CALIFORNIA DEPARTMENT OF CONSUMER AFFAIRS

Recommended Practices for Protecting the Confidentiality of Social Security Numbers

June 28, 2002

400 R Street, Suite 3000 ¦ Sacramento, CA 94814 ¦ www.privacy.ca.gov

OFFICE OF Privacy Protection

Recommended Practices for Protecting the Confidentiality of Social Security Numbers

Introduction

The Office of Privacy Protection in the California Department of Consumer Affairs has the statutorily mandated purpose of "protecting the privacy of individuals' personal information in a manner consistent with the California Constitution by identifying consumer problems in the privacy area and facilitating development of fair information practices."[1] The law specifically directs the Office to "make recommendations to organizations for privacy policies and practices that promote and protect the interests of California consumers."[2]

In fulfillment of those obligations, the Office of Privacy Protection is publishing these recommended practices for protecting the confidentiality of Social Security numbers. While many of the recommendations might be applied to protect any sensitive personal information, the focus is on Social Security numbers because of the role they have come to play in the marketplace and in identity theft and other forms of fraud.

In developing the recommendations, the Office of Privacy Protection received consultation and advice from an advisory committee made up of representatives of the financial, insurance, health care, retail and information industries and of consumer privacy advocates.[3] The committee members' contributions were very helpful and are greatly appreciated.

Unique Status of the Social Security Number As a Privacy Risk

The Social Security number (SSN) has a unique status as a privacy risk. No other form of personal identification plays such a significant role in linking records that contain sensitive information that individuals generally wish to keep confidential.[4]

Created by the federal government in 1936 to track workers' earnings and eligibility for retirement benefits, the SSN is now used in both the public and private sectors for a myriad of purposes totally unrelated to this original purpose. It is used so widely because the SSN is a unique identifier that does not change, allowing it to serve many record management purposes.[5]

Today SSNs are used as representations of individual identity, as secure passwords, and as the keys for linking multiple records together. The problem is that these uses are incompatible. The widespread use of the SSN as an individual identifier, resulting in its appearance on mailing labels, ID cards and badges, and various publicly displayed

documents, makes it unfit to be a secure password providing access to financial records and other personal information.[6]

The broad use and public exposure of SSNs has been a major contributor to the tremendous growth in recent years in identity theft and other forms of credit fraud. The need to significantly reduce the risks to individuals of the inappropriate disclosure and misuse of SSNs, has in recent years led California and a few other states to take steps to limit their use and display.[7]

California Law on SSN Confidentiality: Civil Code Section 1798.85

The law, which takes effect beginning July 1, 2002 and must be fully effective no later than July 1, 2005, applies to individuals and non-governmental entities. Under the law's provisions, companies may not do any of the following:

- post or publicly display SSNs,
- print SSNs on identification cards or badges;
- require people to transmit an SSN over the Internet unless the connection is secure or the number is encrypted;
- require people to log onto a web site using an SSN without a password.
- print SSNs on anything mailed to a customer unless required by law or the document is a form or application;

The law has a phased-in compliance schedule:

All subject entities but those involved in providing health care or insurance

7/1/02 Must comply with all requirements for new accounts. May continue former practices on existing accounts, but must comply with requirements within 30 days upon written request from customer.

Entities providing health care or insurance

1/1/03 Must comply with all requirements except ban on putting SSNs on identification cards, for individual policyholders

1/1/04 Must comply with all requirements, including identification card requirement, for new individual and group policyholders.

7/1/05 Must comply with all requirements for all individual and group policyholders in existence prior to 1/1/04.

Fair Information Practice Principles

In developing the recommendations, the Office of Privacy Protection looked first to the widely accepted principles that form the basis of most privacy laws in the United States, Canada, Europe and other parts of the world. The Fair Information Practice Principles are openness, collection limitation, purpose specification, use limitation, data quality, individual participation, security and accountability.[8] While they were developed to guide the drafting of national privacy legislation, the principles are also appropriate for organizations to follow in developing their privacy policies and practices. The practices recommended here are all derived from these basic privacy principles.

Recommended Practices for Protecting the Confidentiality of SSNs

The Office of Privacy Protection's recommendations are intended to serve as guidelines to assist organizations in moving towards the goal of aligning their practices with the widely accepted fair information practice principles described below. These recommended practices address, but are not limited to, the provisions of California Civil Code section 1798.85.

The recommendations are relevant for private- and public-sector organizations, and they apply to the handling of all SSNs in the possession of an organization: those of customers, employees and business partners.

