CALIFORNIA
OFFICE OF
PRIVACY
PROTECTION

Recommended Practices on Protecting the Confidentiality of Social Security Numbers

April 2008

June 2002
Rev. January 2003
Rev. April 2007
Rev. April 2008

California Office of Privacy Protection
www.privacy.ca.gov
866-785-9663

Contents

Introduction

The California Office of Privacy Protection 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 line with those obligations, the Office of Privacy Protection offers 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 SSN 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.

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. [4]

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, badges, and various publicly displayed documents, makes it unfit to be a secure password providing access to financial records and other personal information.[5]

Protecting SSNs

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

In 2003, the public posting or display of SSNs was prohibited. The following year, laws that banned printing an entire SSN on a pay stub and created a procedure for truncating the numbers in family court records took effect. In 2007, laws were passed requiring truncation of SSNs in abstracts of judgment, tax liens, Uniform Commercial Code filings and publicly available records of local government agencies.[6]

Many other states have followed California's lead and enacted similar laws restricting the use of SSNs.[7] The federal government is focusing efforts on reducing federal agencies' use of the numbers. In May 2007 the Office of Man-

agement and Budget, following up on the recommendation of the President's Task Force on Identity Theft, issued guidance urging federal agencies to eliminate unnecessary use of SSNs and explore alternatives to the numbers as individual identifiers.[8]

Recommended Practices

Fair Information Practice Principles

In developing these recommendations, the California 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.[9] 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 all derived from these basic privacy principles.

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. They are not legal opinions or binding regulations. 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 Social Security numbers in the possession of an organization: those of customers, employees, and business partners.

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.

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).

Eliminate the 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.[10]

- 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.

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.

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.[11]

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 Government Code section 11549.5, subdivision (a).

[2] California Government Code section 11549.5, subdivision(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] *Social Security Numbers: Government Benefits from SSN Use but Could Provide Better Safeguards*, GAO-02-352, May 2002. Available at <www.gao.gov>.

[5] Chris Hibbert, Computer Professionals for Social Responsibility, *Frequently Asked Questions on SSNs and Privacy*, last modified January 24, 2004. Available at <http://www.cpsr.org/issues/privacy/ssn-faql>.

[6] See Appendix 1.

[7] See the *Compilation of State and Federal Privacy Laws*, published by Privacy Journal, for current information on state laws restructing the use of SSNs.

[8] See OMB Memorandum M-07-17, Safeguarding Against and Responding to the Breach of Personally Identifiable Information. The findings and recommendations of the President's Task Force on Identity Theft may be found in *Combatting identity Theft: A Strategic Plan*, April 2007, available online at <www.idtheft.gov>.

[9] 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 <www1.oecd.org>. 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 speci-

fied, 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.

[10] See Appendices 1-3 for federal and California laws that require the collection of SSNs or restrict the disclosure of the numbers. The lists are not comprehensive.

[11] 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. In addition, section 628 of the Fair Credit Reporting Act (15 U.S. Code section 1681-1681u) requires the proper disposal of records containing consumer information derived from consumer reports.

Appendix 1: California Laws Restricting SSN Disclosure

Public Posting or Display of SSNs

Summary of Civil Code Sections 1798.85-1798.89

Civil Code Sections 1798.85-1798.86 took effect beginning July 1, 2002 and was phased in through January 1, 2007. It applies to any person or entity and prohibits the following practices:

- Posting or publicly display SSNs,
- Printing SSNs on identification cards or badges,
- Requiring people to transmit an SSN over the Internet unless the connection is secure or the number is encrypted,
- Requiring people to log onto a web site using an SSN without a password, and
- Printing SSNs on anything mailed to a customer unless required by law or the document is a form or application.[8]

It also prohibits filing with a county recorder a publicly available document displaying more than the last four digits of an SSN.

Text of Civil Code Sections 1798.85-1798.89

1798.85. (a) Except as provided in this section, a person or entity may not do any of the following:

(1) Publicly post or publicly display in any manner an individual' s social security number. "Publicly post" or "publicly display" means to intentionally communicate or otherwise make available to the general public.

(2) Print an individual's social security number on any card required for the individual to access products or services provided by the person or entity.

(3) Require an individual to transmit his or her social security number over the Internet, unless the connection is secure or the social security number is encrypted.

(4) Require an individual to use his or her social security number to access an Internet Web site, unless a password or unique personal identification number or other authentication device is also required to access the Internet Web site.

