Consumer Privacy and IDENTITY Theft

A Summary of Key Statutes and Guide for Lawmakers

California Senate Office of Research

2008 Edition

Consumer Privacy and IDENTITY Theft

A Summary of Key Statutes and Guide for Lawmakers

Saskia Kim

California Senate Office of Research

Agnes Lee, Director ■ 3rd Edition ■ January 1, 2008

Contents

Introduction 7

The Constitution and General Privacy

- Overview 11
- Constitutional Right to Privacy 12
- Constructive Invasion of Privacy 14
- Invasion of Privacy: Common Law Tort 14
- Invasion of Privacy: Penal Code 15
- Preemption 16

Credit Cards

- Overview 21
- Activation Process Required for Substitute Credit Cards 21
- Change of Address and Credit Card Requests 22
- Credit Card or Debit Card Numbers Printed on Receipts 24
- Disclosure of Minimum Payment Amount 25
- Fraudulent Use of Information ("Skimming") 26
- Preprinted Checks: Disclosures 26
- Recording Credit Card Numbers on Checks 27
- Recording Personal Information on Credit Card Transaction Forms 27
- Verification of Credit Applicant's Address 27

Credit Reporting

- Overview 33
- Credit Reporting 34
- Investigative Consumer Reporting Agencies 37
- Security Alerts 38
- Security Freezes 40

Data Security
Overview 43
Destruction of Business and Medical Records 44
Notification of Breach in Data Security 46
Personal Information: Reasonable Security Procedures 47

Financial Privacy and Related Issues
Overview 51
Account Numbers 52
Debt Collection 52
Financial Privacy 53
Insurance Information and Privacy Protection Act 55
Insurers: Genetic Testing 56

Identity Theft
Overview 59
Crime of Identity Theft 60
Debt Collection Activities 61
Deceptive Identification Documents 61
Department of Justice Identity Theft Victim Database 62
Falsely Obtaining Department of Motor Vehicles' Documents 62
Identity Theft Victim's Right to Free Credit Reports 63
Issuance of a Search Warrant 64
Judicial Determination of Innocence 64
Jurisdiction for Prosecuting Identity Theft Crime 64
Law Enforcement Investigation Required 65
Right to Bring Legal Action Against a Creditor 65
Right to Obtain Records of Fraudulent Transactions or Accounts 66
Statute of Limitations 67
Youth in Foster Care: Request for Credit Report 68

Marketing
Overview 71
Affiliate Marketing 72

Cell Phone Directory: Opt in Required 73
Credit Card Solicitations 73
Direct Marketing: Medical Information 73
Disclosure of Alumni Names and Addresses 74
Disclosure of Personal Information to Direct Marketers 75
Marketing to Children Under 16 Years of Age 75
On-Campus Marketing: Credit Cards 76
Satellite and Cable Television Subscribers 76
Supermarket Club Card Disclosure Act of 1999 77
Telecommunications: Residential Subscriber Information 77
Telemarketing: "Do Not Call" Registry 78
Telephone Consumer Protection Act of 1991 79
Unsolicited Commercial E-mail Messages (Spam) 79
Unsolicited Text Messages 81

Medical Privacy

Overview 85
Medical Privacy 86
Office of HIPAA Implementation 92
Patient Access to Medical Records 92
Retention of Patient Records 93

Online Privacy and Related Issues

Overview 97
Anti-Phishing Act of 2005 98
Children's Online Privacy Protection Act 98
Computer Spyware 99
Online Privacy Policy 99
Posting Personal Information on the Internet 100
State Agency Collection of Personal Information on the Internet 101
Unauthorized Access to Computers, Computer Systems, and Data 101

U.S. SAFE WEB Act 102
Wireless Network Security 102

Public Records

Overview 105
Birth and Death Record Indices 106
Birth and Death Records: Confidential Information 107
Birth and Death Records: Release of Records 107
Court Records: Personal Information of Victims and Witnesses 108
Court Records: Sealing Information Regarding Financial Assets and Liabilities 108
Department of Motor Vehicles' Records 109
Driver's License Information: "Swiping" Licenses 110
Driver's Privacy Protection Act of 1994 110
Information Practices Act of 1977 111
Marriage License Information 112
Privacy Act of 1974 112
Public Records: Address Confidentiality 112
Public Records Act 113
State Agencies: Mailing Personal Information 114
State Agencies' Privacy Policies 114
State Agency Databases: Researcher Access 115
Voter Information 115
Voter Information: Outsourcing 117

Social Security Numbers

Overview 121
Confidentiality 122
County Recorders' Records 123
Court Records 124
Drivers' Licenses 124
Employee Compensation 125

Family Court Records 125
Franchise Tax Board Liens 125
Local Agencies' Records 126
Powers of Attorney 126
Secretary of State Filings 126
Use by Colleges and Universities 128
Use in Credit Reports 128

Other Key Statutes

Overview 131
Criminal Investigation Information 132
Eavesdropping on Confidential Communications 132
Electronic Communications Privacy Act of 1986 133
Electronic Surveillance Technology: Rental Cars 133
Electronic Tracking Devices on Vehicles 134
Identification Devices: Forced Human Implants 134
Office of Information Security and Privacy Protection 134
Personal Information: Domestic Violence, Sexual Assault, and Stalking 135
Personal Information: Inmate Access 136
Pretexting 137
Real ID Act of 2005 138
Student Records 141
Taxpayer Information 142
Unfair Competition Law 142
Vehicle Event Data Recorders 143
Video Image Evidence: Parking Enforcement 143
Video Sale or Rental 144

Index 147

Introduction

For the seventh year in a row, identity theft tops the Federal Trade Commission's list of top 10 consumer complaints. The most common form of reported identity theft is credit card fraud, followed by phone or utilities fraud, bank fraud, and employment fraud. And among the 50 states, California ranks third in identity theft victims per capita, after Arizona and Nevada.

