual's SSN in any manner; (2) printing an individual's SSN on any card required to receive products or services; (3) requiring an individual to transmit his or her SSN over the Internet unless the number is encrypted or the connection is secure; (4) requiring the use of a SSN to access an Internet Web site unless a password or other security device is used; and (5) printing an individual's SSN on any material to be mailed to the individual, unless the inclusion of the SSN is required by law.
Indiana (2005)	Ind. Code § 4-1-10-1 et seq.	Generally prohibits a state agency from disclosing an individual's SSN, unless otherwise required by law.
Indiana (2005)	Ind. Code § 9-24-6-2; § 9-24-9-2; § 9-24-11-5; § 9-24-16-3	Removes the requirement that SSNs be displayed on commercial driver's licenses. Requires that applications for driver's licenses, permits, and identification cards allow applicants to indicate whether the SSN or another distinguishing number shall be used on the license, permit, or identification card, and prohibits the use of the SSN if the applicant does not indicate a preference.
Louisiana (2004)	La. Rev. Stat. Ann. 9:5141; 35:17	Requires that only last four digits of SSN appear on mortgage records and notarial acts.

[1] As currently codified, Fla. Stat. ch. 97.0585 does not contain the provisions summarized here. The changes will take effect on January 1, 2006.

[2] Not yet codified.

[3] The provisions summarized here are codified, but will not take effect until July 1, 2006.

State (year passed)	Code section	Summary of key provisions
Maryland (2005)	Md. Code Ann., Com. Law § 14-3301 et seq.[4]	Generally prohibits any person or entity, except government entities, from (1) publicly displaying or posting an individual's SSN; (2) printing an individual's SSN on any card required to receive products or services; (3) requiring an individual to transmit his or her SSN over the Internet unless the number is encrypted or the connection is secure; (4) initiating the transmission of an individual's SSN unless the connection is secure; (5) requiring the use of a SSN to access an Internet Web site unless a password or other security device is used; (6) printing an individual's SSN on any material to be mailed to the individual, unless the inclusion of the SSN is required by law; (7) electronically transmitting an individual's SSN unless the connection is secure or the SSN is encrypted; and (8) faxing an individual's SSN to that individual.
Michigan (2004)	Mich. Comp. Laws § 445.81 et seq.	Generally prohibits any person or entity from (1) publicly posting or displaying more than four sequential digits of an individual's SSN; (2) using more than four sequential digits of an individual's SSN as the primary account number for an individual; (3) visibly printing more than four sequential digits of an individual's SSN on any identification badge or card, membership card, or permit or license; (4) requiring an individual to transmit more than four sequential digits of his or her SSN over the Internet unless the number is encrypted or the connection is secure; (5) requiring the use of more than four sequential digits of an individual's SSN to access an Internet Web site unless a password or other security device is used; and (6) printing more than four sequential digits of an individual's SSN on any material to be mailed to the individual.
Minnesota (2005)	Minn. Stat. § 325E.59[5]	Generally prohibits any person or entity, except government entities, from (1) publicly posting or displaying an individual's SSN in any manner; (2) printing an individual's SSN on any card required to receive products or services; (3) requiring an individual to transmit his or her SSN over the Internet unless the number is encrypted or the connection is secure; (4) requiring the use of a SSN to access an Internet Web site unless a password or other security device is used; and (5) printing an individual's SSN on any material to be mailed to the individual, unless the inclusion of the SSN is required by law.
Missouri (2003)	Mo. Rev. Stat. § 407.1355	Generally prohibits any person or entity, except government entities, from (1) publicly displaying or posting an individual's SSN, including any activity that would make the SSN available to an individual's coworkers, (2) requiring an individual to transmit his or her SSN over the Internet unless the number is encrypted or the connection is secure, (3) requiring the use of a SSN to access an Internet Web site unless a password or other security device is used, and (4) requiring an individual to use his or her SSN as an employee number.

[4] Not yet codified.

[5] Not yet codified.

