



United States Government Accountability Office
Washington, DC 20548

September 19, 2008

The Honorable Charles E. Schumer
Chairman
Subcommittee on Administrative Oversight and the Courts
Committee on the Judiciary
United States Senate

Subject: Social Security Numbers Are Widely Available in Bulk and Online Records, but Changes to Enhance Security Are Occurring

Various public records in the United States contain Social Security numbers (SSN) and other personal identifying information that could be used to commit fraud and identity theft. For the purposes of this report, public records are generally defined as government agency-held records made available to the public in their entirety for inspection, such as property and court records. Although public records were traditionally accessed locally in county courthouses and government records centers, public record keepers in some states and localities have more recently been maintaining electronic images of their records. In electronic format, records can be made available through the Internet or easily transferred to other parties in bulk quantities. Although we previously reported on the types of public records that contain SSNs and access to those records, less is known about the extent to which public records containing personal identifying information such as SSNs are made available to private third parties through bulk sales. In light of these developments, you asked us to examine (1) to what extent, for what reasons, and to whom are public records that may contain SSNs available for bulk purchase and online, and (2) what measures have been taken to protect SSNs that may be contained in these records.

To answer these questions, we collected and analyzed information from a variety of sources. Specifically, we conducted a survey of county record keepers on the extent and reasons for which they make records available in bulk or online, the types of records that they make available, and the types of entities (e.g., private businesses or individuals) that obtain their records. We focused on county record keepers because, in scoping our review, we determined that records with SSNs are most likely to be made available in bulk or online at the county level. We surveyed a sample of 247 counties—including the 97 largest counties by population and a random sample of 150 of the remaining counties, received responses from 89

percent, and used this information to generate national estimates to the extent possible. Our survey covered 45 states and the District of Columbia, excluding five states where recording of documents is not performed at the county level (Alaska, Connecticut, Hawaii, Rhode Island, and Vermont). We used the information gathered in this survey to calculate estimates about the entire population of county record keepers.¹

To obtain information on how businesses use information from public records, we identified and interviewed a judgmentally selected group of private businesses representing a cross section of industries that obtain records in bulk or online. Furthermore, we conducted site visits in Illinois, Texas, California, and the Washington, D.C. area to speak with county record keepers and businesses that obtain records in bulk or online. We visited these locations based on the large volume of records they maintain, as well as recent statutory and administrative efforts in those states to place limits on bulk transfers or the availability of SSNs in public documents. In addition, we interviewed interest groups we identified while planning our work that represent record keepers and businesses that utilize public records. We also reviewed relevant federal privacy and records laws and recently proposed legislation related to information privacy, reviewed state laws we identified from outside sources, and reviewed available information on select foreign data protection laws. We performed our work from September 2007 through September 2008 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

On September 4, 2008, we briefed your staff on the results of our work. This letter formally conveys the information provided during that briefing

¹Because we followed a probability procedure based on random selections, our sample is only one of a large number of samples that we might have drawn. Since each sample could have provided different estimates, we express our confidence in the precision of our particular sample's results as a 95 percent confidence interval (i.e., plus or minus 15 percentage points). This is the interval that would contain the actual population value for 95 percent of the samples we could have drawn. As a result, we are 95 percent confident that each of the confidence intervals in this report will include the true values in the study population. In addition, for reporting purposes, each sample element selected was subsequently weighted in the analysis to account statistically for all the members of the population.

(see enc. I). Concurrently with this letter, we are issuing an electronic supplement that shows the responses to all survey items.²

Results in Brief

Many counties make public records that may contain Social Security numbers (SSNs) available in bulk to businesses and individuals in response to state open records laws, and also because private companies often request access to these records to support their business operations. Our sample allows us to estimate that 85 percent of the largest counties make records with full or partial SSNs available in bulk or online,³ while smaller counties are less likely to do so (41 percent). According to county officials and businesses we interviewed, SSNs are generally found in certain types of records such as property liens and appear relatively infrequently. However, because millions of records are available, many SSNs may be displayed. Counties in our survey cited state laws as the primary reason for making records available, and requests from companies may also drive availability, as several told us they need bulk records to support their businesses models. Counties generally do not control how records are used. Of counties that make records available in bulk or online, only about 16 percent place any restrictions on the types of entities that can obtain these records. We found that title companies are the most frequent recipients of these records, but others such as mortgage companies and data resellers that collect and aggregate personal information often obtain records as well. Private companies we interviewed told us they obtain records to help them conduct their business, including using SSNs as a unique identifier. For example, a title company or data reseller may use the SSN to ensure that a lien is associated with the correct individual, given that many people have the same name. Information from these records may also be used by companies to build and maintain databases or resold to other businesses. Businesses we contacted told us they have various safeguards in place to secure information they obtain from public records, including computer systems that restrict employees' access to records. In some cases, information from these public records is sent overseas for processing, a practice referred to as offshoring. We were not able to determine the extent of offshoring, but both record keepers and large companies that obtain records in bulk told us that it is a common practice. In the course of our work, we found that public records data are commonly sent to at least two countries—India and the Philippines.