Social security numbers are the most frequently used recordkeeping numbers in the nation, and because they can be used to assume another person's identity, they are one of the three most sought after pieces of information (in addition to names and birth dates) by identity thieves.

Both the U.S. Supreme Court and California Supreme Court issued rulings in 2007 that affect consumers (and even state employees in particular, see "Public Records Act" on page 113) and their privacy rights. Federal agencies also issued final rules last year that implement consumer protection statutes.

In California, lawmakers approved measures that, to highlight just a few, restrict how social security numbers are displayed in many public records; prohibit the forced human implantation of identification devices that can transmit personal information; and extend the state's first-in-the-nation breach-notification law, which now requires that a consumer must be notified if his or her medical information has been breached.

These and numerous other state and federal laws are featured in this year's edition of *Consumer Privacy and Identity Theft*. (Readers are encouraged to consult the statutory texts for more detail, and please note that all citations to the Fair Credit Reporting Act include amendments to the act contained in the Fair and Accurate Credit Transactions Act of 2003 [FACTA].)

Consumers will begin to feel the impact of these new state and federal laws this year, as many went into effect on January 1, 2008.

The Constitution and General Privacy

Overview

- California is one of only ten states whose state constitutions expressly recognize a right to privacy.[1] The U.S. Constitution, however, does not contain an explicit right to privacy; the U.S. Supreme Court has instead held that the federal constitution implicitly recognizes an individual's right to privacy with respect to certain rights. For example, the First Amendment safeguards an individual's freedom of expression and association, and the Fourth Amendment protects an individual against unreasonable search and seizure. Yet these rights only protect against intrusive governmental activities. California's constitution, on the other hand, has been interpreted by the courts to protect against both governmental and private entities.

- In addition to constitutional protections, California has enacted statutory provisions safeguarding the general privacy of individuals. For instance, California law provides for civil liability for the constructive invasion of privacy and imposes criminal penalties for certain kinds of privacy invasions, such as unauthorized wiretapping and electronic eavesdropping. California courts have also recognized the tort of invasion of privacy that allows an injured party to bring a lawsuit seeking redress. The California Supreme Court recently considered this issue in a case in which an academic researcher was alleged to have misrepresented her position to obtain sensitive personal information.

- The ability of states to act to protect privacy is also critical. Preserving the states' long-standing ability to enact laws relating to consumer privacy and identity theft has become a significant issue as Congress

[1] National Conference of State Legislatures, "Privacy Protections in State Constitutions," http://www.ncsl.org/programs/lis/privacy/stateconstpriv03.htm.

has increasingly included preemption provisions in proposed federal legislation. Furthermore, federal regulatory agencies—such as the Office of the Comptroller of the Currency and the Office of Thrift Supervision—have taken a broadly preemptive view of the powers of federally chartered financial institutions that has implicated some privacy-related issues. And both state and federal courts have invalidated some state laws on the basis that federal law preempts state action in various instances.

- To provide a better understanding of the framework in which state law operates, this report outlines how specified federal laws impact state statutes, although it is important to note that whether a state law is preempted by federal law is ultimately an issue decided by the courts.[2] In some cases, courts have invalidated California law on the basis of preemption; these instances are noted in this report. In other cases, although federal law may contain provisions that arguably preempt California law, the courts have yet to rule on the matter. As a result, the extent and practical effect of the particular preemption provision is not yet known.

Constitutional Right to Privacy

California Law

State law specifies in the California Constitution that all people have an inalienable right to pursue and obtain privacy. [California Constitution, Article I, Section 1.] The right of privacy was added to the constitution by initiative (Proposition 11) in November 1972.

[2] Related to this point, the California Constitution prohibits state administrative agencies from declaring a statute unenforceable or refusing to enforce a statute on the basis that it is preempted by federal law or federal regulations unless an appellate court makes a determination that the statute is preempted by federal law or regulations. [California Constitution, Article I, Section 3.5.]

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, e.g., *American Academy of Pediatrics v. Lungren* (1997) 16 Cal. 4th 307, 326, citing *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, a plaintiff must establish the following three elements: (1) a legally protected privacy interest, (2) a reasonable expectation of privacy in the circumstances, and (3) conduct by the defendant that constitutes a serious invasion of privacy. [*Hill*, 7 Cal. 4th at 39-40; *Pioneer Electronics (USA), Inc. v. Superior Court* (2007) 40 Cal. 4th 360.]