State (year passed)	Code section	Summary of key provisions
Nevada (2005)	Nev. Rev. Stat. Chapter 239; Chapter 239B; Chapter 603	Requires a governmental entity, except in certain circumstances, to ensure that SSNs in its books and records are maintained in a confidential manner. Prohibits the inclusion of SSNs in certain documents that are recorded, filed, or otherwise submitted to a governmental agency. Requires governmental agencies or certain persons who do business in the state to notify individuals if personal information is reasonably believed to have been acquired by an unauthorized person.
New Jersey (2005)	N.J. Stat. Ann. § 47:1-16	Prohibits any person, including any public or private entity, from printing or displaying in any manner an individual's SSN on any document intended for public recording with any county recording authority. Provides that, in the case of certain documents, the county recording authority is authorized to delete, strike, obliterate or otherwise expunge an SSN that appears on the document without invalidating it.
New Mexico (2003)	N.M. Stat. Ann. § 57-12B-1 et seq.	Prohibits a business from requiring a consumer's SSN as a condition for the consumer to lease or purchase products, goods or services from the business. A company acquiring or using SSNs of consumers shall adopt internal policies that (1) limit access to the SSNs to those employees authorized to have access to that information to perform their duties; and (2) hold employees responsible if the SSNs are released to unauthorized persons.
North Dakota (2003)	N.D. Cent. Code § 39-06-14	Prohibits the use of SSNs on driver's licenses.
Oklahoma (2004)	Okla. Stat. tit. 40, § 173.1	Generally prohibits employing entity from (1) publicly displaying or posting an employee's SSN; (2) printing the SSN of an employee on any card required for the employee to access information, products, or services; (3) requiring an employee to transmit his or her SSN over the Internet unless the number is encrypted or the connection is secure; (4) requiring an employee to use an SSN to access an Internet Web site unless a password or other security device is used; and (5) printing an employee's SSN on any materials mailed to the employee, unless the SSN is required by law to be in the materials.
Rhode Island (2004)	R.I. Gen. Laws § 6-13-19	Prohibits any person, firm, corporation, or other business entity that offers discount cards for purchases made at any business maintained by the offeror from requiring that a person who applies for a discount card furnish his or her SSN or driver's license as a condition precedent to the application for the consumer discount card.
South Carolina (2004)	S.C. Code Ann. § 7-5-170	SSNs provided in voter registration applications must not be open to public inspection.
South Dakota (2005)	S.D. Codified Laws § 32-12-17.10; § 32-12-17.13	Prohibits the display of SSNs on driver's licenses or non-driver's identification cards and the use of electronic barcodes containing SSN data.
Texas (2005)	Tex. Bus. & Com. Code Ann. 35.48	Requires that businesses disposing of business records containing a customer's personal identifying information must modify, by shredding, erasing, or other means, the personal identifying information to make it unreadable or undecipherable.

State (year passed)	Code section	Summary of key provisions
Texas (2003)	Tex. Bus. & Com. Code Ann. 35.58	Generally prohibits any person or entity, except government entities, from (1) intentionally communicating an individual's SSN to the general public; (2) printing an individual's SSN on any card required to access or receive products or services; (3) requiring an individual to transmit his or her SSN over the Internet unless the number is encrypted or the connection is secure; (4) requiring the use of a SSN to access an Internet Web site unless a password or other security device is used; and (5) printing an individual's SSN on any materials mailed to the individual, unless the SSN is required by law to be in the materials.
Texas (2003)	Tex. Elec. Code Ann. § 13.004	Provides that a SSN, Texas driver's license number, or number of a personal identification card furnished on a voter registration application is confidential and does not constitute public information. Requires the registrar to ensure that such personal data are excluded from disclosure.
Utah (2004)	Utah Code Ann. § 31A-21-110	Prohibits insurers from publicly posting an individual's SSN in any manner or printing an individual's SSN on any card required for the individual to access products or services provided or covered by the insurer.
Virginia (2005)	Va. Code Ann. § 59.1-443.2	Generally prohibits any person or entity from (1) intentionally communicating an individual's SSN to the general public; (2) printing an individual's SSN on any card required to access or receive products or services; (3) requiring the use of a SSN to access an Internet Web site unless a password or other security device is used; and (4) mailing a package with the SSN visible from the outside.
Wisconsin (2003)	Wis. Stat. § 36.32	Prohibits private institutions of higher education from assigning to any student an identification number that is identical to or incorporates the student's SSN.
West Virginia (2003)	W. Va. Code § 17E-1-11	Removes the requirement that a SSN appear on commercial driver's license.