²GAO, *Social Security Numbers: Transfers and Sales of Public Records That May Contain Social Security Numbers, an E-supplement to GAO-08-1009R*, [GAO-08-1004SP](#) (Washington, D.C.: Sept 19, 2008).

³Unless otherwise noted, all estimates have a margin of error of 15 percent or less.

State and local governments, as well as the federal government, are taking various actions to safeguard SSNs in public records, but these actions are a recent phenomenon. Based on our survey, we estimate that about 12 percent of counties have completed redacting or truncating SSNs that are in public records—that is, removing the full SSN from display or showing only part of it—and another 26 percent are in the process of doing so. Some are responding to state laws requiring redaction or truncation, but others have acted on their own based on concerns about the potential for identity theft. For example, California and Florida recently passed laws that require record keepers to truncate or redact SSNs in their publicly available documents, while one clerk in Texas told us that in response to public concern about the vulnerability of SSNs to misuse, the county is redacting SSNs from records on its own initiative. In recent years, 25 states have enacted some form of statutory restriction on displaying SSNs in public records. Some states have also enacted laws allowing individuals to request that their SSNs be removed from certain records such as military discharge papers. For example, in one of the states we visited, we saw notices posted by county recorders describing the right to make this request. At the federal level, our prior work found that some federal agencies have taken action by truncating SSNs they place in the public record at the local level. For example, the Internal Revenue Service (IRS) recently started truncating SSNs in tax liens it files with local clerks and recorders, and the Department of Justice (Justice) initiated a similar practice for some liens and other records in response to our prior recommendations. However, we did not identify any federal laws restricting state or local governments from making public records available in bulk or governing how private entities may use SSNs obtained from public records, including the offshoring of records with SSNs. Although their governments have enacted measures that may address data security in the two countries where we were told public records data are sent, the extent to which those measures protect SSNs from inappropriate use is unclear. There are several bills pending in the current Congress that would limit both private and government entities' ability to sell or display SSNs to other parties. For example, one of the bills has a provision that would limit posting SSNs that are contained in public records on the Internet. The bills do not address how SSNs or personal information from public records that has been sent offshore should be handled.

Concluding Observations

Recent actions by states and counties to limit the display of SSNs in records made available to the public through redaction or truncation are positive steps, but these actions will only protect SSNs in future transactions, as millions of records with SSNs have already been obtained in bulk or online. Additional concerns remain about the security of SSNs in these records. In particular, because many record keepers cannot or do not restrict what entities can obtain public records with SSNs or control

how they are used, and some businesses are sending records with SSNs offshore where little is known about how they are used or protected, ensuring the security of SSNs is an ongoing challenge.

In weighing how best to address some of these open issues over the availability of SSNs in public records, Congress will need to balance the need to keep SSNs confidential with the long standing tradition of open access to public records, the rights of states and localities to regulate the availability of records they maintain, and the use of SSNs in the private sector. Recent actions taken by the IRS, Justice, and states to truncate SSNs represent one effort that may strike an appropriate balance between protecting SSNs from misuse and making a portion available for appropriate parties to firmly establish the identity of specific individuals.

Agency Comments

We provided a draft of this report to the Social Security Administration (SSA) and the Federal Trade Commission (FTC) for review and comment. SSA and FTC provided only technical comments which we incorporated as appropriate.

As agreed with your office, unless you publicly announce its contents earlier, we plan no further distribution of this report until 30 days after its issue date. At that time, we will send copies of this report to relevant congressional committees, the Commissioner of SSA, the Chairman of FTC, and other interested parties and will make copies available to others on request. In addition, this report will be available at no charge on GAO's Web site at <http://www.gao.gov>. If you or your staff have any questions about this report, please contact me at 202-512-7215 or bertonid@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this study include Jeremy Cox (Assistant Director), Joel Marus (Analyst-in-Charge), Daniel Concepcion, and Jill Yost. In addition, Carolyn Boyce, Justin Fisher, Sheila McCoy, George Quinn, Walter Vance, and Charles Willson provided significant assistance.