(5) Print an individual's social security number on any materials that are mailed to the individual, unless state or federal law requires the social security number to be on the document to be mailed. Notwithstanding this paragraph, social security numbers may be included in applications and forms sent by mail, including documents sent as part of an application or enrollment process, or to establish, amend or terminate an account, contract or policy, or to confirm the accuracy of the social security number. A social security number that is permitted to be mailed under this section may not be printed, in whole or in part, on a postcard or other mailer not requiring an envelope, or visible on the envelope or without the envelope having been opened.

(b) This section does not prevent the collection, use, or release of a social security number as required by state or federal law or the use of a social security number for internal verification or administrative purposes.

(c) This section does not apply to documents that are recorded or required to be open to the public pursuant to Chapter 3.5 (commencing with Section 6250), Chapter 14 (commencing with Section 7150) or Chapter 14.5 (commencing with Section 7220) of Division 7 of Title 1 of, Article 9 (commencing with Section 11120) of Chapter 1 of Part 1 of Division 3 of Title 2 of, or Chapter 9 (commencing with Sec-

tion 54950) of Part 1 of Division 2 of Title 5 of, the Government Code. This section does not apply to records that are required by statute, case law, or California Rule of Court, to be made available to the public by entities provided for in Article VI of the California Constitution.

(d) (1) In the case of a health care service plan, a provider of health care, an insurer or a pharmacy benefits manager, a contractor as defined in Section 56.05, or the provision by any person or entity of administrative or other services relative to health care or insurance products or services, including third-party administration or administrative services only, this section shall become operative in the following manner:

(A) On or before January 1, 2003, the entities listed in paragraph (1) shall comply with paragraphs (1), (3), (4), and (5) of subdivision (a) as these requirements pertain to individual policyholders or individual contractholders.

(B) On or before January 1, 2004, the entities listed in paragraph (1) shall comply with paragraphs (1) to (5), inclusive, of subdivision (a) as these requirements pertain to new individual policyholders or new individual contractholders and new groups, including new groups administered or issued on or after January 1, 2004.

(C) On or before July 1, 2004, the entities listed in paragraph (1) shall comply with paragraphs (1) to (5), inclusive, of subdivision (a) for all individual policyholders and individual contractholders, for all groups, and for all enrollees of the Healthy Families and Medi-Cal programs, except that for individual policyholders, individual contractholders and groups in existence prior to January 1, 2004, the entities listed in paragraph (1) shall comply upon the renewal date of the policy, contract, or group on or after July 1, 2004, but no later than July 1, 2005.

(2) A health care service plan, a provider of health care, an insurer or a pharmacy benefits manager, a contractor, or another person or entity as described in paragraph (1) shall make reasonable efforts to cooperate, through systems testing and other means, to ensure that the requirements of this article are implemented on or before the dates specified in this section.

(3) Notwithstanding paragraph (2), the Director of the Department of Managed Health Care, pursuant to the authority granted under Section 1346 of the Health and Safety Code, or the Insurance Commissioner, pursuant to the authority granted under Section 12921 of the Insurance Code, and upon a determination of good cause, may grant extensions not to exceed six months for compliance by health care service plans and insurers with the requirements of this section when requested by the health care service plan or insurer. Any extension granted shall apply to the health care service plan or insurer's affected providers, pharmacy benefits manager, and contractors.

(e) If a federal law takes effect requiring the United States Department of Health and Human Services to establish a national unique patient health identifier program, a provider of health care, a health care service plan, a licensed health care professional, or a contractor, as those terms are defined in Section 56.05, that complies with the federal law shall be deemed in compliance with this section.

(f) A person or entity may not encode or embed a social security number in or on a card or document, including, but not limited to, using a barcode, chip, magnetic strip, or other technology, in place of removing the social security number, as required by this section.

(g) This section shall become operative, with respect to the University of California, in the following manner:

(1) On or before January 1, 2004, the University of California shall comply with paragraphs (1), (2), and (3) of subdivision (a).

(2) On or before January 1, 2005, the University of California shall comply with paragraphs (4) and (5) of subdivision (a).

(h) This section shall become operative with respect to the Franchise Tax Board on January 1, 2007.

(i) This section shall become operative with respect to the California community college districts on January 1, 2007.

(j) This section shall become operative with respect to the California State University system

on July 1, 2005.