1. Reduce the collection of SSNs.
   Fair Information Practice Principles: Collection Limitation, Use Limitation

   - Collect SSNs preferably only where required to do so by federal or state law.
   - When collecting SSNs as allowed, but not required, by law, do so only as reasonably necessary for the proper administration of lawful business activities.
   - If a unique personal identifier is needed, develop your own as a substitute for the SSN.

2. Inform individuals when you request their SSNs.
   Fair Information Practice Principle: Openness, Purpose Specification

   - Whenever you collect SSNs as required or allowed by law, inform the individuals of the purpose of the collection, the intended use, whether the law requires the number to be provided or not, and the consequences of not providing the number.
   - If required by law, notify individuals (customers, employees, business partners, etc) annually of their right to request that you do not post or publicly display their SSN or do any of the other things prohibited in Civil Code Section 1798.85(a).

3. Eliminate public display of SSNs.
   Fair Information Practice Principle: Security

   - Do not put SSNs on documents that are widely seen by others, such as identification cards, badges, time cards, employee rosters, bulletin board postings, and other materials.
   - Do not send documents with SSNs on them through the mail, except on applications or forms or when required by law[9].
   - When sending applications, forms or other documents required by law to carry SSNs through the mail, place the SSN where it will not be revealed by an envelope window. Where possible, leave the SSN field on forms and applications blank and ask the individual to fill it in before returning the form or application.
   - Do not send SSNs by email unless the connection is secure or the SSN is encrypted.
   - Do not require an individual to send his or her SSN over the Internet or by email, unless the connection is secure or the SSN is encrypted.
   - Do not require individuals to use SSNs as passwords or codes for access to Internet web sites or other services.

4. Control access to SSNs.
   Fair Information Practice Principle: Security

   - Limit access to records containing SSNs only to those who need to see the numbers for the performance of their duties.
   - Use logs or electronic audit trails to monitor employees' access to records with SSNs.
   - Protect records containing SSNs, including back-ups, during storage by encrypting the numbers in electronic records or storing records in other media in locked cabinets.
   - Do not store records containing SSNs on computers or other electronic devices that are not secured against unauthorized access.
   - Avoid sharing SSNs with other companies or organizations except where required by law.
   - If you do share SSNs with other companies or organizations, including contractors, use written agreements to protect their confidentiality.
     - Prohibit such third parties from re-disclosing SSNs, except as required by law.
     - Require such third parties to use effective security controls on record systems containing SSNs.
     - Hold such third parties accountable for compliance with the restrictions you impose, including monitoring or auditing their practices.
   - If SSNs are disclosed inappropriately and the individuals whose SSNs were disclosed are put at risk of identity theft or other harm, promptly notify the individuals potentially affected.

5. Protect SSNs with security safeguards.
   Fair Information Practice Principle: Security

   - Develop a written security plan for record systems that contain SSNs.
   - Develop written policies for protecting the confidentiality of SSNs, including but not limited to the following:
     - Adopt "clean desk/work area" policy requiring employees to properly secure records containing SSNs.
     - Do not leave voice mail messages containing SSNs and if you must send an SSN by fax, take special measures to ensure confidentiality.
     - Require employees to ask individuals (employees, customers, etc.) for identifiers other than the SSN when looking up records for the individual.
     - Require employees to promptly report any inappropriate disclosure or loss of records containing SSNs to their supervisors or to the organization's privacy officer.
     - When discarding or destroying records in any medium containing SSNs, do so in a way that protects their confidentiality, such as shredding.[10]

6. Make your organization accountable for protecting SSNs.
   Fair Information Practice Principle: Accountability

   - Provide training and written material for employees on their responsibilities in handling SSNs.
     - Conduct training at least annually.
     - Train all new employees, temporary employees and contract employees.
   - Impose discipline on employees for non-compliance with organizational policies and practices for protecting SSNs.
   - Conduct risk assessments and regular audits of record systems containing SSNs.
   - Designate someone in the organization as responsible for ensuring compliance with policies and procedures for protecting SSNs.

Notes

[1] California Business & Professions Code section 350(a).

[2] California Business & Professions Code section 350(c).

[3] The Advisory Committee members were Victoria Allen of the California Credit Union League; Jennie Bretschneider, Legislative Aide to Senator Debra Bowen; James W. Bruner, Jr., of Orrick, Herrington & Sutcliffe; Shelley Curran of Consumers Union; Mari Frank, Esq., privacy consultant; Beth Givens of the Privacy Rights Clearinghouse; Tony Hadley of Experian; Michael Hensley of LexisNexis; Chris Lewis of Providian and the California Chamber of Commerce; Deborah Pierce of Privacy Activism; Rebecca Richards of TRUSTe; Wendy Schmidt of Federated Department Stores and the California Retailers Association; Elaine Torres of Wells Fargo Bank; and Lee Wood of the Association of California Life & Health Insurance Companies.