If a plaintiff establishes these three elements, the defendant may prove that the invasion of privacy is justified because it "furthers legitimate and important competing interests." [*Hill*, 7 Cal. 4th at 38.] In *Hill*, the California Supreme Court explained this balancing test: "Invasion of a privacy interest is not a violation of the state constitutional right to privacy if the invasion is justified by a competing interest." [Id.]

Federal Law

Federal law does not contain an express right to privacy in the U.S. Constitution. Instead, the U.S. Supreme Court has recognized an individual's right to privacy implicit in the constitution with respect to certain rights. For example, the Court has recognized First Amendment safeguards for freedom of expression and association and Fourth Amendment protections against unreasonable search and seizure. [See, e.g., *Griswold v. Connecticut* (1965) 381 U.S. 479; *Katz v. United States* (1967) 389 U.S. 347.] The Court has also recognized a limited constitutional right to informational privacy. [*Whalen*

v. Roe (1977) 429 U.S. 589.] In these cases, individuals are protected against intrusive governmental activities.

Constructive Invasion of Privacy

California Law

State law 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 and could not have been obtained without a trespass unless the device was used. [California Civil Code Section 1708.8(b).]

Invasion of Privacy: Common Law Tort

California Law

State law 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 overview, four types of activities are considered an invasion 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. [William L. Prosser, *Privacy*, 48 Cal. L. Rev. 383, 389 (1960). See

also, Restatement (Second) of Torts, Sections 652A-652E and 5 Witkin, Summary of Cal. Law Torts (10th ed.) Torts, Section 651.]

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 [or she] 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.]

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

In February 2007 the California Supreme Court considered an invasion of privacy case in which an academic researcher was alleged to have misrepresented her position to obtain sensitive personal information. In this case, the court held that the researcher could be held liable in an invasion-of-privacy lawsuit for improperly intruding into private matters but dismissed the plaintiff's other privacy-related claims. [*Taus v. Loftus* (2007) 40 Cal. 4th 683.]

Invasion of Privacy: Penal Code

California Law

State law prohibits the invasion of privacy with the intent to protect Californians' right to privacy. [California Penal Code Section 630 et seq.] Among other things, these statutes contain criminal penalties for unauthorized wiretapping, electronic eavesdropping, intercepting cellular telephone communications, and electronic tracking of individuals, except as specified.

Preemption

Federal Law

The doctrine of federal preemption provides that congressional action pursuant to an enumerated, or specific, power may override state laws. There are three tests the courts refer to when deciding whether federal regulation preempts state law: (1) express preemption, in which Congress, through explicit statutory language, restricts the ability of states and localities to legislate in specific areas, (2) field 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 or where state law stands as an obstacle to the congressional purpose of the federal law. [*Gade v. National Solid Waste Management Association* (1992) 505 U.S. 88, 98.]

Even where preemption is found, the court must still determine the precise extent of the preemption. There has been heightened interest in the issue of preemption in general, as Congress has increasingly included preemption provisions in proposed federal legislation, and federal regulatory agencies have also increasingly taken a broad view of the powers of federally chartered financial institutions.

For example, the Fair Credit Reporting Act (FCRA) preempts state action in certain matters. On this point it is important to note that the preemption language included in FCRA, as amended by the Fair and Accurate Credit Transactions Act of 2003 (FACTA), varies depending on the specific FCRA provision, as FACTA introduced a different, and arguably narrower, form of preemption. Some preemption provisions, for instance, arguably appear quite narrow, only precluding states from enacting requirements "with respect to the conduct required" by specific provisions of 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.] While the "conduct required" preemption standard appears to be narrower than the "subject matter regulated" standard, it is important to note that the scope of these preemption provisions has not yet been tested in court.

Increasingly, some federal regulatory agencies have also taken a broad view of the powers of the federally chartered entities they regulate, which has implicated some privacy-related issues.[3] For example, the Office of the Comptroller of the Currency, which regulates national banks under the National Bank Act (12 U.S.C. 21 et seq.), issued a final rule in 2004 identifying the types of state laws that are preempted with respect to federally chartered banks and their operating subsidiaries.[4] The rule provides that, except where made applicable by federal law, state laws that obstruct, impair, or condition a national bank's ability to fully exercise its lending or deposit-taking powers are preempted. Under the rule, a state law does not apply to a national bank if the law obstructs, impairs, or conditions the bank's ability to fully exercise its powers to conduct federally authorized activities. [12 C.F.R. Parts 7 and 34.]

The final rule issued by the Office of the Comptroller of the Currency also identifies those state laws that are not preempted with respect to a national bank's deposit-taking, lending, or other powers granted to it by federal law. These include state laws regarding contracts, rights to collect debt, torts, and property transfers to the extent that they only incidentally affect the exercise of a national bank's power in the area. The Office of the Comptroller of the Currency retains the ability to determine whether a particular state law is preempted (and therefore does not apply to a national bank or its operating subsidiaries) on a case-by-case basis. [12 C.F.R. Parts 7 and 34.]