(k) This section shall become operative, with respect to the California Student Aid Commission and its auxiliary organization, in the following manner:

(1) On or before January 1, 2004, the commission and its auxiliary organization shall comply with paragraphs (1), (2), and (3) of subdivision (a).

(2) On or before January 1, 2005, the commission and its auxiliary organization shall comply with paragraphs (4) and (5) of subdivision (a).

1798.86. Any waiver of the provisions of this title is contrary to public policy, and is void and unenforceable.

1798.89. Unless otherwise required to do so by state or federal law, no person, entity, or government agency shall present for recording or filing with a county recorder a document that is required by any provision of law to be open to the public if that record displays more than the last four digits of a social security number.

SSNs on Pay Stubs

Summary of Labor Code Section 226(a)

Labor Code Section 226 requires employers to print no more than the last four digits of an employee's SSN, or to use an employee ID number other than the SSN, on employee pay stubs or itemized statements. Employers must comply by January 1, 2008.

Text of Labor Code Section 226(a)

226. (a) Every employer shall, semimonthly or at the time of each payment of wages, furnish each of his or her employees, either as a detachable part of the check, draft, or voucher paying the employee's wages, or separately when wages are paid by personal check or cash, an accurate itemized statement in writing showing

(1) gross wages earned,

(2) total hours worked by the employee, except for any employee whose compensation is solely based on a salary and who is exempt from payment of overtime under subdivision (a) of Section 515 or any applicable order of the Industrial Welfare Commission,

(3) the number of piece-rate units earned and any applicable piece rate if the employee is paid on a piece-rate basis,

(4) all deductions, provided that all deductions made on written orders of the employee may be aggregated and shown as one item,

(5) net wages earned,

(6) the inclusive dates of the period for which the employee is paid,

(7) the name of the employee and his or her social security number, except that by January 1, 2008, only the last four digits of his or her social security number or an employee identification number other than a social security number may be shown on the itemized statement,

(8) the name and address of the legal entity that is the employer, and

(9) all applicable hourly rates in effect during the pay period and the corresponding number of hours worked at each hourly rate by the employee. The deductions made from payments of wages shall be recorded in ink or other indelible form, properly dated, showing the month, day, and year, and a copy of the statement or a record of the deductions shall be kept on file by the employer for at least three years at the place of employment or at a central location within the State of California.

SSNs in Government Records

Summary of Commercial Code Section 9526.5: Uniform Commercial Code Filings

This law requires the Secretary of State to create versions of Uniform Commercial Code filings that contain only truncated SSNs.

Text of Commercial Code Section 9526.5

9526.5. (a) For purposes of this section, the following terms have the following meanings:

(1) "Official filing" means the permanent archival filing of all instruments, papers, records, and attachments as accepted for filing by a filing office.

(2) "Public filing" means a filing that is an exact copy of an official filing except that any

social security number contained in the copied filing is truncated. The public filing shall have the same legal force and effect as the official filing.

(3) "Truncate" means to redact at least the first five digits of a social security number.

(4) "Truncated social security number" means a social security number that displays no more than the last four digits of the number.

(b) For every filing containing an untruncated social security number filed before August 1, 2007, a filing office shall create a public filing.

(c) A filing office shall post a notice on its Web site informing filers not to include social security numbers in any portion of their filings. A filing office's online filing system shall not contain a field requesting a social security number.

(d) Beginning August 1, 2007, for every filing containing an untruncated social security number filed by means other than the filing office's Web site, a filing office shall create a public filing.

(e) When a public filing version of an official filing exists, both of the following shall apply:

(1) Upon a request for inspection, copying, or any other public disclosure of or any other public disclosure of an official filing that is not exempt from disclosure, a filing office shall make available only the public filing version of that filing.

(2) A filing office shall publicly disclose an official filing only in response to a subpoena or order of a court of competent jurisdiction.

(3) Nothing in this article shall be construed to restrict, delay, or modify access to any official filing, or modify any existing agreements regarding access to any official filing, prior to the creation and availability of a public filing version of that official filing.

(f) A filing office shall be deemed to be in compliance with the requirements of this section and shall not be liable for failure to truncate a social security number if he or she uses due diligence to locate social security numbers in official records and truncate the social security numbers in the public filing version of those official filings. The use of an automated program with a high rate of accuracy shall be deemed to be due diligence.