[4] Mark Rotenberg, Executive Director, Electronic Privacy Information Center and Adjunct Professor, Georgetown University Law Center, "Testimony and Statement for the Record," Joint Hearing on SSNs and Identity Theft, Subcommittee on Oversight and Investigations, Committee on Financial Services, and Subcommittee on Social Security, Committee on Ways and Means, U. S. House of Representatives, November 8, 2001. Available at www.epic.org/privacy/ssn/testimony_11_08_2001.html .

[5] *Social Security Numbers: Government Benefits from SSN Use but Could Provide Better Safeguards*, GAO-02-352, May 2002. Available at www.gao.gov.

[6] Chris Hibbert, Computer Professionals for Social Responsibility, "Frequently Asked Questions on SSNs and Privacy," last modified February 16, 2002. Available at www.cpsr.org/cpsr/privacy/ssn/ssn.faq.html.

[7] Arizona and Rhode Island prohibit the display of students' SSNs on the Internet. In Washington, as the result of an April 2000 executive order of the Governor, state agencies have removed SSNs from many documents where their display was determined not to be necessary. Minnesota's Government Data Practices Act classes SSNs as not public information.

[8] The Fair Information Practice Principles were first formulated by the U.S. Department of Health, Education and Welfare in 1973. They may be found in the Organisation for Economic Cooperation and Development's *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, available at http://www1.oecd.org/publications/e-book/9302011E.PDF. The Principles are the following:

- *Openness*: There should be a general policy of openness about the practices and policies with respect to personal information.
- *Collection Limitation*: Personal information should be collected by lawful and fair means and with the knowledge or consent of the subject. Only the information necessary for the stated purpose should be collected.
- *Purpose Specification*: The purpose for collecting personal information should be specified at the time of collection. Further uses should be limited to those purposes.
- *Use Limitation*: Personal information should not be used for purposes other than those specified, except with the consent of the subject or by the authority of law.
- *Data Quality*: Personal information should be accurate, complete, timely and relevant to the purpose for which it is to be used.
- *Individual Participation*: Individuals should have the right to inspect and correct their personal information.
- *Security*: Personal information should be protected by reasonable security safeguards against such risks as unauthorized access, destruction, use, modification, and disclosure.
- *Accountability*: Someone in an organization should be held accountable for compliance with the organization's privacy policy. Regular privacy audits and employee training should be conducted. The principles

[9] See Appendix 1 for a partial list of laws that authorize or mandate the collection and use of SSNs. See Appendix 2 for a list of laws restricting the disclosure of SSNs. Both Appendices will be updated with more comprehensive information

[10] Note that California Civil Code Section 1798.81requires businesses to destroy customer records containing personal information by shredding, erasing, or otherwise modifying the personal information in those records to make it unreadable or undecipherable, before discarding them.

Appendix 1: Federal and California Laws That Authorize or Mandate the Collection and Use of Social Security Numbers[1]

Federal Laws

Federal statute	General purpose for collecting or using SSN	Government entity and authorized or required use
Tax Reform Act of 1976 42 U.S.C. 405(c)(2)(c)(i)	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 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(1)	Eligibility benefits under the Medicaid program	Requires that, as a condition of eligibility for Medicaid benefits, applicants for and recipients of these benefits furnish their SSNs to the state administering program
Housing and Community Development Act of 1987 42 U.S.C. 3543(a)	Eligibility for HUD programs	Authorizes the secretary of the Department of Housing and Urban Development to require applicants and participants in HUD programs 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)	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. 510(c)	Eligibility for Veterans Affairs compensation or pension benefits programs	Requires 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)	Eligibility of potential jurors	Authorizes states and political subdivisions of states to use SSNs to determine eligibility of potential jurors
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; creates national database for child support enforcement purposes

[1] Table taken from "Social Security Numbers: SSNs Are Widely Used by Government and Could Be Better Protected," Statement of Barbara D. Bovbjerg, Director of Education, Workforce, and Income Security Issues, GAO, April 29, 2002,GAO-02-691T. Available at www.gao.gov.