---

[3] Federal regulations within the power of the issuing agency may preempt state law; the U.S. Supreme Court has stated that federal regulations "have no less pre-emptive effect than federal statutes." [*Fid. Fed. Sav. & Loan Ass'n v. de la Cuesta* (1982) 458 U.S. 141, 153.] The Court also noted: "Pre-emption may result not only from action taken by Congress itself; a federal agency acting within the scope of its congressionally delegated authority may pre-empt state regulation." [*La. Public Serv. Com v. FCC* (1986) 476 U.S. 355, 369.]

[4] In April 2007 the U.S. Supreme Court held that state laws do not apply to a national bank's mortgage lending activities, whether those activities are conducted by the bank itself or the bank's operating subsidiary. [*Watters v. Wachovia Bank, N.A.* (2007) 127 S. Ct. 1559, 1564.] Instead, national banks and their operating subsidiaries—such as mortgage companies that operate as subsidiaries of national banks—are subject to exclusive regulation by the Office of the Comptroller of the Currency and not to the "licensing, reporting, and visitorial" regime of the state in which the subsidiary operates. [Id. at 1564-1565.] The Court noted that certain state laws that do not conflict with the purpose of the National Bank Act are applicable to national banks. These include state laws regarding usury, contracts made by national banks, and acquisition and transfer of property by national banks. [Id. at 1567.]

The Office of Thrift Supervision, which regulates federal savings associations under the Home Owners' Loan Act of 1933 (12 U.S.C. 1461 et seq.), has also promulgated regulations that preempt state law "purporting to address the subject of the operations of a Federal savings association." [12 C.F.R. Part 545.2.] Regulations issued by the Office of Thrift Supervision further state that the office "occupies the entire field of lending regulation for federal savings associations." [12 C.F.R. Part 560.2.]

The regulations issued by the Office of the Comptroller of the Currency and the Office of Thrift Supervision have both been interpreted to preempt California Civil Code Section 1748.13, which requires credit card issuers to include a warning statement and other specified information regarding minimum payments in billing statements provided to cardholders. [*American Bankers Association v. Lockyer* (2002) 239 F. Supp. 2d 1000.]

None of the above-described regulations are directed specifically to a state's ability to enact laws protecting consumer privacy or addressing identity theft issues, nor do the regulations appear grounded in hostility toward the states' interest in these areas. Instead, they deal more generally with the powers of a federally chartered institution. The regulations may, however, have a preemptive effect if state laws regarding consumer privacy or identity theft are found to interfere improperly with the operations of the federally chartered institutions regulated by these agencies.

Other federal agencies also take an active role in consumer privacy and identity theft protections. For example, the Federal Trade Commission (FTC) is charged with preventing unfair methods of competition and unfair or deceptive acts or practices in interstate commerce. [15 U.S.C. 45 et seq.] Several other statutes also form the basis for the FTC's authority in protecting consumers, including the Gramm–Leach–Bliley Act (15 U.S.C. 6801 et seq.), Fair Credit Reporting Act (15 U.S.C. 1681 et seq.), and Children's Online Privacy Protection Act (15 U.S.C. 6501 et seq.).

Credit Cards

Overview

- Both state and federal law regulate credit cards. In 2003, for example, Congress passed the Fair and Accurate Credit Transactions Act (FACTA), which amended the Fair Credit Reporting Act (FCRA). FACTA contains provisions relating to requirements that a credit card issuer must meet when responding to a request for a change of address. And federal agencies recently issued a final rule implementing these requirements. California law also contains similar provisions.

- While both FACTA and FCRA contain provisions preempting state action, the specific preemption language varies and, in several cases, federal regulations are necessary before federal law may be fully implemented. Furthermore, whether or not these provisions preempt state law has yet to be tested in court. As a result, the exact reach of FACTA and FCRA preemption is not yet known.

Activation Process Required for Substitute Credit Cards

California Law

Under state law, a credit card issuer may not issue a substitute credit card unless the cardholder is required to contact the issuer to activate the credit card before using it. [California Civil Code Section 1747.05.]

Change of Address and Credit Card Requests

California Law

State law 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. This notice must be sent within 30 days in other specified instances. [California Civil Code Section 1799.1b(a).]

The notice may be given by telephone or e-mail communication if the credit card issuer reasonably believes it has the current telephone number or e-mail address of the cardholder who requested the address change. If the notification is provided in writing, however, it may not include the cardholder's account number, social security number, or other personal identifying information although it may contain the cardholder's name, previous address, and new address of record. [California Civil Code Section 1799.1b(c).]

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

The federal Fair Credit Reporting Act (FCRA), as amended by the Fair and Accurate Credit Transactions Act of 2003 (FACTA), required the Federal Trade Commission, National Credit Union Administration, and specified financial-institution agencies to issue regulations on this matter. [Fair Credit Reporting Act Section 615(e), 15 U.S.C. 1681m.] In July 2006 the agencies issued

proposed regulations and a final rule was issued in October 2007.[5] The final rule is effective January 1, 2008, and covered financial institutions and other entities must be in compliance by November 1, 2008.

The final rule includes "Red Flag" regulations, which are intended to identify patterns, practices, and specific forms of activity that indicate the possible existence of identity theft.

