Consumer Privacy and Identity Theft: A Summary of Key Statutes

California State Senate
Senate Office of Research
February 2006

Consumer Privacy and Identity Theft: A Summary of Key Statutes

by Saskia Kim

California State Senate
Senate Office of Research
Don Moulds, Director
1020 N Street, Suite 200
Sacramento, California 95814
(916) 651-1500
www.sen.ca.gov/sor

Updated February 2006

Contents

Introduction

In recent years, the issue of one's privacy and the protection of nonpublic personal information has been of considerable interest to the California Legislature and Congress. Unlike the U.S. Constitution, the California Constitution explicitly protects an individual's right to privacy. But simply stating in the constitution that individuals have a right to privacy does not end the discussion—far from it. Matters that have been legislated range from the public posting of social security numbers to the sharing of consumers' nonpublic personal information by financial institutions. And the debate continues.

Recent studies indicate that consumers are increasingly worried about protecting their privacy. A CBS News/New York Times poll released on October 2, 2005, found that 52 percent of Americans believe that the right to privacy in the United States is "under serious threat," while 30 percent believe "it has already been lost." The same poll showed that 83 percent of respondents agreed that the collection of personal information by companies is "mostly a bad thing because it makes it easier for the information to be shared inappropriately." Thirteen percent, on the other hand, believe collecting personal data is "mostly good because it allows companies to better serve their customers and process financial transactions quickly."

In June 2005, 78 percent of respondents to a Privacy & American Business and Deloitte & Touche LLP survey agreed that "consumers have lost all control over how personal information is collected and used by companies." Fifty-nine percent also agreed that "existing laws and organization practices do not provide a reasonable level of protection for consumer privacy today."[1] And a June 2005 telephone survey conducted for the Cyber Security

[1] Privacy & American Business and Deloitte & Touche LLP survey, conducted by Harris Interactive, June 29, 2005.

Industry Alliance found that 97 percent of respondents think identity theft is a serious problem.[2]

In light of the extensive interest in this issue, this report provides an overview of key state and federal laws relating to consumer privacy and identity theft. While the descriptions provide a brief synopsis of the relevant laws, they are not exhaustive, and the reader is encouraged to consult the statutory texts for more detail.

In some cases, measures passed by the Legislature and signed by the governor during the 2005 legislative session amended or added the relevant statutes. The descriptions contained in this report incorporate these changes, indicating that they became effective January 1, 2006.

Please note that all citations to the Fair Credit Reporting Act (FCRA), Section 601, 15 U.S.C. 1681 et seq., include amendments to the FCRA set forth in the Fair and Accurate Credit Transactions Act of 2003 (FACT Act), Pub. L. 108-159, 117 Stat. 1952. In addition, it is important to point out that the preemption language included in the FCRA, as amended by the FACT Act, may vary. For example, in some instances Congress precluded states from enacting requirements "with respect to the conduct required" by specific provisions of the FCRA. [Fair Credit Reporting Act Section 625(b)(5), 15 U.S.C. 1681t]

In other cases, states are preempted from enacting any requirement or prohibition "with respect to any subject matter regulated" under a specified provision. [Fair Credit Reporting Act Section 625(b)(1), 15 U.S.C. 1681t]

Whether or not these federal provisions preempt state laws has not yet been tested in court. As a result, the extent and practical effect of the preemption provisions is not yet known.

[2] Cyber Security Industry Alliance survey, conducted by Pineda Consulting, June 15, 2005.

The Constitution and General Privacy

Constitutional Right to Privacy – Specifies in the California Constitution that all people have an inalienable right to pursue and obtain privacy. [California Constitution, Article I, Section 1]

California's constitution gives Californians greater privacy protections than those recognized by the U.S. Constitution. For example, whereas federal protections apply only to government action, California's right to privacy protects individuals from actions by both the government and private entities. [See, for example, *American Academy of Pediatrics*, 16 Cal. 4th at 326, citing *Skinner v. Railway Labor Executives' Assn.* (1989) 489 U.S. 602; *Hill v. National Collegiate Athletic Association* (1994) 7 Cal. 4th 1, 15-20]

The California Supreme Court has held that the California Constitution in and of itself "creates a legal and enforceable right of privacy for every Californian." [*White v. Davis* (1975) 13 Cal. 3d 757, 775]

To successfully assert a claim for invasion of one's constitutional right to privacy, an individual must prove there was a legally protected privacy interest, he or she had a reasonable expectation of privacy in the circumstances, and the defendant committed some conduct constituting a serious invasion of privacy. [*Hill*, 7 Cal. 4th at 39-40]

Constructive Invasion of Privacy – Provides civil liability for the constructive invasion of privacy when a defendant attempts to capture, in a manner offensive to a reasonable person, any type of visual image, sound recording, or other physical impression of an individual engaging in a personal or familial activity. The individual must have had a reasonable expectation of privacy in the circumstances, and the image, recording, or impression must have

been obtained through a visual or auditory enhancing device. [California Civil Code Section 1708.8(b)]

Invasion of Privacy: Common Law Tort – Provides civil liability for invasion of privacy under the common law. While full treatment of this common law tort is beyond the scope of this report, four types of activities are considered invasions of privacy, giving rise to civil liability:

1. Intrusion upon the plaintiff's seclusion or solitude or into his or her private affairs;

2. Public disclosure of private facts about the plaintiff;

3. Publicity that places the plaintiff in a false light in the public eye; and

4. Misappropriation, for the defendant's advantage, of a person's name or likeness. [*Hill*, 7 Cal. 4th at 24; *Kapellas v. Kofman* (1969) 1 Cal. 3d 20, 35, fn. 16]

An injured plaintiff may recover damages for a violation. [*Metter v. Los Angeles Examiner* (1939) 35 Cal. App. 2d 304, 310]

However, not every kind of conduct appearing to fall within one of the four categories noted above gives rise to a common law cause of action for invasion of privacy. Instead, courts generally consider whether the conduct in question is "highly offensive to a reasonable person," considering, among other things, "the degree of the intrusion, the context, conduct and circumstances surrounding the intrusion, as well as the intruder's motives and objectives, the setting into which he intrudes, and the expectations of those whose privacy is invaded." [*Hill*, 7 Cal. 4th at 25-26, citing *Miller v. National Broadcasting Co.* (1986) 187 Cal. App. 3d 1463, 1483-1484]

Invasion of Privacy: Penal Code – Prohibits the invasion of privacy with the intent to protect Californians' right to privacy. [California Penal Code Section 630 et seq.]

Among other things, the invasion of privacy statutes contain criminal penalties for unauthorized wiretapping, electronic

eavesdropping, intercepting cellular telephone communications, and electronic tracking of individuals, except as specified.

Preemption – Provides, under the doctrine of federal preemption, that Congressional action pursuant to an enumerated power may override state laws. There are three tests the courts refer to in deciding whether federal regulation preempts state law: (1) express preemption in which Congress, through explicit statutory language, prohibits states and localities from legislating in specific areas; (2) implied preemption in which Congress "occupies the field"; and (3) conflict preemption in which it is impossible for an entity to comply with both state and federal law at the same time. Even where preemption is found, the court still may have to determine the precise extent of the preemption. There has been heightened interest in the issue of preemption regarding state laws that relate to consumer privacy and identity theft, as Congress increasingly has included preemption provisions in federal legislation.