(g) In the event that a filing office fails to truncate a social security number contained in a record pursuant to subdivision (b) or (d), any person may request that the filing office truncate the social security number contained in that record. Notwithstanding that a filing office may be deemed to be in compliance with this section pursuant to subdivision (f), a filing office that receives a request that identifies the exact location of an untruncated social security number that is required to be truncated pursuant to subdivision (b) or (d) within a specifically identified record, shall truncate that number within 10 business days of receiving the request. The public filing with the truncated social security number shall replace the record with the untruncated number.

(h) The Secretary of State shall not produce or make available financing statements in the form and format described in Section 9521 that provide a space identified for the disclosure of the social security number of an individual.

(i) The Secretary of State shall produce and make available financing statements in the form and format described in Section 9521, except that the financing statements shall not provide a space identified for the disclosure of the social security number of an individual.

(j) The provisions of this section shall not apply to a county recorder.

Summary of Government Code Sections 27300-27307: County Recorders

This law requires county recorders to create versions of documents recorded back to 1980 that contain only trancated SSNs. If authorized by boards of supervisors, they may levy a fee to cover the costs of truncation.

Text of Government Code Sections 27300-27307

27300. As used in this article, the following terms have the following meanings:

(a) "Official record" means the permanent archival record of all instruments, papers, and notices as accepted for recording by a county

recorder.

(b) "Public record" means a record that is in an electronic format and is an exact copy of an official record except that any social security number contained in the copied record is truncated. The public record shall have the same legal force and effect as the official record.

(c) "Truncate" means to redact the first five digits of a social security number.

(d) "Truncated social security number" means a social security number that displays only the last four digits of the number.

27301. The county recorder of each county shall establish a social security number truncation program in order to create a public record version of each official record. The program shall include both of the following components, which the recorder shall implement concurrently:

(a) For each official record recorded between January 1, 1980, and December 31, 2008, the recorder shall create in an electronic format an exact copy of the record except that any social security number contained in the copied record shall be truncated. In order to create a public record copy, the recorder shall first truncate the social security numbers in all records that already exist in an electronic format and then create an electronic version of all other records and truncate social security numbers contained in those records. Each group of records shall be handled in descending chronological order.

(b) For each official record recorded on or after January 1, 2009, the recorder shall create a copy of that record in an electronic format and truncate any social security number contained in that record.

(c) Nothing in this article shall be construed to restrict, delay, or modify access to any official record, or modify any existing agreements regarding access to any official record, prior to the creation and availability of a public record version of that official record. A county recorder shall not charge any new fee or increase any existing fees in order to fund the social security number truncation program pursuant to this article, except as provided in subdivision (d) of Section 27361.

(d) Notwithstanding subdivisions (a) and (b), a county recorder shall not be required to create a public record version of an official record if the fee authorized in Section 27304 is determined by the recorder to be insufficient to meet the cost of creating the public record version. In that case, the county recorder shall determine whether the fee is sufficient to meet the cost of creating a public record version of only a fraction of the official records described in subdivisions (a) and (b). If the fee is sufficient to meet the cost of creating a public record version of a fraction of the official records, the recorder shall be required to create a public record version of that fraction only.

27302. (a) A county recorder shall be deemed to be in compliance with the requirements of Section 27301 and shall not be liable for failure to truncate a social security number if he or she uses due diligence to locate social security numbers in official records and truncate social security numbers in the public record version of those official records. The use of an automated program with a high rate of accuracy shall be deemed to be due diligence.

(b) In the event that a county recorder fails to truncate a social security number contained in a public record, any person may request that the county recorder truncate the social security number contained in that record. Notwithstanding that a county recorder may be deemed to be in compliance with Section 27301 pursuant to subdivision (a), a county recorder that receives a request that identifies the exact location of an untruncated social security number within a specifically identified public record, shall truncate that number within 10 business days of receiving the request. The public record with the truncated social security number shall replace the record with the untruncated number.

27303. When a public record version of an official record exists, both of the following shall apply:

(a) Upon a request for inspection, copying, or any other public disclosure of an official record that is not exempt from disclosure, a county recorder shall make available only the

public record version of that record.

(b) A county recorder shall publicly disclose an official record only in response to a subpoena or order of a court of competent jurisdiction.

27304. (a) Each county may use funds generated by fees authorized by subdivision (d) of Section 27361 to implement a social security number truncation program required by this article.

(b) No later than June 1, 2008, the county recorder of each county shall petition the board of supervisors in that county for the authority to levy the fee authorized by subdivision (d) of Section 27361.