The final rule requires specified financial institutions and creditors to implement a written Identity Theft Prevention Program, which must contain policies and procedures to detect, prevent, and mitigate identity theft related to the opening of an account or any existing account. These policies and procedures must: (1) identify relevant Red Flags and incorporate them into the program, (2) detect Red Flags that have been incorporated into the program, (3) respond appropriately to any Red Flags that are detected to prevent and mitigate identity theft, and (4) ensure the program is updated periodically to reflect changes in identity theft risks.

Under the final rule, if a credit card or debit 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 until the issuer notifies the cardholder or has otherwise assessed the validity of the change of address in accordance with the policies and procedures established under its Identity Theft Prevention Program.

Any written or electronic notification given by the card issuer pursuant to these requirements must be clear and conspicuous and provided separately from other regular correspondence with the cardholder. And a card issuer must provide a cardholder with a "reasonable" means for promptly reporting incorrect address changes when the issuer notifies the cardholder of the request for an additional or replacement card.

---

[5] Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003, 12 C.F.R. Part 41, 12 C.F.R. Part 222, 12 C.F.R. Parts 334 and 364, 12 C.F.R. Part 571, 12 C.F.R. Part 717, and 16 C.F.R. Part 681 (2007).

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)(F).] This provision therefore preempts state laws only to the extent of the "conduct required." The scope of this preemption language as applied to the final rule has yet to be tested in court. As a result, the extent and practical effect of the preemption provision is not yet known.

Credit Card or Debit Card Numbers Printed on Receipts

California Law

Under state law, any person who accepts credit cards or debit cards for payment may not print more than the last five digits of the credit card or debit card account number or the expiration date on a receipt provided to the cardholder. The prohibition applies only to electronically printed receipts 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. Beginning January 1, 2009, these restrictions are extended to any receipt retained by the business as well. [California Civil Code Section 1747.09.]

Federal Law

Federal law contains a similar provision under the Fair Credit Reporting Act (FCRA), as amended by the Fair and Accurate Credit Transactions Act of 2003 (FACTA). Specifically, federal law requires businesses to truncate credit card and debit card numbers on electronic receipts issued at the point of sale. Like California law, FCRA prohibits the printing of more than the last five digits of the card number or expiration date on receipts provided to the cardholder. The federal law also applies only to electronically printed receipts and does not apply to transactions in which the sole means of recording the number is by handwriting or an imprint or copy of the card. [Fair Credit Reporting Act Section 605(g), 15 U.S.C. 1681c(g).]

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

Disclosure of Minimum Payment Amount

California Law

While this state law is no longer enforceable, as described below, credit card issuers were required to include a warning statement and other specified information regarding minimum payments in billing statements provided to cardholders. [California Civil Code Section 1748.13.] The warning statement must say: "Minimum Payment Warning: Making only the minimum payment will increase the interest you pay and the time it takes to repay your balance." [California Civil Code Section 1748.13(a)(1).] The statute also requires credit card issuers to provide information in billing statements regarding the length of time it will take to pay off various balances if a cardholder pays only the minimum amount. [California Civil Code Section 1748.13(a)(2).]

These provisions were challenged by the American Bankers Association and various banks on the basis that they were preempted by federal banking laws. In *American Bankers Association v. Lockyer,* the trial court held that California's law was preempted in its entirety with respect to federally chartered savings and loans by the Home Owners' Loan Act and related regulations issued by the Office of Thrift Supervision.

As applied to national banks and federal credit unions, the court found that most—but not all—of California's law was preempted by the National Bank Act, Federal Credit Union Act, and related regulations. Specifically, the court found that the minimum payment warning itself [California Civil Code Section 1748.13(a)(1)] was likely not preempted because it did not impose a significant burden on credit card issuers (any burden imposed was likely to be de minimus).

However, the court could not sever this provision so that it applied only to national banks and federal credit unions and not to federally chartered savings and loans regulated under the Home Owners' Loan Act and Office of Thrift Supervision. The court also found that severing this provision would, in effect, require it to "rewrite" the statute, thereby impermissibly intruding on a legislative function. As a result, the court held that the statute in its entirety could not be enforced against federally chartered credit card issuers. [*American Bankers Association v. Lockyer* (2002) 239 F. Supp. 2d 1000.] Pursuant to stipulation, the court later ordered that the statute also would not be enforced against nonfederally chartered credit card issuers. [*American Bankers Association v. Lockyer* (2003) 2003 U.S. Dist. LEXIS 4320.]

Fraudulent Use of Information ("Skimming")

California Law

State law provides that any person who intends to defraud and knowingly and willfully 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(a).]

Preprinted Checks: Disclosures

California Law

State law requires a credit card issuer who extends credit to a cardholder using a preprinted check to disclose that the cardholder's account will be charged if the check is used; in addition, the issuer must indicate the annual percentage rate and the finance charges that will be incurred and whether the finance charges will be triggered immediately upon using the check. [California Civil Code Section 1748.9.] In *Rose v. Chase Manhattan Bank USA, N.A.,* the trial court held that this provision was preempted by the federal National Bank Act (12 U.S.C. 21 et seq.) and as a result cannot be enforced against national banks. [*Rose v. Chase Manhattan Bank USA, N.A.* (2005) 396 F.Supp. 2d 1116.]