Credit Cards

Activation Process Required for Substitute Credit Cards – Requires a credit card issuer to prohibit a substitute credit card from being issued unless the cardholder is required to take steps to activate the card before using it. [California Civil Code Section 1747.05]

Change of Address and Request for Replacement Credit Card – Requires a credit card issuer—when the issuer receives a change of address request from a cardholder as well as a replacement credit card request within 60 days—to send a change of address notice to the cardholder at his or her previous address. [California Civil Code Section 1799.1b]

When a credit card issuer receives a request to change a cardholder's billing address, and a request for an additional credit card within 10 days, the issuing company is prohibited from activating the card or mailing a new card until it has verified the address change. [California Civil Code Section 1747.06(c)]

Federal law also touches on this subject. The Fair Credit Reporting Act (FCRA), as amended by the Fair and Accurate Credit Transactions Act of 2003 (FACT Act), requires the Federal Trade Commission, National Credit Union Administration, and specified banking agencies to issue regulations on this matter. The regulations must ensure that if a card issuer receives notification of an address change for an existing account, and receives a request for an additional or a replacement card for the same account within at least 30 days after the change-of-address notification is received, the card issuer may not issue the replacement or the additional card unless the issuer notifies the cardholder at his or her former address, or uses other means of verifying the address change. At the time this report was written, the regulations had not yet been issued; as a result, any preemptive effect of the regulations on the state law provisions

described above is not yet known. [Fair Credit Reporting Act Section 615(e)(1)(C), 15 U.S.C. 1681m. See also Section 625(b)(5)(F) for specific preemption provision]

Credit Card Numbers Printed on Receipts – Prohibits any person who accepts credit cards for payment from printing more than the last five digits of the credit card account number or the expiration date on a receipt. The prohibition applies only to receipts that are electronically printed and does not apply to transactions in which the sole means of recording the person's credit card number is by handwriting or an imprint or copy of the card. As of January 1, 2006, this provision also applies to the last five digits of a debit card account number. [California Civil Code Section 1747.09]

The FCRA, as amended by the FACT Act, contains a substantially similar provision under federal law. Specifically, the law requires businesses to truncate credit card and debit card numbers on electronic receipts issued at the point of sale. The effective date of the statute depends upon when the cash register or machine used to electronically print receipts was first put into use. [Fair Credit Reporting Act Section 605(g), 15 U.S.C. 1681c]

The FCRA preempts state law requirements with respect to the conduct required by the provision. [Fair Credit Reporting Act Section 625(b)(5)(A), 15 U.S.C. 1681t]

Because the nearly identical federal law is not yet fully implemented, and California's statute became fully operative on January 1, 2004, the state law will remain in effect pending federal law becoming operative.

Fraudulent Use of Information Stored on Credit or Debit Cards – Provides that any person who knowingly, willfully, and with the intent to defraud uses a scanning device to access, read, obtain, memorize, or store information encoded on the magnetic strip of a credit card, debit card, or other payment card is guilty of a misdemeanor. [California Penal Code Section 502.6]

Recording Credit Card Numbers on Checks – Prohibits retailers, when a consumer pays for goods or services by check, from requiring that the consumer provide a credit card as a condition of accepting the check or recording the credit card's number. [California Civil Code Section 1725]

Recording Personal Information on Credit Card Transaction Forms – Prohibits any person who accepts a credit card for payment from recording the consumer's personal identification information on the credit card transaction form, except as specified. [California Civil Code Section 1747.08]

Verification of Credit Applicant's Address – Requires, under state law, a credit card issuer who mails a credit card solicitation and, in response, receives a completed credit card application that lists an address different from the one on the solicitation, to verify the change of address by contacting the person to whom the solicitation was mailed. [California Civil Code Section 1747.06]

The FCRA, as amended by the FACT Act, contains related provisions under federal law. The FCRA now requires nationwide consumer reporting agencies to notify a credit-report requester when a consumer's address differs substantially from the addresses in the consumer's file. The requester of the report must then comply with regulations specifying the procedure to be followed; however, at the time this report was written, these regulations had not yet been issued. [Fair Credit Reporting Act Section 605(h), 15 U.S.C. 1681c]

The FCRA also requires the Federal Trade Commission, National Credit Union Administration, and specified banking agencies to establish and maintain "red flag" guidelines and related regulations to alert financial institutions and creditors to potential signs of identity theft and to help prevent such theft. In addition, regulations will require financial institutions and creditors to establish reasonable policies and procedures to "identify possible risks to account holders or customers or to the safety and soundness of the institution or customers." [Fair Credit Reporting Act Section 615(e), 15 U.S.C. 1681m]

These regulations, which have not yet been issued, are intended to preempt state laws with respect to the conduct required by the specified provisions. [Fair Credit Reporting Act Section 625(b)(5)(F), 15 U.S.C. 1681t]

Credit Reporting

Consumer Credit Reporting Agencies Act – Creates a state law counterpart to the Fair Credit Reporting Act (FCRA) regulating consumer credit reporting agencies. Among other things, the statute requires every consumer credit reporting agency to allow a consumer, upon request and proper identification, to visually inspect all files pertaining to him or her that the agency maintains. The agency must identify any recipients who obtained the consumer's credit report, and disclose a record of all inquiries within the preceding 12 months that identified the consumer in connection with a credit transaction not initiated by the consumer. [California Civil Code Section 1785.10]

A consumer may request that his or her name and address be removed from lists that a consumer credit reporting agency furnishes for credit card solicitations. [California Civil Code Sections 1785.11(d)(1) and 1785.11.8]

Existing law also permits consumers to dispute inaccurate information and requires a consumer credit reporting agency to reinvestigate disputed information. [California Civil Code Section 1785.16]

A consumer credit reporting agency must delete from a consumer's credit report all inquiries that the agency has verified were the result of identity theft [California Civil Code Section 1785.16.1], and it must block information appearing on the consumer credit report that is a result of identity theft. [California Civil Code Section 1785.16(k)]

Any person who uses a consumer credit report to extend credit must take reasonable steps to verify the accuracy of the consumer's personal information if the first and last name, address, or social security number provided on the credit application does not match, within a reasonable degree of

certainty, the information listed on the credit report. [California Civil Code Section 1785.20.3(a) See "Verification of Credit Applicant's Address" on page 13 for related FCRA provisions]

If the user of the consumer credit report has been notified that the applicant has been a victim of identity theft, he or she may not lend money or extend credit without taking reasonable steps to verify the consumer's identity and confirm that the application is not the result of identity theft. [California Civil Code Section 1785.20.3(b)]

Fair Credit Reporting Act (FCRA) – Provides consumers, upon request, with one free credit report from each nationwide consumer reporting agency in a 12-month period. [Fair Credit Reporting Act Section 612(a),15 U.S.C. 1681j, as amended by the Fair and Accurate Credit Transactions Act (FACT Act) of 2003, Pub. L. 108-159, 117 Stat. 1952]

Except as specified, a consumer reporting agency is required to clearly and accurately disclose to a consumer:

1. All information in his or her file at the time of the request;

2. The sources of the information;

3. Identification of each person who obtained a consumer report;

4. The dates, original payees, and amounts of any checks upon which an adverse characterization of the consumer is based;

5. A record of all inquiries received by the credit reporting agency during the preceding one-year period where the consumer was identified with a credit or insurance transaction that he or she did not initiate; and

6. A notification that the consumer also may request his or her credit *score*, if the consumer originally only requested a copy of his or her credit *file.* [Fair Credit Reporting Act Section 609(a), 15 U.S.C. 1681g]

The FACT Act amendments to the FCRA also permit a consumer to dispute inaccurate information directly with the entity that furnished the information to the consumer reporting agency; it

also requires that the entity investigate the disputed information. [Fair Credit Reporting Act Section 623(a)(8),15 U.S.C. 1681s-2]

If an entity learns that it provided inaccurate or incomplete information to a consumer reporting agency, it must promptly notify the agency and provide accurate and complete information. The entity also is required to notify all consumer reporting agencies that received the information of the correction. [Fair Credit Reporting Act Section 623(a)(2), 15 U.S.C. 1681s-2]

If the consumer's file contains information that resulted from an alleged identity theft and the consumer provides documentation supporting this claim, the consumer reporting agency is required to block the reporting of that information and notify the entity that supplied the information related to the identity theft. [Fair Credit Reporting Act Section 605B, 15 U.S.C. 1681c-2]

That entity also must have in place reasonable procedures to prevent refurnishing the information related to the identity theft in the future.