Daniel Bertoni
Director, Education, Workforce, and
Income Security Issues

Enclosure



Social Security Numbers Are Widely Available in Bulk and Online Records, but Changes to Enhance Security Are Occurring

**Briefing for Senator Charles E. Schumer,
Chairman, Subcommittee on Administrative Oversight and the Courts,
Committee on the Judiciary**

September 4, 2008

Overview

- Key Objectives
- Scope and Methodology
- Summary of Results
- Background
- Findings
- Concluding Observations

Key Objectives

The Chairman of the Senate Subcommittee on Administrative Oversight and the Courts, Committee on the Judiciary, requested that we conduct this study. We answered the following questions:

- To what extent, for what reasons, and to whom are public records that may contain Social Security numbers (SSNs) available for bulk purchase and online?
 - What measures have been taken to protect SSNs that may be contained in these records?
-

Scope and Methodology

To answer these questions, we

- conducted a survey of county record keepers;
 - interviewed companies from a cross section of industries that use public records for business purposes;
 - visited county record keepers and businesses in Illinois, Texas, California, and the Washington, D.C., area; and
 - interviewed organizations representing government public record keepers and organizations representing businesses that utilize public records.
-

Scope and Methodology: Survey

- The survey was sent to offices in 247 counties responsible for recording documents—including the 97 largest counties by population and a random sample of 150 of the remaining counties. Overall response rate was 88.9 percent.
 - AK, CT, HI, RI, and VT were omitted from our sample because document recording is not done at the county level.
 - The survey was Web-based and was pretested prior to distribution.
 - We used the information gathered in this survey to calculate estimates of the entire population of county record keepers. Unless otherwise noted, the margin of error for all estimates is 15 percent or less.
-

Scope and Methodology: Analysis of Laws to Protect SSNs

- We reviewed relevant federal privacy and records laws and proposed legislation.
 - We reviewed select state statutory provisions identified through interviews and prior research conducted by the Social Security Administration, but did not conduct our own exhaustive search of state legal requirements.
 - Information on foreign laws in this report does not reflect our independent legal analysis, but is based on interviews and secondary sources.
-

Summary of Results

-
- We estimate that 85 percent of large counties and 41 percent of small counties make records that may contain SSNs available in bulk or online.
 - Counties cited state laws as a key reason for providing records. Generally, counties do not place restrictions on who obtains records or how they are used.
 - Businesses obtain these records to use or resell data in them and may use SSNs to link identifying information on records back to specific individuals, such as ensuring that liens are applied to the correct individuals, since many people share the same name. In some cases, businesses send information from these records overseas for processing.
-

Summary of Results (continued)

- Federal, state, and local governments have recently taken steps to safeguard SSNs in public records. We estimate more than a third of counties have already removed (redacted) or truncated SSNs or are currently removing SSNs from their records; some in response to state laws and others of their own accord.
- Some federal agencies have taken steps to remove full SSNs from documents they provide to counties. However, we did not identify any federal laws that appeared to restrict the bulk transfer of state and local public records or the display of SSNs in those records, nor did we identify any federal law that provides protections for SSNs obtained from public records and sent overseas by private parties. Several bills are pending in Congress that would limit the display or sale of SSNs to the public or to private entities.

Background

- Although originally created to track workers' earnings and Social Security benefits, SSNs have become the universal identifier of choice for government agencies and are currently used for myriad non-Social Security purposes.
 - The SSN's widespread use has also made it a key piece of information used to create false identities for financial misuse or to assume another individual's identity.
 - The Federal Trade Commission (FTC) estimated that in 2005, 8.3 million people discovered they were victims of identity theft, translating into estimated losses of billions of dollars.
-

Background (continued)

- For purposes of this report, we define public records to include records or documents that are routinely made available to the public by a government agency or the courts.
 - There are many types of public records, including birth, death, and marriage records; criminal and civil court case files; and records that concern property ownership, such as property liens. The records are stored in formats such as paper, microfilm, and electronic image.
 - Public records that used to be accessible only in the county recorder's office can now be accessed electronically from other locations.
 - Some records contain personal identifying information, such as SSNs, dates of birth, and credit card or bank account numbers.
-