Recording Credit Card Numbers on Checks

California Law

State law prohibits retailers, when a consumer pays for goods or services by check, from: (1) requiring the consumer to provide a credit card as a condition of accepting the check, or (2) recording the credit card's number. [California Civil Code Section 1725.]

Recording Personal Information on Credit Card Transaction Forms

California Law

Under state law, any person who accepts a credit card for payment may not record 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

California Law

State law requires 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(a).]

Under California's Consumer Credit Reporting Agencies Act, 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).]

Federal Law

Federal law contains related provisions under the federal Fair Credit Reporting Act (FCRA). Under FCRA, as amended by the Fair and Accurate Credit Transactions Act of 2003 (FACTA), nationwide consumer reporting agencies are required to notify the requester of a credit report when the consumer's address contained in the request differs substantially from the addresses in the consumer's file. [Fair Credit Reporting Act Section 605(h), 15 U.S.C. 1681c.]

FACTA required the Federal Trade Commission, National Credit Union Administration, and specified financial-institution agencies to issue regulations providing guidance on reasonable policies and procedures a user of credit reports should employ when the user receives a notice of an address discrepancy. In July 2006 the agencies issued proposed regulations and a final rule was adopted in October 2007.[6] The final rule is effective January 1, 2008, and covered financial institutions and other entities must be in compliance by November 1, 2008.

The final rule requires a credit report user to develop and implement reasonable policies and procedures designed to enable the user—when a notice of an address discrepancy has been received by the user—to form a reasonable belief that a consumer report relates to the consumer in question. The rule provides examples of reasonable policies and procedures, such as

---

[6] Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003, 12 C.F.R. Part 41, 12 C.F.R. Part 222, 12 C.F.R. Parts 334 and 364, 12 C.F.R. Part 571, 12 C.F.R. Part 717, and 16 C.F.R. Part 681 (2007).

comparing information contained in the report with information the user has obtained and used to verify the consumer's identity in accordance with the requirements of the Customer Identification Program (CIP) rules pursuant to the USA PATRIOT Act [31 U.S.C. 5318(l)].

Although many FCRA 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 imposing any requirement or prohibition "with respect to any subject matter regulated" by FCRA's Section 605 regarding information contained in consumer reports. State laws in effect on September 30, 1996, are exempt. [Fair Credit Reporting Act Section 625(b)(1)(E), 15 U.S.C. 1681t.]

Although the "subject matter regulated" standard would appear to be a preemption standard with broader reach than the "conduct required" standard, whether it preempts the above-described state law regarding verification of a credit applicant's address is ultimately a matter to be decided by the courts. At this time, the extent of this preemption provision has not yet been tested in a court of law, therefore the preemptive effect of this FCRA provision is not yet known.

Credit Reporting

Overview

- A credit report is a credit history about a particular consumer and contains a great deal of information, including annual income; outstanding debt; bill-paying history; the number, types, and age of the accounts; current and previous addresses; social security number; date of birth; telephone number; and, in some cases, employment history, bankruptcies, foreclosures, and tax liens.

- Credit reports are compiled by credit reporting agencies with information from various sources, such as utility or telephone companies, banks, and companies that have granted credit to the consumer. There are different types of credit reporting agencies: nationwide credit bureaus, such as Equifax, Experian, and TransUnion, and specialty consumer reporting agencies, which compile reports about consumers' medical conditions, residential or tenant history, check-writing history, employment history, and insurance claims. The companies sell the information contained in these reports to creditors, insurers, employers, landlords, and other businesses with a "legitimate business need," as specified.[7] Credit reports are used by these entities to evaluate a consumer's application for credit, insurance, employment, or a lease.[8]

- A credit report can play an important role in determining whether a consumer is able to obtain credit, secure employment, rent an apartment, or acquire insurance. As a result, both state and federal law regulate credit reporting agencies.

- Credit reports also help guard against identity theft because they offer consumers a way to monitor their credit histories and look for

---

[7] See Fair Credit Reporting Act, 15 U.S.C. 1681b, for additional discussion.

[8] See Federal Trade Commission, "Building a Better Credit Report," June 2006, http://www.ftc.gov/bcp/edu/pubs/consumer/credit/cre03.pdf, and Privacy Rights Clearinghouse, "How Private is My Credit Report?" October 2006, http://www.privacyrights.org/fs/fs6-crdt.htm.

potentially fraudulent accounts. Accordingly, both state and federal law provide consumers with access to their credit reports. Most recently, the Fair and Accurate Credit Transactions Act of 2003 (FACTA) gave consumers the right to obtain one free credit report from each nationwide credit reporting agency every year.

- California was the first state to give consumers the right to place a "security freeze" on their credit reports, which blocks access to their personal credit information. This provision helps prevent identity theft because credit cannot be extended without the consumer's permission.

Credit Reporting

California Law

California's Consumer Credit Reporting Agencies Act, the state's counterpart to the federal Fair Credit Reporting Act (FCRA), regulates consumer credit reporting agencies. [California Civil Code Section 1785.1 et seq.] Among other things, the statute requires every consumer credit reporting agency to allow a consumer, upon request and with proper identification, to visually inspect all files pertaining to him or her that the agency maintains at the time of the request. The agency must identify recipients who obtained the consumer's credit report within specified time periods, 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 excluded from any list provided by a credit reporting agency for firm offers of credit. [California Civil Code Section 1785.11(d)(1).] Similarly, a consumer may also request that his or her name and address be removed from lists that a consumer credit reporting agency furnishes for credit card solicitations, and

this direction must be honored for a minimum of two years. [California Civil Code Section 1785.11.8.]