Please note that additional significant provisions of the FCRA, as amended by the FACT Act, are described in other summaries throughout this report.

Investigative Consumer Reporting Agencies – Regulates investigative consumer reporting agencies under state law and defines such agencies as any person, corporation, or other entity that collects, reports, or transmits information concerning consumers for the purpose of providing investigative consumer reports to third parties. Investigative consumer reports may be given only to third parties the agency believes is using the information: (1) for employment purposes; (2) to determine a consumer's eligibility for insurance; (3) in connection with the leasing of a residential unit; or (4) for other specified reasons. [California Civil Code Section 1786 et seq.]

Security Alerts – Allows a consumer to place a "security alert" on his or her credit report noting that his or her identity may have been used without consent to fraudulently obtain goods or services in the consumer's name. The alert remains in place for at least 90 days, and the consumer may renew the alert. Any person who receives notice of the security alert and who uses the consumer's

credit report to approve credit may not lend money, extend credit, or complete the purchase, lease, or rental of goods or services without first taking reasonable steps to verify the consumer's identity to ensure that the application is not the result of identity theft. [California Civil Code Section 1785.11.1]

The FCRA, as amended by the FACT Act, contains related provisions under federal law regarding nationwide consumer reporting agencies. These provisions permit a consumer to place one of three kinds of "alerts" on their credit files maintained by nationwide agencies: (1) a fraud alert; (2) an extended fraud alert; or (3) an active-duty alert. The three alerts differ in what is required to initiate them, the length of time they are imposed, and the limits that are imposed on users of a consumer's report. However, the consumer reporting agency that receives any one of the three alerts must forward the pertinent information to the other nationwide consumer reporting agencies. This requirement allows consumers to place an alert on their files with a call to only one nationwide credit reporting agency. [Fair Credit Reporting Act Section 605A, 15 U.S.C. 1681c-1]

A fraud alert lasts for 90 days, and consumers may place one on their credit file if they suspect they are—or are about to become—a victim of fraud or a related crime, including identity theft. Extended fraud alerts remain in place for seven years, and in order to place one on their file, consumers must submit an identity theft report. Active-duty military personnel also may place alerts on their credit reports for 12 months; this period may be renewed if an individual receives an extended deployment. [Fair Credit Reporting Act Sections 605A(a)-(c), 15 U.S.C. 1681c-1]

All three alerts must state that the consumer does not authorize new credit, the issuance of an additional credit card, or any increase in a credit limit on an existing account. For fraud and active-duty alerts, persons or businesses who use the consumer's report must "utilize reasonable policies and procedures to form a reasonable belief that the user knows the identity of the person making the request." They may either contact the consumer at a designated telephone number or take reasonable steps to verify the consumer's identity and confirm that the application is not the result of identity theft. For an extended alert, however, they must contact the consumer in person or use another method designated by the consumer to confirm that the application is not the result of

identity theft. [Fair Credit Reporting Act Section 605A(h), 15 U.S.C. 1681c-1]

Congress preempted states from enacting any requirement or prohibition with respect to the conduct required by these specific provisions. [Fair Credit Reporting Act Section 625(b)(5)(B), 15 U.S.C. 1681t]

However, states may be able to act where federal law does not impose a specific requirement. While the extent of this preemption standard has yet to be tested in court, in those areas where federal law is silent with respect to conduct required, a state arguably remains free to act.

Security Freezes – Allows a consumer to place a "security freeze" on his or her credit report, which prohibits credit reporting agencies from releasing the consumer's credit report or any information from it without the consumer's authorization. The security freeze remains in place until the consumer requests its removal. Credit reporting agencies may charge a consumer no more than $10 for each security freeze, removal of the freeze, or a temporary lift of the freeze for a specific time period, and no more than $12 for a temporary lift of the freeze for a specific party; no fee may be charged to a victim of identity theft, as specified. [California Civil Code Section 1785.11.2]

Data Security

Destruction of Business Records – Requires businesses, when disposing of customer records, to take all reasonable steps to destroy personal information in the records by shredding, erasing, or otherwise modifying the personal information so that it is unreadable or undecipherable. [California Civil Code Section 1798.81]

Federal law also addresses this issue. For consumer reports or information derived from such reports, the Fair Credit Reporting Act (FCRA), as amended by the Fair and Accurate Credit Transactions Act of 2003 (FACT Act), requires businesses and individuals to take appropriate measures to dispose of such sensitive information. The law applies to anyone who uses consumer reports and covers information obtained from a consumer reporting agency that is used, or is expected to be used, in establishing a consumer's eligibility for credit, employment, or insurance, among other things. [Fair Credit Reporting Act Section 628, 15 U.S.C. 1681w]

The FCRA preempts state law requirements "with respect to the conduct required" by its document-destruction provision. [Fair Credit Reporting Act Section 625(b)(5)(I), 15 U.S.C. 1681t]

As with other parts of the FACT Act where Congress preempted states from enacting any requirement or prohibition regarding the "conduct required by specific provisions," states still may be able to act where federal law does not impose a specific requirement. The extent and practical effect of the preemption provisions of the FACT Act are not yet known. It also is important to note that since California law is broader—applying to more than just information obtained from credit reports—the preemptive effect of the FCRA on the state law described above may be limited.

Notification of Breach in Data Security – Requires state agencies and businesses that own or license computerized data containing personal information to disclose any breach of the system's security to a California resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made in the most expedient manner and without unreasonable delay (although the notification may be delayed if a law enforcement agency determines it will impede a criminal investigation).