Background (continued)

- Individuals and businesses are able to obtain large numbers of public records. This generally involves the transfer of bulk or individual records:
 - Bulk: An entity (e.g., a private business or individual) obtains or buys all records held by a record keeper (such as property liens) and may receive regular updates, such as a weekly update of all such documents filed in the last week.
 - Individual: An entity obtains records one at a time, usually over the Internet, hereafter referred to as online. Service may be free or may require users to register and pay for access.
-

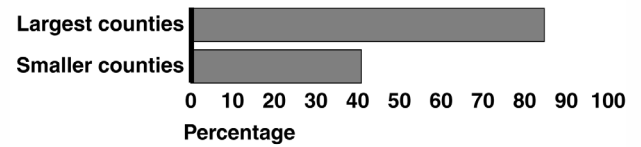
Finding 1: Availability and use of records



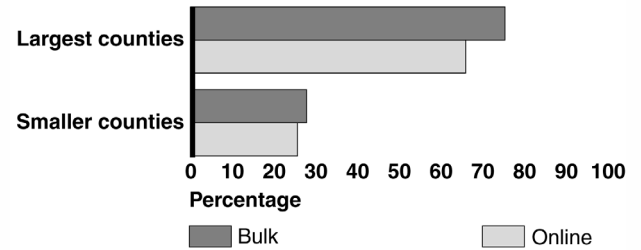
Many Counties Make Records Available in Bulk or Online

- For the states covered by our survey,¹ we estimate that about 85 percent of large counties and 41 percent of small counties make records that may contain SSNs available in bulk or online.
- The 100 largest counties have a combined population of about 118 million.
- Some smaller counties indicated that they lack the resources to make records available in bulk or online.

Availability of Records That May Contain SSNs



Availability of Records That May Contain SSNs by Mode of Transfer



Source: GAO survey.

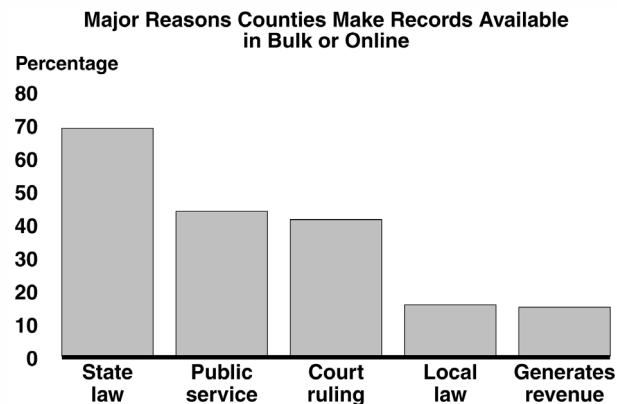
¹ This includes 45 states and the District of Columbia.

While Record Keepers and Bulk Users Report SSNs Appear Relatively Infrequently in Records, the Total Number of Records with SSNs Could Be Large

- Counties and businesses we interviewed told us:
 - SSNs generally appear more often in certain types of documents, including state and federal liens.
 - To a lesser extent, SSNs appear in judgments and mortgage records.
 - The prevalence of SSNs in documents is relatively low and has decreased over time.
- However, because record keepers can maintain millions of documents, many SSNs may be displayed.

Counties Make Records Available for Various Reasons

- In our survey, counties cited requirements under state law as the most common major reason for making records available in bulk or online.



Demand from Businesses May Also Drive the Availability of Records

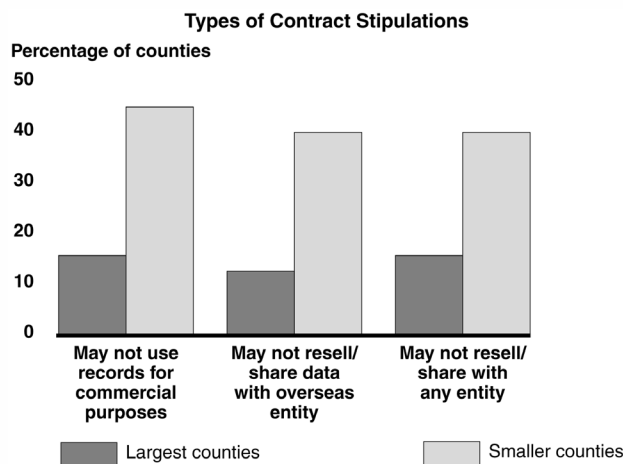
- Several companies we interviewed said they need to obtain records in bulk to support their business models, such as developing a database of title records (known as a title plant).
- One title company told us that obtaining records in bulk increases the efficiency of its operations as opposed to having to physically travel to the recorder's office to search records.