Existing state law also permits consumers to dispute inaccurate information and requires a consumer credit reporting agency to reinvestigate disputed information without charge. [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.] If a consumer submits a copy of a valid police report or investigative report from the Department of Motor Vehicles, the agency must block information appearing on the consumer credit report that is a result of identity theft. [California Civil Code Section 1785.16(k).]

California law also places requirements on users of consumer credit reports: 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).]

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).]

Federal Law

The federal Fair Credit Reporting Act (FCRA) provides consumers with one free credit report from each nationwide consumer reporting agency in a 12-month period, upon request. [Fair Credit Reporting Act Section 612(a),15 U.S.C. 1681j,

as amended by the Fair and Accurate Credit Transactions Act of 2003 (FACTA), Pub. L. 108-159, 117 Stat. 1952.]

Except as specified, federal law requires a consumer reporting agency 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 during the previous two years if the report was procured for employment purposes, or the previous year if procured for any other purpose;
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 in which the consumer was identified with a credit or insurance transaction that he or she did not initiate; and
6. A notice 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.]

Generally, a consumer is entitled to a notice when a company takes an adverse action against the consumer, based on information contained in his or her credit report. [Fair Credit Reporting Act Section 615, 15 U.S.C. 1681m(a).] A recent U.S. Supreme Court decision sought to clarify this notice requirement. In *Safeco Insurance Co. of America v. Burr; Geico General Insurance Co. v. Edo*, (2007) 127 S. Ct. 2201, the Court held that a consumer's credit report must have been a necessary condition for the higher rate offered (the adverse action). Furthermore, the Court permitted a first-time applicant for credit or insurance to sue a company under the FCRA when the company must send the consumer an adverse action notice and does not do so. The Court also ruled that companies may be held liable for willful violations of the FCRA when they recklessly disregard the law.

The FACTA amendments to FCRA permit a consumer to dispute inaccurate information directly with the entity that furnished the information to the

consumer reporting agency; it also requires the entity to investigate the disputed information in some circumstances. [Fair Credit Reporting Act Section 623(a)(8),15 U.S.C. 1681s-2.]

If an entity determines 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.]

Federal law requires that, 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 within four business days and notify the entity that supplied the information related to the identity theft, as specified. [Fair Credit Reporting Act Section 605B, 15 U.S.C. 1681c-2.]

Additional significant provisions of FCRA, as amended by FACTA, are described in other summaries throughout this report.

Investigative Consumer Reporting Agencies

California Law

State law regulates investigative consumer reporting agencies. [California Civil Code Section 1786 et seq.] These agencies are defined 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, as specified. [California Civil Code Section 1786.2.] Investigative consumer reports may be given only to third parties the agency believes is using the information for (1) employment purposes, (2) determining

a consumer's eligibility for insurance, (3) leasing a residential unit, or (4) other specified reasons. [California Civil Code Section 1786.12.]

Security Alerts

California Law

Under state law, consumers may place a "security alert" on their credit reports noting that their identity may have been used without consent to fraudulently obtain goods or services in the consumers' names. A consumer credit reporting agency must place a security alert on the consumers' credit reports within five business days after receiving a request. The agency must also notify each person who requests the credit information about the existence of the alert.

The alert remains in place for at least 90 days, and consumers may renew the alert. Any person who uses the consumer's credit report to approve credit and who receives notice of the security alert may not lend money, extend credit, or complete the purchase, lease, or rental of goods or services without first taking reasonable steps to verify a consumer's identity to ensure that the application is not the result of identity theft. [California Civil Code Section 1785.11.1.] See the federal discussion on page 39 for details on the possible preemptive effect of FCRA.

Federal Law

Federal law contains related provisions under the Fair Credit Reporting Act (FCRA), as amended by the Fair and Accurate Credit Transactions Act of 2003 (FACTA), 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 by what is required to initiate them, the length of time they are imposed, and the limits that are imposed on those who use 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 federal 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 to place such an alert 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; pursuant to a rule issued by the Federal Trade Commission, 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; Federal Trade Commission, 16 C.F.R. Parts 603, 613, and 614.]

All three federal 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.]

Federal law regarding security alerts contains preemption provisions. Specifically, Congress preempted states from enacting any requirement or prohibition with respect to the conduct required by the federal security alert provisions described above. [Fair Credit Reporting Act Section 625(b)(5)(B), 15 U.S.C. 1681t.] This provision may arguably preempt California's security alert law to the extent that it relates to the same conduct required under federal law. However, states may be able to act where federal law does not impose a specific requirement. While the scope 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 remains free to act.

Security Freezes

California Law

Under state law, a consumer may 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.[9]

Certain specified entities may access a consumer's credit report even if a security freeze is in place, including law enforcement acting pursuant to a court order or warrant, a child support agency, or the Franchise Tax Board.