State agencies and businesses that maintain, but do not own, computerized data that includes personal information are required to notify the owner or licensee of the information of any security breach of the data immediately following the discovery if personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The statutes contain related definitions of key terms, such as "breach of the security of the system," "personal information," and "notice." [California Civil Code Sections 1798.29 and 1798.82]

Personal Information: Reasonable Security Procedures – Requires a business that owns or licenses personal information about a California resident to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect personal information from unauthorized access, destruction, use, modification, or disclosure. Similar requirements apply when a business discloses information about a California resident pursuant to a contract with a nonaffiliated third party. The section does not apply to financial institutions, health care providers, or other specified entities. [California Civil Code Section 1798.81.5]

Financial Privacy and Related Issues

California Financial Information Privacy Act – Places restrictions on the sharing of consumers' nonpublic personal information[3] by financial institutions. A financial institution must first obtain the consent of a consumer before it may disclose or share the consumer's nonpublic personal information with any nonaffiliated third party (known as an "opt-in"). And before disclosing nonpublic personal information to an affiliate, a financial institution must give a consumer an opportunity to direct that his or her information not be disclosed (known as an "opt-out").[4] Provided that the consumer has not opted out, a financial institution may share the consumer's personal information with another financial institution when they enter into a joint marketing agreement to offer a financial product or service that meets specified requirements. The unrestricted sharing of nonpublic personal information between a financial institution and its wholly owned financial-institution subsidiaries in the same line of business also is permitted, irrespective of any consumer choice, provided that specified requirements are met. [California Financial Code Sections 4053(a)-(c)]

---

[3] Nonpublic personal information is defined as personally identifiable financial information that is: (1) provided by a consumer to a financial institution; (2) the result of a transaction with a consumer or a service performed for a consumer; or (3) otherwise obtained by a financial institution. Nonpublic personal information does not include publicly available information. [California Financial Code Section 4052]

[4] This provision was challenged by the American Bankers Association, the Financial Services Roundtable, and the Consumer Bankers Association on the basis that it was preempted by the Fair Credit Reporting Act (FCRA). The U.S. Court of Appeal for the Ninth Circuit agreed and directed the U.S. District Court to determine the scope of the preemption. On October 5, 2005, the district court issued its ruling that no part of this provision survives preemption and enjoined the state from enforcing the affiliate-sharing restrictions to the extent they are preempted by the FCRA. The court made clear in its ruling, however, that other provisions of California's financial privacy law still stand. On November 3, 2005, the attorney general's office filed a notice of appeal with the U.S. Court of Appeal for the Ninth Circuit. This appeal is currently pending.

Existing California law contains a statutory form that a financial institution may use to offer consumers an opportunity to communicate their privacy choices. A financial institution that uses the statutory form is deemed to have complied with the notice requirements; a financial institution also may use an alternate form subject to specified limitations. [California Financial Code Section 4053(d)]

Fair Debt Collection Practices Act – Regulates the business practices of third-party debt collectors under federal law by, among other things, requiring a debt collector to make an initial disclosure to the debtor that the collector is attempting to collect a debt and that any information obtained will be used for that purpose. The act also prohibits any threats, harassment, or various false or misleading representations, and limits the amount of information about a debtor that a collector may reveal to a third party. The act specifically allows for state regulation regarding debt collection practices, provided that state laws are not inconsistent with federal law. State laws may even give consumers greater protection than federal law. [Fair Debt Collection Practices Act, 15 U.S.C. 1692 et seq.]

Also see the "Rosenthal Fair Debt Collection Practices Act" on page 25.

Gramm-Leach-Bliley Act (GLB) – Prohibits, under federal law, a financial institution from disclosing a consumer's nonpublic personal information to a nonaffiliated third party unless the financial institution: (1) provides the consumer with a clear and conspicuous disclosure of specified privacy policies and practices of the financial institution; (2) gives the consumer the opportunity to stop the disclosure before the information is initially disclosed; and (3) provides the consumer with an explanation of how to exercise his or her right to opt out.

Under the GLB, financial institutions are permitted to disclose personal information to a third party, even if a consumer has opted out, if the disclosure is to enable the third party to perform services for or functions on behalf of the financial institution, including the marketing of the institution's own products or services, or products or services offered jointly between two or more financial institutions that comply with the provisions of the GLB Act (often referred to as a "joint marketing agreement"). In

this case, the financial institution must enter into a contractual agreement with the third party that requires the third party to maintain the confidentiality of the information. The GLB also specifically invites states to enact greater privacy protections than those contained in the federal act. [Gramm-Leach-Bliley Act of 1999, Pub. L. 106-102, 113 Stat. 1338]

Insurance Information and Privacy Protection Act – Governs the collection, use, and disclosure of information gathered in connection with insurance transactions. The act limits disclosure of personal information by insurers and agents without the written consent of the individual. [California Insurance Code Section 791 et seq.]

Rosenthal Fair Debt Collection Practices Act – Regulates third-party debt collectors in a manner that is similar to the federal law described in "Fair Debt Collection Practices Act" on page 24. State law also prohibits any threats, harassment, or various false or misleading representations, and limits the amount of information about a debtor that a collector may reveal to a third party. Furthermore, the act allows debtors to bring an action for actual damages against a debt collector who has violated the statute. [California Civil Code Section 1788 et seq.]

Identity Theft

Crime of Identity Theft – Provides that it is unlawful to willfully use someone else's personal identifying information for an unlawful purpose, including to obtain or even attempt to obtain credit, goods, services, or medical information in the name of the other person without the consent of that person. "Personal identifying information" includes, among other things, name, address, telephone number, social security number, driver's license number, mother's maiden name, checking or savings account number, unique biometric data (such as a fingerprint), or credit card number. As of January 1, 2006, higher fines now can be imposed on the perpetrator of the identity theft if the crime victim is a deployed member of the military services. [California Penal Code Section 530.5]

Debt Collection Activities – Requires debt collectors to cease collection activities for a specific debt if a debtor provides a police report showing that he or she is the victim of an identity theft crime for that particular debt. The debtor also must provide a written statement declaring that, for the debt in question, he or she has been the victim of an identity theft. The debt collector must review the information provided by the debtor and may only recommence collection activities upon a good faith determination that the information and police report do not establish that the debtor is not responsible for the debt in question. [California Civil Code Section 1788.18]

Deceptive Identification Documents – Provides that, as of January 1, 2006, it is a misdemeanor to possess a document-making device with the intent to manufacture, alter, or authenticate a deceptive identification document. [California Penal Code Section 483.5]

Department of Justice Identity Theft Victim Database – Requires the department to create and maintain a database

of identity theft victims and limit access to criminal justice agencies, identity theft victims, and individuals and agencies authorized by the victims. [California Penal Code Section 530.7]

Falsely Obtaining Department of Motor Vehicles' Documents – Provides that it is a misdemeanor for any person to obtain, or assist another person in obtaining, a driver's license, identification card, vehicle registration certificate, or any other official document issued by the Department of Motor Vehicles with the knowledge that the person obtaining the document is not entitled to it. [California Penal Code Section 529.7]

In addition, in many cases those involved in obtaining false Department of Motor Vehicles' documents can be prosecuted for felony conspiracy (a conspiracy is an agreement between two or more people to commit a crime and acts done in furtherance of the criminal goal of the conspiracy). A person convicted of conspiracy to commit identity theft may be fined by up to $25,000. [California Penal Code Section 182]

Identity Theft Victim's Right to Free Credit Reports – Requires, under state law, consumer credit reporting agencies to provide identity theft victims with up to 12 free copies of their credit files during a consecutive 12-month period, not to exceed one copy per month. The victim first must provide an identity theft police report or a similar report. [California Civil Code Section 1785.15.3(b)]

The Fair Credit Reporting Act (FCRA), as amended by the Fair and Accurate Credit Transactions Act of 2003 (FACT Act), similarly requires nationwide consumer reporting agencies to provide free reports to identity theft victims under federal law. A consumer who requests adding a fraud alert to his or her file is entitled to a free copy of the file; a consumer who requests an extended fraud alert and submits an identity theft report may have two free copies during a 12-month period that begins the date the alert was added (for more information on fraud alerts, see "Security Alerts" on page 17). [Fair Credit Reporting Act Section 605A(a)(2) and (b)(2), 15 U.S.C. 1681c-1]

Congress included preemption language in the FACT Act amendments to the FCRA and provided that state laws with

respect to the conduct required by these sections are preempted. [Fair Credit Reporting Act Section 625(b)(5)(B), 15 U.S.C. 1681t]

However, it has not yet been tested in court whether a state law that gives more rights (or, in this case, more free credit reports) to identity theft victims, as California law does, would be preempted by a federal law that grants some—but more limited—rights. In addition, federal law applies only to nationwide credit reporting agencies.