(c) It is the intent of the Legislature that in the interest of enabling county recorders to act expeditiously to protect the privacy of Californians, counties be permitted to seek revenue anticipation loans or other outside funding sources for the implementation of a social security number truncation program to be secured by the anticipated revenue from the fee authorized by subdivision (d) of Section 27361.

27305. (a) To assist the Legislature in monitoring the progress of each county recorder's social security number truncation program, the County Recorders Association of California, no later than January 1, 2009, and annually thereafter, shall submit to the chairpersons of the Assembly Committee on Judiciary and of the Senate Committee on Judiciary, and to the Office of Privacy Protection, or any successor agency, a report on the progress each county recorder has made in complying with this article.

(b) Upon the Office of Privacy Protection making a determination that all counties have completed the component of the program described in subdivision (a) of Section 27301, the report described in subdivision (a) of this section shall no longer be required.

27307. A county recorder is authorized to take all actions required by this article notwithstanding subdivision (d) of Section 27203 or any other provision of law.

Summary of Government Code Section 15705: Franchise Tax Board Records

This law requires the Franchise Tax Board to truncate SSNs in documents released to the public.

Text of Government Code Section 15705

15705. Notwithstanding any other provision of law, unless prohibited by federal law, the Franchise Tax Board shall truncate social security numbers on lien abstracts and any other records created by the board that are disclosable under Chapter 3.5 (commencing with Section 6250) of Division 7 of Title 1 before disclosing the record to the public. For purposes of this section, "truncate" means to redact the first five digits of a social security number.

Summary of California Family Code Section 2024.5: Certain Court Records

This law establishes a procedure for keeping SSNs confidential in court filings for legal separation, dissolution, or nullification of marriage.

Text of Family Code Section 2024.5

2024.5. (a) Except as provided in subdivision (b), the petitioner or respondent may redact any social security number from any pleading, attachment, document, or other written material filed with the court pursuant to a petition for dissolution of marriage, nullity of marriage, or legal separation. The Judicial Council form used to file such a petition, or a response to such a petition, shall contain a notice that the parties may redact any social security numbers from those pleadings, attachments, documents, or other material filed with the court. (b) An abstract of support judgment, the form required pursuant to subdivision (b) of Section 4014, or any similar form created for the purpose of collecting child or spousal support payments may not be redacted pursuant to subdivision (a).

Summary of Code of Civil Procedure Section 674: Abstracts of Judgment

Abstracts of judgment and decrees requiring the payment of money may contain only the last four digits of the judgment debtor's SSN.

Text of Code of Civil Procedure Section 674

674. (a) Except as otherwise provided in Section 4506 of the Family Code, an abstract of a judgment or decree requiring the payment of money shall be certified by the clerk of the court where the judgment or decree was entered and shall contain all of the following:

(1) The title of the court where the judgment or decree is entered and cause and number of the action.

(2) The date of entry of the judgment or decree and of any renewals of the judgment or decree and where entered in the records of the court.

(3) The name and last known address of the judgment debtor and the address at which the summons was either personally served or mailed to the judgment debtor or the judgment debtor's attorney of record.

(4) The name and address of the judgment creditor.

(5) The amount of the judgment or decree as entered or as last renewed.

(6) The last four digits of the social security number and driver' s license number of the judgment debtor if they are known to the judgment creditor. If either or both of those sets of numbers are not known to the judgment creditor, that fact shall be indicated on the abstract of judgment.

(7) Whether a stay of enforcement has been ordered by the court and, if so, the date the stay ends.

(8) The date of issuance of the abstract.

(b) An abstract of judgment, recorded after January 1, 1979, that does not list the social security number and driver's license number of the judgment debtor, or either of them, as required by subdivision (a) or by Section 4506 of the Family Code, may be amended by the recording of a document entitled "Amendment to Abstract of Judgment." The Amendment to Abstract of Judgment shall contain all of the information required by this section or by Section 4506 of the Family Code, and shall set forth the date of recording and the book and page location in the records of the county recorder of the original abstract of judgment.