Counties Generally Do Not Place Restrictions on Who Obtains Records

- We estimate that only about 16 percent of counties that make records available in bulk or online place some restrictions on the types of entities that can obtain records.
- Additionally, we estimate that only about 23 percent of counties that make records available in bulk or online take any steps to verify the identity of entities that obtain records.
- A majority of counties reported that there is no state or local law that requires or prohibits them from obtaining the identity of those who receive records in bulk or online.

Counties Generally Do Not Control How Records Are Used

- We estimate that about 38 percent of counties require users of bulk or online records to enter into a contract or agreement.
- Among those counties, we found that smaller counties are more likely to have certain types of restrictions in place than are the largest counties.

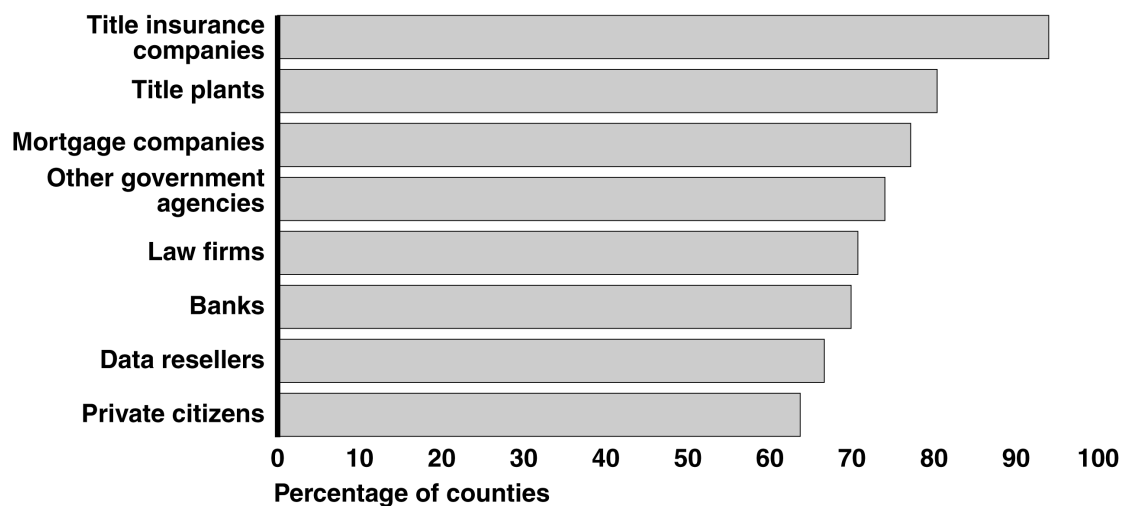


Source: GAO survey.

Note: Confidence intervals for this chart range from 4.7 to 5 percent for the largest counties and 23.5 to 23.9 for smaller counties.