Federal statute	General purpose for collecting or using SSN	Government entity and authorized or required use
Debt Collection Improvement Act of 1996 31 U.S.C. 7701(c)	Persons doing business with a federal agency	Requires those doing business with a federal agency, i.e., lenders in a federal guaranteed loan program; applicants for federal licenses, permits, right-of-ways, grants, or benefit payments; contractors of an agency and others to furnish SSNs to the agency
Higher Education Act Amendments of 1998 20 U.S.C. 1090(a)(7)	Financial assistance	Authorizes the secretary of education to include the SSNs of parents of dependent students on certain financial assistance forms
Internal Revenue Code (various amendments) 26 U.S.C. 6109	Tax returns	Authorizes the commissioner of the Internal Revenue Service to require that taxpayers include their SSNs on tax returns

Appendix 2: Federal and California Laws That Restrict Disclosure of SSNs[2]

Federal Laws

The following federal laws establish a framework for restricting SSN disclosure:

The Freedom of Information Act (FOIA) (5 U.S.C. 552)
This act establishes a presumption that records in the possession of agencies and departments of the executive branch of the federal government are accessible to the people. FOIA, as amended, provides that the public has a right of access to federal agency records, except for those records that are protected from disclosure by nine stated exemptions. One of these exemptions allows the federal government to withhold information about individuals in personnel and medical files and similar files when the disclosure would constitute a clearly unwarranted invasion of personal privacy. According to Department of Justice guidance, agencies should withhold SSNs under this FOIA exemption. This statute does not apply to state and local governments.

The Privacy Act of 1974 (5 U.S.C. 552a)
The act regulates federal government agencies' collection, maintenance, use and disclosure of personal information maintained by agencies in a system of records.[1] The act prohibits the disclosure of any record contained in a system of records unless the disclosure is made on the basis of a written request or prior written consent of the person to whom the records pertains, or is otherwise authorized by law. The act authorizes 12 exceptions under which an agency may disclose information in its records. However, these provisions do not apply to state and local governments, and state law varies widely regarding disclosure of personal information in state government agencies' control. There is one section of the Privacy Act, section 7, that does apply to state and local governments. Section 7 makes it unlawful for federal, state, and local agencies to deny an individual a right or benefit provided by law because of the individual's refusal to disclose his SSN. This provision does not apply (1) where federal law mandates disclosure of individuals' SSNs or (2) where a law existed prior to January 1, 1975 requiring disclosure of SSNs, for purposes of verifying the identity of individuals, to federal, state or local agencies maintaining a system of records existing and operating before that date. Section 7 also requires federal, state and local agencies, when requesting SSNs, to inform the individual (1) whether disclosure is voluntary or mandatory, (2) by what legal authority the SSN is solicited, and (3) what uses will be made of the SSN. The act contains a number of additional provisions that restrict federal agencies' use of personal information. For example, an agency must maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose required by statute or executive order of the president, and the agency must collect information to the greatest extent practicable directly from the individual when the information may result in an adverse determination about an individual's rights, benefits and privileges under federal programs.

The Social Security Act Amendments of 1990 (42 U.S.C. 405(c)(2)(C)(viii))
A provision of the Social Security Act bars disclosure by federal, state and local governments of SSNs collected pursuant to laws enacted on or after October 1, 1990. This provision of the act also contains criminal penalties for "unauthorized willful disclosures" of SSNs; the Department of Justice would determine whether to prosecute a willful disclosure violation. Because the act specifically cites willful disclosures, careless behavior or inadequate safeguards may not be

[2] Taken from *Social Security Numbers: Government Benefits from SSN Use but Could Provide Better Safeguards*, GAO-02-352, May 2002. Available at www.gao.gov.

subject to criminal prosecution. Moreover, applicability of the provision is further limited in many instances because it only applies to disclosure of SSNs collected in accordance with laws enacted on or after October 1, 1990. For SSNs collected by government entities pursuant to laws enacted before October 1, 1990, this provision does not apply and therefore, would not restrict disclosing the SSN. Finally, because the provision applies to disclosure of SSNs collected pursuant to laws requiring SSNs, it is not clear if the provision also applies to disclosure of SSNs collected without a statutory requirement to do so. This provision applies to federal, state and local governmental agencies; however, the applicability to courts is not clearly spelled out in the law.

California Laws

Confidentiality of Social Security Numbers (CA Civil Code Section 1798.85)

This law, passed in 2001, bars businesses in California from publicly displaying SSNs in specified ways. It takes effect beginning in July 2002 and ending with its application to health care entities by January 2005. The law was passed to help control many of the common uses of SSNs that can expose people to the risk of identity theft. For details, see Confidentiality of Social Security Numbers, Civil Code Section 1798.85.