Issuance of a Search Warrant – Permits a magistrate in the county where an identity theft victim resides to issue a warrant to search a person or property in another county. [California Penal Code Section 1524]

Judicial Determination of Innocence – Permits a person who reasonably believes that he or she is an identity theft victim to petition a court for an expedited judicial determination of his or her factual innocence for crimes committed by the identity thief. This provision applies when: (1) the identity thief was arrested or cited for or convicted of a crime using the victim's identity; (2) a criminal complaint was filed against the identity thief in the victim's name; or (3) the victim's identity was mistakenly associated with a criminal record. If the court determines there is no reasonable cause to believe that the victim committed the offense, it shall find the victim innocent and issue an order certifying this finding. [California Penal Code Sections 530.6(b) and 851.8]

Jurisdiction for Prosecuting Identity Theft Crime – Specifies that the jurisdiction of a criminal action for unauthorized use of personal identifying information includes either the county where the theft of the information occurred, or the county where the information was used for an illegal purpose. [California Penal Code Section 786(b)]

Law Enforcement Investigation Required – Requires law enforcement to complete a police report and begin an investigation when contacted by a person who has learned or suspects that he or she is a victim of identity theft. [California Penal Code Section 530.6(a)]

Right to Bring Legal Action Against Claimant – Gives identity theft victims the right to bring legal action against a person who purports to have a claim to money or property in connection with a transaction procured through identity theft. The victim may seek an injunction, actual damages, attorney's fees and costs, and any equitable relief deemed appropriate by the court. [California Civil Code Section 1798.92 et seq.]

Right to Obtain Records of Fraudulent Transactions or Accounts – Provides that if an identity theft victim discovers that an unauthorized person has filed an application in his or her name for, among other things, a loan, credit card, public utility service, or mail receiving or forwarding service, the victim is entitled to receive information related to the application or account, including a copy of the application and a record of transactions or charges associated with the account. The victim first must provide a copy of an identity theft police report. [California Penal Code Section 530.8]

Similar requirements specifically apply to credit card issuers [California Civil Code Section 1748.95], supervised financial organizations [California Financial Code Section 4002], and finance lenders. [California Financial Code Section 22470]

Federal law also contains provisions on this issue. The FCRA, as amended by the FACT Act, similarly requires a business that has provided credit to or accepted payment from an identity thief to provide a copy of the application and business transaction records to the victim and law enforcement. Before disclosing the records, the business may first require the victim to provide a copy of an identity-theft police report and complete an affidavit. The FCRA specifies the identification requirements that a victim must meet unless the business, at its discretion, "has a high degree of confidence that it knows the identity of the victim" making the request. A business may decline to provide the requested information if, in the exercise of good faith, it determines that, among other things, it "does not have a high degree of confidence in knowing the true identity of the individual requesting the information" or the request is based on a factual misrepresentation by the victim. [Fair Credit Reporting Act Section 609(e), 15 U.S.C. 1681g]

Although many FACT Act provisions preempt the states only with respect to the "conduct required by specific provisions" of the act, the preemption standard for this provision is somewhat different: specifically, states are preempted from enacting any requirement or prohibition "with respect to any subject matter regulated" by Section 609(e) relating to information available to victims. [Fair Credit Reporting Act Section 625(b)(1)(G), 15 U.S.C. 1681t]

As previously noted, the extent and practical effect of the FACT Act's preemption provisions are not yet known.

Statute of Limitations – Provides that the statute of limitations for identity theft crimes, which is generally three or four years, commences upon discovery of the theft. [California Penal Code Sections 801, 801.5, 803, and 803.5]

Marketing

Cell Phone Directory: Opt-in Required – Requires that cellular telephone companies and their agents get a subscriber's consent before including the subscriber's telephone number in a directory. Consent may be given in a document that is signed and dated by the subscriber and not attached to any other document, or, as of January 1, 2006, consent may be given on an Internet Web site, and the company receiving the consent must send a confirmation notice to the subscriber's e-mail or postal address. [California Public Utilities Code Section 2891.1]

Credit Card Solicitations – Permits a consumer to request that his or her name be removed from any list that a consumer credit reporting agency furnishes for credit card solicitations. [California Civil Code Section 1785.11.8]

Direct Marketing: Medical Information – Prohibits businesses from directly requesting any medical information from an individual, regardless of whether the information pertains to the individual, and using, sharing, or otherwise disclosing that information for direct marketing purposes without following these steps prior to obtaining the information:

1. Disclosing in a clear and conspicuous manner that the business is obtaining the information to market or advertise products, goods, or services to the individual. If the request is verbal, the business must make the disclosure to the individual in the same conversation during which the request was made.

2. Obtaining the consent of the individual to whom the information pertains (or a person legally authorized to provide consent for that individual) to permit his or her medical information to be used or shared to market or advertise products, goods, or services to the individual. If the request is

in writing, the consent also must be in writing. If the request is verbal, the business must make an audio recording of the disclosure and consent and maintain the recording for two years. [California Civil Code Section 1798.91]

Disclosure of Alumni Names and Addresses – Authorizes, as of January 1, 2006, the governing bodies and alumni associations of the California State University (CSU), University of California (UC), and Hastings College of Law to disclose the names and addresses of alumni to businesses offering various commercial products and services, provided that specified privacy requirements are met. These provisions sunset on January 1, 2011. [California Education Code Sections 89090 and 92630]

Disclosure of Personal Information to Direct Marketers – Requires a business that discloses personal information for marketing purposes to either: (1) disclose to customers, upon request, a list of the categories of personal information (for example, name, address, telephone number, social security number, e-mail address, or occupation) the business has disclosed to third parties for marketing purposes and the names and addresses of those third parties; or (2) provide customers with the opportunity to prevent information sharing for marketing purposes through either an opt-in or opt-out approach. The provision does not apply to financial institutions that are in compliance with California's Financial Information Privacy Act, as specified. [California Civil Code Section 1798.83]

Marketing to Children Under 16 Years of Age – Makes it unlawful to use a child's personal information to directly contact the child or his or her parent to offer a commercial product or service, and to knowingly fail to comply with the parent's request to take steps to limit access to his or her child's information. Furthermore, marketers are required to permit a parent to withdraw consent to use his or her child's personal information in writing; failure to comply within 20 days of a parent's written request is a misdemeanor.