Source: GAO analysis.

Appendix IV: List of Proposed Federal Legislation as of August 2005

Bill Number	Title	Selected Provisions
H.R. 3375	Financial Data Security Act of 2005	Consumer must be notified if investigation reveals that information would cause substantial inconvenience or harm.
H.R. 3374	Consumer Notification and Financial Data Protection Act of 2005	Provide written notice to consumer whose sensitive financial personal information was compromised in a data breach; sensitive financial personal data must be properly disposed of so that such information or compilation cannot practicable be read or reconstructed.
S. 1408	Identity Theft Protection Act	If a covered entity determines that a breach of security affects sensitive personal information, the entity must notify each individual; a consumer can request a security freeze on his/her credit report; no covered entity may solicit any SSN from an individual unless there is a specific use of the SSN for which no other identifier can be reasonably used; SSNs can not be printed on (1) any identification card or tag (2) driver's licenses.
H.R. 3140	Consumer Data Security and Notification Act of 2005	Amends the Fair Credit Reporting Act to cover any persons that communicates personally identifiable or financial information for compensation. Requires identity verification of any person requesting consumer reports. Protects nonpublic consumer information. Requires notice of security breach.
S. 1332	Personal Data Privacy and Security Act of 2005	No person may (1) display any individual's SSN to a third party without the voluntary and affirmatively expressed consent of such individual, (2) sell or purchase any SSN of an individual without the voluntary and affirmatively expressed consent of such individual, or (3) harvest SSNs from federal public records for the purpose of displaying or selling such number to the public.
S. 1336	Consumer Identity Protection and Security Act	Customer has the right to request that a consumer reporting agency place a security freeze on a private information file.
S. 810	SAFE-ID Act	Generally, prohibits business enterprises from disclosing personally identifiable information regarding U.S. residents to any branch, affiliate, subcontractor, or unaffiliated third party located in a foreign country.
S. 768	Comprehensive Identity Theft Prevention Act	In general, no person may solicit any SSN unless (1) the SSN is necessary for the normal course of business or (2) there is a specific use for the SSN for which no other identifying number can be used; no employer may display the SSN on any identification card issued to its employees; it shall be unlawful for any person to (1) sell or purchase an SSN or display to the general public an SSN or (2) obtain or use an SSN for the purpose of locating or identifying an individual with the intent to cause physical harm or use the identity of such individual.
H.R. 220	Identity Theft Prevention Act of 2005	Prohibits using an SSN except for specified Social Security and tax purposes; prohibits the Social Security Administration from divulging the Social Security account number of an individual to any federal, state, or local government agency or instrumentality, or to any other individual.
H.R. 92	To amend title XVIII of the Social Security Act to permit Medicare beneficiaries upon request to use an identification number other than a social security account number under the Medicare Program in order to deter identity theft.	Directs the Secretary of Health and Human Services to establish a procedure under which, upon the request of an individual entitled to Medicare benefits, the Secretary shall provide for the issuance of an (1) identification number other than the individual's Social Security account number for Medicare purposes and (2) an appropriate Medicare card containing such an alternative identification number.