Title Companies are the Most Common Recipients of Online or Bulk Documents

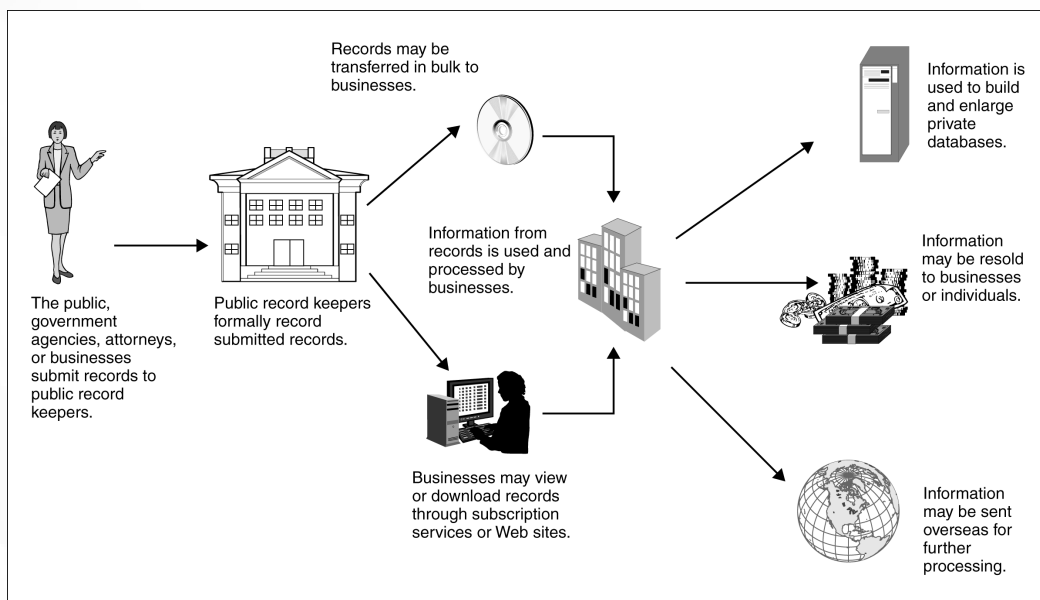
Customers Obtaining Public Records



Source: GAO survey.

Note: Margins of error for this chart range from 9.6 to 19.1 percent.

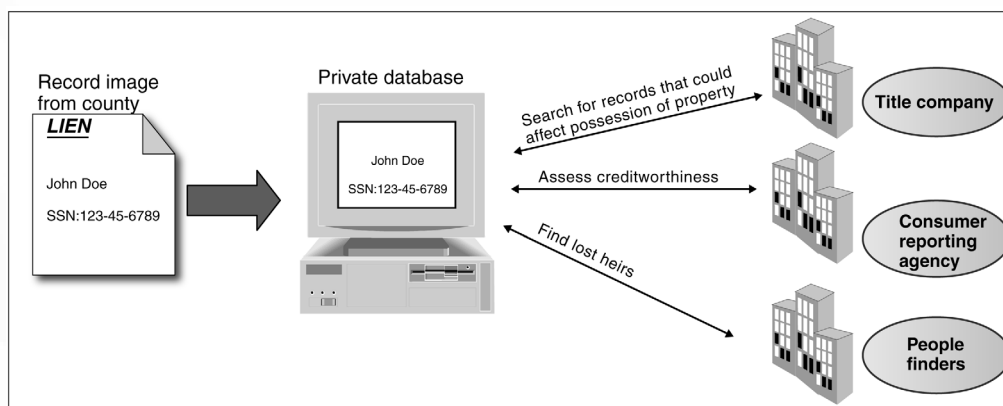
Information from Public Records Can Change Hands Many Times



Sources: GAO; Art Explosion (clip art).

Businesses Use SSNs to Match Public Records Information to Specific Individuals

- Information from records is used by businesses, such as title companies and data resellers, to build and maintain private databases and perform a variety of queries.



Sources: GAO; Art Explosion (clip art).

Some Businesses Rely on SSNs in Records More than Others

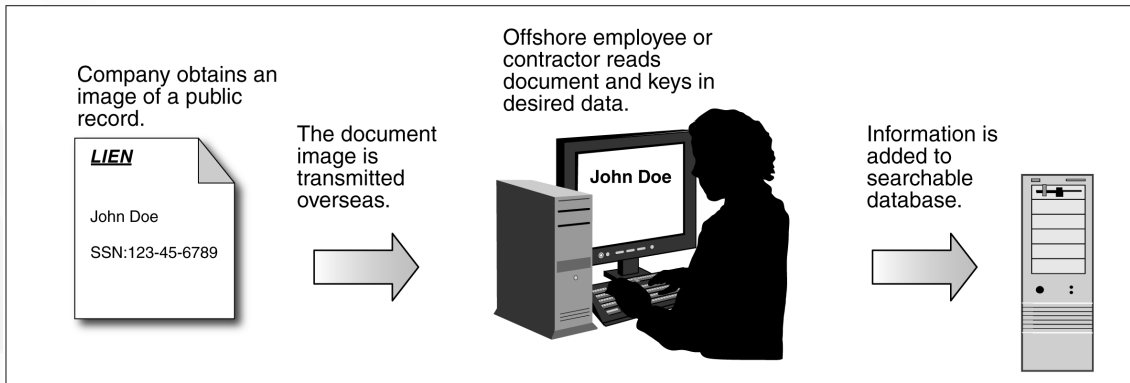
Some businesses told us...	Because...	Examples include...
Having the complete SSN is critical for them.	They must ensure that they match information to the correct individual. There are many people in the nation with the same name.	Consumer reporting agencies, people finders
A partial SSN (e.g., the last four digits) is sufficient.	They still need to match to an individual, but pertinent records are at the county level where the universe of individuals is smaller.	Title insurance industry ²
Having an SSN is inconsequential.	They are not interested in matching data to individuals, but are instead interested in specific information such as recent home purchases.	Marketing firms

Source: GAO

² One title company told us that it is voluntarily truncating SSNs from the 4 billion documents in its repository.