Any person who sells children's products or services through the mail also must maintain a list of all the individuals and their addresses who have requested that the person discontinue sending materials to them or to their children. Violation is a misdemeanor. [California Penal Code Section 637.9]

Satellite and Cable Television Subscribers – Prohibits satellite or cable television providers, without the subscriber's written consent, from recording or monitoring conversations that take place in a subscriber's residence, or providing a third party with a subscriber's individually identifiable information, including television viewing habits, shopping choices, interests, medical information, banking data, or any other personal or private information. [California Penal Code Section 637.5]

Supermarket Club Card Disclosure Act of 1999 – Places various restrictions on supermarket club cards. For example, club card issuers may not request or require an applicant's driver's license number or social security number, unless the card also can be used as identification to cash checks or to withdraw money from the cardholder's checking or savings account. [California Civil Code Section 1749.64]

Club card issuers also are prohibited from selling or sharing a cardholder's name, address, telephone number, or other personal identification information. [California Civil Code Section 1749.65(a)]

However, a club card issuer may share marketing information, including names and addresses, if it: (1) charges a fee for a club card that must be renewed annually; (2) permits only cardholders to make purchases in the supermarket; (3) alerts cardholders in the text of the application and in the annual renewal materials that their marketing information will be shared with outside companies, and the cardholder has agreed to allow the issuer to share this information; and (4) obtains a confidentiality agreement with the outside company stating that it agrees not to sell or share the cardholder's information. [California Civil Code Section 1749.65(c)]

Telecommunications: Residential Subscriber Information – Prohibits telephone companies from disclosing, without the residential subscriber's written consent, the subscriber's personal calling patterns, credit or other personal financial information, services purchased, or demographic information, and contains specified exceptions. [California Public Utilities Code Section 2891]

Telemarketing: "Do Not Call" Registry – Provides for a nationwide "Do Not Call" Registry in which consumers may include their personal home and cellular telephone numbers to reduce

unwanted telemarketing sales calls. Exceptions to the rule include calls from companies with whom a consumer has an existing business relationship, and calls from or on behalf of political organizations, charities, and telephone surveyors. [Telemarketing Sales Rule, 16 C.F.R. Part 310]

After federal implementation of the nationwide registry, California repealed its "Do Not Call" Registry, which required the attorney general to maintain a list of telephone numbers of consumers who did not wish to receive unsolicited telemarketing calls. Instead, California law now is coordinated with the federal registry; the federal list is now the "master list," and California does not have to bear the cost of a separate registry. However, California law prohibits certain activities related to the "Do Not Call" Registry, including a ban on denying or interfering with a subscriber's right to place a California telephone number on the list for free. [California Business and Professions Code Section 17590 et seq.]

Telephone Consumer Protection Act of 1991 – Places restrictions, under federal law, on the use of automated telephone equipment and prerecorded messages. [Telephone Consumer Protection Act of 1991, 47 U.S.C. 227]

Unsolicited Commercial E-mail Messages: Federal Law – Regulates, under federal law, e-mail messages with the primary purpose of advertising or promoting a commercial product or service under the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act). [15 U.S.C. 7701]

The CAN-SPAM Act bans false or misleading header information and deceptive subject lines. Those who send commercial e-mail messages must include a return e-mail address or another Internet-based response method that a recipient can use to inform the sender to stop sending e-mail messages. Senders must comply with those requests. Commercial e-mail must be clearly and conspicuously identified as an advertisement or solicitation, and include a clear and conspicuous notice that the recipient can opt out of receiving future commercial e-mail from the sender. The act also contains other prohibitions, including a ban on e-mail address "harvesting" (a process in which addresses are obtained by using an automated system that generates possible e-mail addresses by

combining names, letters, or numbers into different permutations). [15 U.S.C. 7704]

CAN-SPAM preempts state laws that regulate the use of e-mail to send commercial messages, except to the extent that the state law "prohibits falsity or deception in any portion" of a commercial e-mail message or attachment. Other state laws that relate to acts of fraud or computer crime also are not preempted. [15 U.S.C. 7707]

Unsolicited Commercial E-mail Messages: State Law – Prohibits any person or entity from sending unsolicited commercial e-mail advertisements from California or to a California e-mail address. [California Business and Professions Code Section 17529.2]

It also is unlawful for a person or entity to advertise in a commercial e-mail advertisement either sent from California or sent to a California e-mail address in any of the following circumstances:

1. The e-mail advertisement contains or is accompanied by a third-party's domain name without the permission of the third party;

2. The e-mail advertisement contains or is accompanied by falsified, misrepresented, or forged header information; or

3. The e-mail advertisement has a subject line that would likely mislead a recipient, acting reasonably under the circumstances, about the message's contents or subject matter. [California Business and Professions Code Section 17529.5]

The statute provides remedies for a violation of this code section and, as of January 1, 2006, a violation is a misdemeanor. Also prohibited is collecting e-mail addresses posted on the Internet, and using an e-mail address obtained from an automated system that randomly combines names, letters, and numbers if the purpose is to initiate or advertise in an unsolicited commercial e-mail advertisement sent from California or to a California e-mail address. [California Business and Professions Code Section 17529.4]

It also is unlawful for registered users of e-mail service providers to use the provider's equipment in violation of the provider's policy prohibiting or restricting the sending of unsolicited e-mail advertisements. [California Business and Professions Code Section 17538.45]

Unsolicited Text Messages – Prohibits a person or business from transmitting unsolicited text-message advertisements to a cellular telephone or pager, except as specified. As of January 1, 2006, this prohibition also applies to candidates or political committees and text messages sent to two-way messaging devices. [California Business and Professions Code Section 17538.41]

Medical Privacy

Confidentiality of Medical Information Act (CMIA) – Prohibits a health-care provider, health-care service plan, or contractor from disclosing medical information regarding a patient, enrollee, or subscriber of a health-care service plan without first obtaining authorization, except as specified. [California Civil Code Section 56.10(a)]

Notwithstanding the above, medical information must be disclosed if required by a court order or search warrant, among other things. In other specified circumstances, disclosure is discretionary. [California Civil Code Section 56.10(b)-(c)]

Violations of CMIA are enforceable by administrative fines or civil penalties, misdemeanor criminal penalties, and a private right of action for compensatory and punitive damages. [California Civil Code Sections 56.35 and 56.36]

Health Insurance Portability and Accountability Act (HIPAA) – Provides, under federal law, for minimum privacy protections for patients' personal medical information [Standards for Privacy of Individually Identifiable Health Information. ("Privacy Rule"), 45 C.F.R. 164.500 et seq.]

The Privacy Rule applies to health plans, health-care clearing-houses, and health-care providers that transmit any health information in electronic form that pertains to a transaction covered by the rule. Under the rule, patients have the right to see and correct their medical records; limits are placed on the use of personal medical information, including the marketing of information; and entities covered under the rule must provide patients with a notice of their privacy practices. While the Privacy Rule preempts contrary state laws, it specifically permits more stringent state laws that relate to the privacy of individually identifiable health information. [45 C.F.R. 160.203]

Patient Access to Medical Records – Gives a patient the right to request, inspect, and copy his or her records maintained by a health-care provider. [California Health and Safety Code Section 123110]

An adult patient has the right to include a written addendum regarding any item or statement in his or her records that he or she believes is incomplete or incorrect. The provider must attach the addendum to the patient's records and include it whenever the provider discloses the allegedly incomplete or incorrect portion to any third party. [California Health and Safety Code Section 123111]

Online Privacy and Related Issues

Anti-Phishing Act of 2005 – Makes it unlawful, as of January 1, 2006, for a person to use a Web page, e-mail message, or any other means via the Internet to solicit, request, or take an action to induce another individual to provide identifying information by falsely representing himself or herself as a legitimate business. The statute also defines key terms and includes various remedies for a violation. [California Business and Professions Code Section 22948 et seq.]