A recorded Amendment to Abstract of Judgment shall have priority as of the date of recordation of the original abstract of judgment, except as to any purchaser, encumbrancer, or lessee who obtained their interest after the recordation of the original abstract of judgment but prior to the recordation of the Amendment to Abstract of Judgment without actual notice of the original abstract of judgment. The purchaser, encumbrancer, or lessee without actual notice may assert as a defense against enforcement of the abstract of judgment the failure to comply with this section or Section 4506 of the Family Code regarding the contents of the original abstract of judgment notwithstanding the subsequent recordation of an Amendment to Abstract of Judgment. With respect to an abstract of judgment recorded between January 1, 1979, and July 10, 1985, the defense against enforcement for failure to comply with this section or Section 4506 of the Family Code may not be asserted by the holder of another abstract of judgment or involuntary lien, recorded without actual notice of the prior abstract, unless refusal to allow the defense would result in prejudice and substantial injury as used in Section 475. The recordation of an Amendment to Abstract of Judgment does not extend or otherwise alter the computation of time as provided in Section 697.310.

(c) (1) The abstract of judgment shall be certified in the name of the judgment debtor as listed on the judgment and may also include the additional name or names by which the judgment debtor is known as set forth in the affidavit of identity, as defined in Section 680.135, filed by the judgment creditor with the application for issuance of the abstract of judgment. Prior to the clerk of the court certifying an abstract of judgment containing any additional name or names by which the judgment debtor is known that are not listed on the judgment, the court shall approve the affidavit of identity. If the court determines, without a hearing or a notice, that the affidavit of identity states sufficient facts upon which the judgment creditor has identified the

additional names of the judgment debtor, the court shall authorize the certification of the abstract of judgment with the additional name or names.

(2) The remedies provided in Section 697.410 apply to a recorded abstract of a money judgment based upon an affidavit of identity that appears to create a judgment lien on real property of a person who is not the judgment debtor.

Summary of Revenue and Taxation Code Section 2191.3: Tax Liens

Tax collector liens may contain only the last four digits of SSNs.

Text of Revenue and Taxation Code Section 2191.3

2191.3. (a) The tax collector may make the filing specified in subdivision (b) where either of the following occurs:

(1) There is a tax on any of the following:

(A) A possessory interest secured only by a lien on that taxed possessory interest.

(B) Goods in transit, not secured by any lien on real property.

(C) Improvements that have been assessed pursuant to Section 2188.2.

(D) Off-roll taxes on escape assessments where the error was not the fault of the assessee and the escape taxes are being paid pursuant to Section 4837.5.

(E) Unsecured property not secured by a lien on any real property, and where the tax has become delinquent or where there are prior unpaid and delinquent taxes with respect to that same property.

(2) A tax has been entered on the unsecured roll pursuant to Section 482, 531.2, or 4836.5, or transferred to the unsecured roll pursuant to any provision of law.

(b) A filing for record without fee in the office of the county recorder of any county of a certificate specifying the amount due, the name, the last four digits of his or her federal social security number, if known, and last known address of the assessee liable for the amount, and compliance with all provisions of this division with respect to the computation and levy of the tax if compliance has in fact occurred. The procedure authorized by this section is cumulative to the procedure provided by Sections 2951 and 3003. The county recorder shall, within 30 days after a filing as described in this subdivision with respect to delinquent taxes on unsecured property, send a notice of the filing to the assessee at the assessee's last known address. The notice shall contain the information contained in the filing, and shall prominently display on its face the following heading:

"THIS IS TO NOTIFY YOU THAT A TAX LIEN HAS BEEN FILED WITH RESPECT TO UNSECURED PROPERTY"

Appendix 2: Federal Laws Authorizing or Mandating SSNs

The following list of federal laws authorizing or mandating the collection and use of Social Security numbers is not comprehensive. It is taken from a report of the U.S. Government Accountability Office, *Social Security Numbers: Federal and State Laws Restrict Use of SSNs, Yet Gaps Remain* (GAO-05-1016T of September 15, 2005).

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, motorvehicle 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
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

Federal Statute	General purpose for collecting or using SSN	Government entity and authorized or required use
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 caue 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. 5101(c)	Eligibility for Veterans Affairs compensation or pension benefitsprograms	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

Federal statute	General purpose for collecting or using SSN	Gpvernmemt 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; creates national database for child support enforcement purposes
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 3: Federal Laws Restricting Disclosure of SSNs

The following list of federal laws that restrict the disclosure of Social Security numbers is not comprehensive. It is taken from a U.S. Government Accountability Office report, *Social Security Numbers: Government Benefits from SSN Use but Could Provide Better Safeguards* (GAO-02-352, May 2002).

The Freedom of Information Act (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 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 Office of Privacy Protection
www.privacy.ca.gov

Office of Information Security and Privacy Protection
www.oispp.ca.gov

State and Consumer Services Agency
www.scsa.ca.gov