Some Businesses, Including the Title Industry, Send Document Images Overseas for Processing

- Officials from some companies we interviewed told us they share data from public records with offshore units or service providers
- India and the Philippines are two locations where public records data are sent.



Sources: GAO; Art Explosion (clip art).

Some Businesses, Including the Title Industry, Send Document Images Overseas for Processing (continued)

- We were unable to determine the overall extent to which businesses send records containing SSNs overseas, but record keepers we interviewed believe it is common. Additionally, our survey shows that some offshore-based entities obtain records directly from counties.
 - Several companies told us that they take measures to screen overseas employees and follow the same information security procedures in their overseas locations as they do in their U.S. locations.
 - Additionally, companies told us they have various safeguards in place, including computer systems that restrict employees' access to records. The extent to which these protections are in place is unclear.
-

Some Counties Are Taking Actions to Remove SSNs from Public Records or Display Only Partial SSNs

- Some counties have started redacting or truncating SSNs in publicly available versions of recorded documents, but are retaining full SSNs in nonpublic versions that are not available online or for bulk purchase.
 - These actions have sometimes been taken in response to state laws: Several counties in California have begun planning for a new truncation requirement, and counties in Florida have begun redacting SSNs in existing records to comply with a state law.
 - Other counties have taken the initiative to begin redaction on their own. For example, the county clerk in Travis County, Texas, began redacting SSNs in response to privacy concerns.
-

Some Counties Are Taking Actions to Remove SSNs from Public Records or Display Only Partial SSNs (continued)

- On the basis of our survey, we estimate that about 12 percent of counties have redacted or truncated SSNs that appear in online or bulk records. Furthermore, another 26 percent are in the process of redacting or truncating SSNs.
- Large counties are more likely to be planning to redact or truncate SSNs in the future: 24 percent of large counties reported they plan to redact or truncate SSNs in the next two years, while less than 5 percent of smaller counties plan to do so.

Some States Have Passed Laws to Limit the Availability of SSNs in Public Records

- In 2007, SSA's Office of Inspector General identified 25 states in a non-exhaustive search that have enacted some form of statutory limit on the display of SSNs in public records.³ These include
 - 11 states that have taken steps to remove SSNs from public documents, unless SSNs are required by federal law to be included in those records.
 - 24 states that have passed laws to protect individuals SSNs from being on public documents.
 - Within these two groups, there is variation in the scope and applicability of these laws. For example:
 - Some states, such as New Jersey and Ohio, prohibit SSNs from appearing in any publicly recorded document.
 - Others limit the requirement to specific types of records; for example, Kansas and Utah prohibit SSNs from being shown in voter registration records.

³Office of the Inspector General, Social Security Administration, *State and Local Governments' Collection and Use of Social Security Numbers*, September 2007, A-08-07-17086. Additional information was obtained from the workpapers for this report. 26

Some States Have Passed Laws to Limit the Availability of SSNs in Public Records (continued)

- We identified other state laws that allow individuals to request that their SSNs be removed from public records.
 - For example, Texas passed a law in 2007 allowing individuals to request that the first five digits of their SSNs be removed from specific public records.
 - Ohio and Tennessee permit veterans to request that their SSNs be redacted from their military discharge records.

States Have Begun to Enact Laws to Redact or Truncate SSNs Displayed in Public Records

For example:

- California—Recorders must begin truncating SSNs in publicly available records recorded between 1980 and 2008. For records filed on or after January 1, 2009, recorders are required to truncate SSNs in the public versions of filings. They can petition their county board of supervisors for authority to charge additional fees.
 - Florida—Since 2002, officials have been required to redact SSNs in records upon written request of the SSN holder, and parties filing documents have generally been required to exclude SSNs. SSNs in electronic records must be kept confidential beginning in 2011.
 - Other states have narrower requirements—Virginia law authorizes circuit court clerks to redact SSNs from certain land records and provides that they may receive reimbursement for this effort from a state trust fund.
-