Computer Spyware – Prohibits, among other things, an unauthorized person or entity from causing, as specified, computer software to be copied onto another person's computer if the software modifies the user's computer settings or collects personally identifiable information. [California Business and Professions Code Section 22947.2]

Online Privacy Policy – Requires commercial Web site operators and online services that collect personally identifiable information about California residents to conspicuously post their privacy policy on their Web site or, in the case of an online service, make that policy available to the public. The policy must meet specified requirements, and an operator is in violation if, after being notified of noncompliance, the policy is not posted within 30 days. [California Business and Professions Code Section 22575]

State Agency Collection of Personal Information on the Internet – Requires state agencies, when electronically collecting personal information on the Internet, to state what type of personal information is being collected and how it will be used. State agencies are prohibited from distributing or selling electronically collected personal information about a user to a third party without the user's permission, except as specified. [California Government Code Section 11015.5]

Unauthorized Access to Computers, Computer Systems, and Data – Makes it unlawful to, among other things, knowingly access and, without permission, alter, damage, delete, destroy, or otherwise use any data, computer, computer system, or computer network to: (1) devise or execute a scheme to defraud or extort; or (2) wrongfully control or obtain money, property, or data. [California Penal Code Section 502]

Public Records

Birth and Death Record Indices – Requires the state registrar to maintain three indices containing birth and death records as follows:

1. Comprehensive birth and death indices must be kept confidential, with access limited to other governmental agencies. No government agency may sell or release any portion of the contents to any person or place the information on the Internet.

2. Noncomprehensive birth and death indices that do not contain the mother's maiden name or any social security numbers must be available to the public.

3. Noncomprehensive birth and death indices containing the mother's maiden name and social security numbers, as specified, must be made available to law enforcement or to certain entities (such as financial institutions or consumer credit reporting agencies) to prevent fraud. [California Health and Safety Code Section 102230]

Those who request both noncomprehensive birth and death indices are required to complete a form, signed under penalty of perjury, that includes an agreement not to sell, assign, or otherwise transfer the indices or use them for fraudulent purposes. [California Health and Safety Code Section 102230]

Restrictions also are imposed on the release of birth and death data files. [California Health and Safety Code Section 102231]

Birth and Death Records: Confidential Information – Provides that confidential information included in birth and death (including fetal death) certificates is exempt from the California

Public Records Act. [California Health and Safety Code Section 102100]

California law makes a parent's medical and social information contained in the second section of a birth certificate confidential, and, as of January 1, 2006, applies this confidentiality to the second section of a fetal death certificate, which contains similar information. In both cases, access is limited to specified persons, and the second section of the certificate must be labeled "Confidential Information for Public Health Use Only." [California Health and Safety Code Section 102430]

Birth and Death Records: Release – Controls the release of and access to birth and death records. Among other things, the statute provides that the state registrar, local registrar, or county recorder may only give a certified copy of a birth or death record to an authorized person. That person must submit a statement sworn under penalty of perjury that he or she is authorized to receive a copy. Authorized persons include the registrant, law enforcement, a specified relative of the registrant, or a funeral establishment employee. In cases in which the requester is not an authorized person, a certified copy may be provided but the document may only be an informational certified copy that states "INFORMATIONAL, NOT A VALID DOCUMENT TO ESTABLISH IDENTITY." [California Health and Safety Code Section 103526]

Court Records: Personal Information of Victims and Witnesses – Protects confidential personal information relating to a witness or victim contained in a police report or search warrant. [California Penal Code Section 964]

Court Records: Sealing Information Regarding Financial Assets and Liabilities – Permits a party to a dissolution of marriage, an annulment, or a legal separation to request the court to seal from public view information concerning the party's financial assets and liabilities. [California Family Code Section 2024.6]

Department of Motor Vehicles' Records – Provides that a residential address in any of the department's records is confidential and may not be disclosed except to a court, law enforcement agency, or other government agency, or, under certain circumstances, to a financial institution, insurance company, or attorney. [California Vehicle Code Section 1808.21]

Another provision, enacted prior to the section cited above, makes the home addresses of certain individuals confidential, including the attorney general, members of the Legislature, judges, district attorneys, and public defenders. If these persons request the confidentiality of their home addresses, they may not be disclosed except to a court, law enforcement agency, an attorney pursuant to a subpoena, or others as specified. [California Vehicle Code Section 1808.4]

Also, the home addresses of the chairperson, executive officer, commissioners, and deputy commissioners of the Board of Prison Terms (now called the Board of Parole Hearings) are kept confidential upon request. [California Vehicle Code Section 1808.6]

Except for home addresses and other information required to be kept confidential, the Department of Motor Vehicles may permit entities access to its electronic database to obtain information for commercial use. [California Vehicle Code Section 1810.7]

The distribution or sale of a driver's license photograph is prohibited. [California Vehicle Code Section 12800.5]

Driver's License Information: Swiping – Permits businesses to "swipe" (or slide) a driver's license through an electronic device only for specified purposes, such as verification of the person's age or authenticity of the card, or to collect or disclose personal information required for reporting, investigating, or preventing fraud, abuse, or material misrepresentation. Businesses may not retain or use information obtained for any purpose that is not specified, and violation of these provisions is a misdemeanor. [California Civil Code Section 1798.90.1]

Driver's Privacy Protection Act of 1994 – Prohibits, under federal law, a state's Department of Motor Vehicles and its employees from knowingly disclosing a driver's personal information to any person or entity except for certain uses, including: (1) a government agency carrying out its functions; (2) a business verifying the accuracy of personal information submitted by the individual to the business; or (3) a licensed private investigative agency using it for various permissible purposes. [Driver's Privacy Protection Act of 1994, 18 U.S.C. 2721 et seq.]

Information Practices Act of 1977 – Imposes limitations on the collection and disclosure of personal information by state agencies. [California Civil Code Section 1798 et seq.]

The Information Practices Act requires, among other things, that state agencies maintain in their records only personal information that is relevant and necessary to accomplish an authorized purpose. [California Civil Code Section 1798.14]

In addition, state agencies must permit individuals to inspect and, if necessary, correct records maintained by the agency. [California Civil Code Sections 1798.34 and 1798.35]

An agency may not disclose any personal information in a manner that would link the information to the individual to whom it pertains unless, among other things, the disclosure is: (1) with the prior written consent of the individual, as specified; (2) to a governmental entity when required by state or federal law; (3) pursuant to the California Public Records Act (see the summary below); (4) pursuant to a search warrant; or (5) to a committee or a member of the Legislature, if the member has permission from the individual or the member provides reasonable assurance that he or she is acting on behalf of the individual. [California Civil Code Section 1798.24]

Public Records Act – Provides that public records are open to inspection, unless exempt. [California Government Code Section 6250 et seq.]