Bill Number	Title	Selected Provisions
H.R. 82	Social Security On-line Privacy Protection Act	Prohibits an interactive computer service from disclosing to a third party an individual's Social Security number or related personally identifiable information without the individual's prior informed written consent.
H.R. 744	Internet Spyware (I-SPY) Prevention Act of 2005	Amends the federal criminal code to prohibit intentionally accessing a protected computer without authorization, or exceeding authorized access, by causing a computer program or code to be copied onto the protected computer and intentionally using that program or code: to obtain or transmit personal information (including an SSN or other government-issued identification number, a bank or credit card number, or an associated password or access code) with intent to defraud or injure a person or cause damage to a protected computer.
H.R. 1069	Notification of Risk to Personal Data Act	Amends the Gramm-Leach-Bliley Act to require a financial institution, at which a breach of personal information is reasonably believed to have occurred, to promptly notify each affected customer; amends the Fair Credit Reporting Act to require a consumer reporting agency to maintain a fraud alert file with respect to any consumer upon receiving notice of a breach of personal information.
H.R. 1078	Social Security Number Protection Act of 2005	Amends the Social Security Act to establish criminal penalties for the sale and purchase of the Social Security number and Social Security account number of any person, except without consent or in certain circumstances.
H.R. 1745	Social Security Number Privacy and Identity Theft Prevention Act of 2005	Amends title II of the Social Security Act to (1) specify restrictions on the sale and display to the general public of by federal, state, and local governments and bankruptcy case trustees; (2) prohibit the display of SSNs on checks issued for payment by such governments; (3) prohibit the federal, state, or local government display of SSNs on employee identification cards or tags (IDs); (4) prohibit access to the SSNs of other individuals by prisoners employed by federal, state, or local governments; and (5) prohibit the selling, purchasing, or displaying of SSNs (with certain exceptions), or the obtaining or use of any individual's SSN to locate or identify such individual with the intent to physically injure or harm such individual or to use the individual's ID for any illegal purpose by any person.
H.R. 2518	Stop the Theft of Our Social Security Numbers Act of 2005	Prohibit disclosure of an individual's SSN services on Medicare-related mailings.
H.R. 2840	Federal Agency Protection of Privacy Act of 2005	Requires federal agencies when publishing a general notice of proposed rule making and when such rule making pertains to the collection, maintenance, use, or disclosure of personally identifiable information from ten or more individuals to prepare an initial assessment describing the rule's impact on individual privacy.
S. 29	Social Security Number Misuse Protection Act	Amends the federal criminal code to prohibit the display, sale, or purchase of SSNs without the affirmatively expressed consent of the individual, except in specified circumstances.
S. 115	Notification of Risk to Personal Data Act	Requires any entity that owns or licenses electronic data containing personal information, following the discovery of a breach of security of the system containing such data, to notify any U.S. resident whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
S. 116	Privacy Act of 2005	Prohibits the sale and disclosure of personally identifiable information by a commercial entity to a nonaffiliated third party unless prescribed procedures for notice and opportunity to restrict such disclosure have been followed; prohibits the display, sale, or purchase SSNs without the affirmatively expressed consent of the individual; prohibits the use of SSNs on (1) checks issued for payment by governmental agencies and (2) driver's licenses or motor vehicle registrations; prohibits a commercial entity from requiring disclosure of an individual's SSN in order to obtain goods or services.

Bill Number	Title	Selected Provisions
S. 751	Notification of Risk to Personal Data Act	Requires any federal agency or person that owns, licenses, or collects personal information data following the discovery of a breach its personal data security system, or upon receiving notice of a system breach, to notify (as specified) the individual whose information was obtained by an unauthorized person.
S. 1216	Financial Privacy Breach Notification Act of 2005	Amends GLBA to require a financial institution to promptly notify the following entities whenever a breach of personal information has occurred at such institution (1) each customer affected by such breach, (2) certain consumer reporting agencies, and (3) appropriate law enforcement agencies.

Source: GAO Analysis.

GAO's Mission

The Government Accountability Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "Subscribe to Updates."

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Gloria Jarmon, Managing Director, JarmonG@gao.gov (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, D.C. 20548

Public Affairs

Paul Anderson, Managing Director, AndersonP1@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548