Existing Federal Laws Do Not Address the Transfer of State and Local Public Records or the Display of SSNs in Them

- Major federal privacy and records laws we reviewed, including the Privacy Act and the Freedom of Information Act (FOIA), do not appear to restrict the bulk transfer of state or local public records or the display of SSNs in those records.
- A 1990 amendment to the Social Security Act requires that SSNs obtained or maintained pursuant to any provision of law enacted on or after October 1, 1990, be kept confidential.⁴
 - Officials at SSA and FTC staff were not aware of any actions taken to enforce this provision, and no regulations have been promulgated implementing the provision.⁵
 - We were unable to identify any federal or state cases addressing this provision, nor could we find anything relevant in the legislative history.
 - As a result, it is not clear whether or how this provision applies to state and local government sales of public records that may contain SSNs.

⁴ 42 U.S.C. § 405(c)(2)(C)(viii).

⁵ In their technical comments on a draft of this report, SSA officials noted that while SSA has general rulemaking authority with respect to this provision, it has not explored the extent of this authority. In addition, SSA officials stated that even if SSA were to promulgate regulations under this provision, it does not have the authority to enforce them. FTC does not have rulemaking authority under the amendment, according to FTC staff.

Federal and Foreign Laws May Not Provide Protection for SSNs Sent Overseas

- We did not identify any federal law that provides protection for SSNs obtained from public records and sent to overseas locations by private parties that obtain public records in bulk or online.
- According to one study, no specific legislation pertaining to data protection has been enacted in India.⁶ However, that study also noted that there may be other laws, such as the Information Technology Act of 2000, that address some issues related to data security.
- An offshore service provider based in the Philippines informed us its government has issued an administrative order enumerating guidelines for protecting personal data but it has not been enacted as law.

⁶ CRID – University of Namur, *First Analysis of the Personal Data Protection Law in India: Final Report*, June 2005.

Selected Pending Federal Legislation Would Limit the Display or Sale of SSNs

<p>S. 238 Generally prohibits the display or purchase of SSNs without the express consent of the SSN holder; contains an exception for certain public records</p>	<p>H.R. 948 Makes it unlawful for any person to sell or purchase SSNs in a manner violating regulations to be promulgated by SSA; does not have explicit provisions applicable to or exempting state and local governments</p>
<p>S. 2915 Prohibits display of SSNs to the general public on the Internet by state and local governments unless truncation standards to be set by SSA in accordance with certain guidelines are met; considers certain unencrypted transmittals of SSNs through the Internet to be a public display</p>	<p>H.R. 3046 With certain exceptions, restricts the sale and display of SSNs to the general public by government entities; Does not specifically address SSNs in public records; Requires SSA to develop uniform truncation standards</p>

Source: GAO.

Efforts to Limit Availability of Records with SSNs Are a Recent Development

- As we previously reported, IRS and DOJ are truncating SSNs in liens and other records that are filed with county record keepers.⁷
- County, state, and federal governments' efforts to limit availability of SSNs have increased in the last several years as concerns about the use of information in public records for identify theft grew.

⁷ GAO, *Social Security Numbers: Federal Actions Could Further Decrease Availability in Public Records, though Other Vulnerabilities Remain*, GAO-07-752, (Washington, D.C., June 15, 2007).

Concluding Observations

- Recent actions by states and counties to limit the display of SSNs in records made available to the public through redaction or truncation are positive steps. However, because millions of records with SSNs have already been obtained in bulk or online, these actions will protect SSNs only in future transfers.
 - The bulk transfer of records raises other concerns about the security of SSNs because
 - Many record keepers do not or cannot restrict the types of entities that can obtain public records and may not know how records are being used.
 - Some businesses are sending records with SSNs offshore, even though not much is known about how they are protected overseas.
-

Concluding Observations (continued)

- Any policy deliberations on further limiting the display of SSNs will need to consider and balance
 - the need to keep SSNs confidential and the longstanding tradition of open access to records,
 - the rights of states and localities to regulate the availability of their records, and
 - existing business practices and appropriate private sector use of SSNs.
 - Recent actions by the IRS, the Department of Justice, and states to truncate SSNs represent one effort that may strike an appropriate balance between protecting SSNs from misuse and making a portion available to appropriate parties to firmly establish the identity of specific individuals.
-

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

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 "E-mail 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, DC 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

Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548