The Public Records Act may not be construed to require disclosure of various records, including: (1) personnel, medical, or similar files if the disclosure would constitute an unwarranted invasion of personal privacy; and (2) records pertaining to pending litigation that the state agency is a party to, until the pending litigation or claim has been adjudicated or otherwise settled. [California Government Code Section 6254]

The California Constitution, as amended by Proposition 59 in November 2004, grants Californians the right of public access to meetings of government bodies and writings of government officials. Statutes furthering public access must be interpreted broadly, and, if they limit access, they must be interpreted narrowly. Also, future statutes that limit access must contain

findings that justify the need for the limitations. Proposition 59 preserves constitutional rights, such as the right to privacy, due process, and equal protection. Existing constitutional and statutory limitations restricting access to certain meetings and records of government bodies and officials, including law enforcement and prosecution records, also are preserved. [California Constitution, Article 1, Section 3]

State Agencies' Privacy Policies – Requires each state agency to enact and maintain a permanent privacy policy based on certain principles, including that the agency specify, at or prior to the time of collection, the purposes for which personally identifiable information is collected. And any subsequent use of the information may not be inconsistent with these identified purposes. [California Government Code Section 11019.9]

State Agency Databases: Researcher Access – Permits state agencies, as of January 1, 2006, to release personal information to the University of California or a nonprofit educational institution conducting scientific research only if the research proposal has been reviewed and approved by the Health and Human Services Agency's Committee for the Protection of Human Subjects. The committee is required to apply specified data protection standards to its review of research proposals. [California Civil Code Section 1798.24(t)]

Voter Information – Requires, as of January 1, 2006, specified information regarding the permissible use of voter information to be posted on the Web sites of every local elections official and the secretary of state, as well as in the state ballot pamphlet. [California Elections Code Section 2157.2]

Also as of January 1, 2006, the signature of a voter shown on a voter registration card is confidential and may not be disclosed to any person unless a person's vote is challenged. [California Elections Code Section 2194]

Voter Information: Outsourcing – Prohibits a requester of voter information, voter signatures, or other information collected for an initiative, a referendum, or a recall petition from sending the information outside of the United States, as of January 1, 2006, as specified. [California Elections Code Section 2188.5]

Social Security Numbers

Confidentiality – Places restrictions on the use of social security numbers, and prohibits: (1) public posting or displaying an individual's social security number; (2) printing an individual's social security number on a card that he or she must use to access products or services; (3) requiring 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) requiring an individual to use his or her social security number to access an Internet Web site unless a password also is required to access the site; and (5) printing an individual's social security number on any materials mailed to him or her unless required by state or federal law. The statute contains delayed implementation dates for various entities. [California Civil Code Section 1798.85]

Drivers' Licenses – Requires that a driver's license applicant include his or her social security number (or other appropriate number) on the application, however, the social security number may not be included on a magnetic tape or strip used to store data on the license. [California Vehicle Code Section 12801]

Employee Compensation – Requires all employers by January 1, 2008, to use only the last four digits of an employee's social security number when providing employees with an itemized statement of earnings. [California Labor Code Section 226]

Family Court Records – Permits a party to the dissolution of a marriage, an annulment, or a legal separation to redact a social security number from any pleading, attachment, document, or other written material filed with the court. However, social security numbers may not be redacted from certain documents, including forms relating to child or spousal-support collection. [California Family Code Section 2024.5]

Powers of Attorney – Deletes, as of January 2, 2006, the line on the statutory power-of-attorney form that requires a social security

number, and adds a notice on the form stating that a third party may require additional identification. [California Probate Code Section 4401]

Use in Credit Reports – Requires, under federal law, a consumer reporting agency to truncate a consumer's social security number when the consumer requests a copy of his or her credit report and asks that the first five digits of his or her social security number not be included in the report. [Fair Credit Reporting Act Section 609(a)(1)(A), 15 U.S.C. 1681g]

Other Key Statutes

Eavesdropping on Confidential Communications – Makes it unlawful to intentionally eavesdrop on a confidential communication, by means of an electronic amplifying or recording device, without the consent of all parties. This prohibition applies whether the communication occurs in person or by telegraph, telephone, or other device. [California Penal Code Section 632]

Electronic Communications Privacy Act of 1986 – Prohibits, under federal law, an individual from intentionally intercepting any wire, oral, or electronic communication. Various oral communications are exempt from this prohibition. There also are several exceptions to the prohibition, including intercepts obtained in the ordinary course of business, or if one of the parties to the communication consents. [Electronic Communications Privacy Act of 1986, 18 U.S.C. 2511]

Electronic Surveillance Technology: Rental Cars – Prohibits a rental car company from using or accessing any information relating to the renter's use of the rental vehicle that was obtained using electronic surveillance technology, such as a Global Positioning System (GPS), wireless technology, or a location-based technology. Certain exceptions apply, such as if the rental car is stolen, law enforcement requests the information pursuant to a subpoena or search warrant, or the renter requests that the vehicle be remotely locked or unlocked. A rental company may not use electronic surveillance technology to track a renter in order to impose fines or surcharges relating to the renter's use of the vehicle. [California Civil Code Sections 1936(o) and (p)]

Electronic Tracking Devices on Vehicles – Makes it unlawful to use an electronic tracking device attached to a vehicle to determine the location or movement of a person, except in specified instances, such as when the vehicle's registered owner has

consented to the use or when law enforcement lawfully uses the device. [California Penal Code Section 637.7]

Office of Privacy Protection – Creates the Office of Privacy Protection in the Department of Consumer Affairs. The office's purpose is to protect 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. The office is required to inform consumers about methods for protecting the privacy of their personal information and make recommendations to organizations for privacy policies and practices that promote and protect the interests of California consumers. The office also may promote voluntary and mutually agreed upon nonbinding arbitration and mediation of privacy-related disputes. [California Business and Professions Code Section 350]

Taxpayer Information – Makes it unlawful for a person to disclose information obtained in the preparation of federal or state income tax returns unless the disclosure is within specified exceptions, including: (1) the taxpayer has consented in writing to the disclosure; (2) the disclosure is expressly authorized by state or federal law; or (3) the disclosure is pursuant to a court order. [California Business and Professions Code Section 17530.5]

Unfair Competition Law – Prohibits unfair competition, which includes: (1) an unlawful, unfair, or fraudulent business act or practice; (2) unfair, deceptive, untrue, or misleading advertising; and (3) an act prohibited by the false advertising statutes. The law provides that actions for relief may be brought by the attorney general; a district attorney; a city attorney or city prosecutor only under specified circumstances; or by any person who has suffered injury in fact and has lost money or property as a result of the unfair competition. Civil penalties for unfair competition violations are not available to consumers. [California Business and Professions Code Section 17200 et seq.]

In many cases, consumer privacy statutes do not contain their own separate cause of action, and the unfair competition law has therefore been used as a means for consumers to obtain relief.

Vehicle Event Data Recorders – Requires a manufacturer of a new motor vehicle sold or leased in California that is equipped with a recording device (commonly referred to as an "event data recorder" or a "sensing and diagnostic module") to disclose that feature in the owner's manual. Data obtained from the recording device may not be downloaded or otherwise retrieved by a person other than the vehicle's registered owner, except under specified circumstances, such as if the registered owner consents or in response to a court order. [California Vehicle Code Section 9951]

Video Privacy Protection Act of 1998 – Provides, under federal law, that any business engaged in the sale or rental of video tapes may disclose a consumer's personally identifiable information only in certain instances, such as to law enforcement pursuant to a warrant, or to any other person if the business has the consumer's informed, written consent. A business also may disclose consumers' names and addresses if: (1) it has provided consumers with the opportunity, in a clear and conspicuous manner, to prohibit the disclosure; and (2) the disclosure does not identify the title, description, or subject matter of the video tapes, although the subject matter may be disclosed if the disclosure is for the exclusive use of marketing goods and services directly to the consumer. Federal law preempts only those state or local laws that require a disclosure prohibited under federal law. [Video Privacy Protection Act of 1998, 18 U.S.C. 2710]

Video Sale or Rental – Prohibits, under state law, any person who provides video-cassette sales or rental services from disclosing personal information, including sales or rental information, to a person without the written consent of the individual to whom the information pertains, except in specified instances. [California Civil Code Section 1799.3]