A consumer credit reporting agency must place a security freeze on a consumer's credit report within five business days after receiving a request; the security freeze remains in place until the consumer requests its removal. Credit reporting agencies must send consumers a written confirmation of the freeze and provide them with a unique personal identification number or password to use to request the release of their credit information. The freeze may be temporarily lifted by a consumer to grant access to the credit report by a specific party or for a particular period of time.

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.]

---

[9] This provision was invalidated by the Court of Appeal, Second Appellate District, on First Amendment grounds as applied to U.D. Registry (a credit reporting agency that provides consumer credit reports to landlords) because its reports are materially drawn from public records. While the court ruled that California Civil Code Section 1785.11.2 was unconstitutional as applied to U.D. Registry (and could not be enforced against the company), the court refused to hold that the statute was unconstitutional on its face (which would have limited enforcement against other credit reporting agencies). [*U.D. Registry, Inc. v. State of California* (2006) 144 Cal. App. 4th 405.] U.D. Registry petitioned the California Supreme Court to grant review of the decision. This petition was rejected. [*U.D. Registry, Inc. v. State of California* 2007 Cal. LEXIS 3098 (Cal. Feb. 7, 2007).] In 2007 the Legislature amended the statute to address the issues raised in *U.D. Registry, Inc. v. State of California* by providing that a credit reporting agency may disclose public record information it obtains lawfully from an open public record to the extent permitted by law. [California Civil Code Section 1785.11.2(n).]

Data Security

Overview

- In 2003 California became the first state in the nation to require companies and government agencies to notify consumers when there is a breach in the security of their personal information. Since that time, 37 other states and the District of Columbia have followed California's lead and enacted breach notification statutes.[10] Congress is also considering whether to mandate that consumers must be notified when the security of their personal information has been breached.

- According to the Privacy Rights Clearinghouse, more than 217 million records containing sensitive personal information have been involved in security breaches since February 2005.[11]

- Notifying consumers when the security of their personal information has been breached can play an important role in identity theft prevention. For example, a consumer can decide to place a fraud alert or security freeze on his or her credit report, depending on the type of information that was breached and who obtained access to it. Such quick action could prevent an identity thief from obtaining new credit in the consumer's name.

- California's law requiring notification of security breaches has also resulted in the public's—and lawmakers'—heightened interest in data security. For instance, both state and federal law impose security requirements on businesses when they destroy customer records. California law also requires businesses to implement and maintain reasonable security procedures to protect the personal information they own or license.

---

[10] Consumers Union, "Notice of Security Breach State Laws," August 21, 2007, http://www.consumersunion.org/campaigns/Breach_laws_May05.pdf.

[11] For a listing of data breaches, see Privacy Rights Clearinghouse, "A Chronology of Data Breaches," http://www.privacyrights.org/ar/ChronDataBreaches.htm. This listing is updated regularly.

Destruction of Business and Medical Records

California Law

State law 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 it is unreadable or undecipherable. The law defines "customer" as "an individual who provides personal information to a business for the purpose of purchasing or leasing a product or obtaining a service from the business." [California Civil Code Sections 1798.80 and 1798.81.]

Under the statute, "personal information" is defined broadly to mean any information that identifies, relates to, describes, or is capable of being associated with a particular individual. In this instance, personal information includes the individual's name, signature, social security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information. [California Civil Code Section 1798.80.]

California's Confidentiality of Medical Information Act also contains provisions safeguarding the destruction and disposal of medical records. The act requires health care providers, health care service plans, pharmaceutical companies, and contractors—when destroying or disposing of medical records—to do so in a manner that preserves the confidentiality of the information contained in the records. [California Civil Code Section 56.101.]

Federal Law

Federal law includes provisions relating to the destruction of business records, but more narrowly addresses the issue. As described on the opposite page, California law concerns all personal information contained in customer records. Yet federal law only relates to consumer reports or information derived from such reports for a business purpose, and its requirements are imposed only on users of those reports.

Under the federal Fair Credit Reporting Act (FCRA) and a related final rule issued in June 2005 by the Federal Trade Commission, businesses and individuals must properly dispose of such information by taking reasonable measures to protect against unauthorized access to, or use of, the information when it is disposed. The law applies to anyone who uses consumer reports and applies to 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, as defined under FCRA. [Fair Credit Reporting Act Section 628, 15 U.S.C. 1681w; Federal Trade Commission, 16 C.F.R. Part 682.]

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.]

Under FACTA, Congress preempted states from enacting any requirement or prohibition regarding the "conduct required by" specific provisions. This language arguably allows states to act where federal law does not impose a specific requirement. The extent and practical effect of the FACTA preemption provisions are not yet known. It also is noteworthy that because California law is broader—applying to more than just information obtained from credit reports and more than just persons or entities who use these reports—the preemptive effect of FCRA on the state law described on the opposite page may be limited.

Notification of Breach in Data Security

California Law

State law 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 data security breach immediately following the discovery if personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

The statutes define "personal information" to mean an individual's first name or first initial and last name in combination with one of the following, when either the name or the data elements are not encrypted: (1) social security number, (2) driver's license or California identification card number, (3) account, credit, or debit card number in combination with a security code or password that would permit access to the individual's financial account, (4) medical information, or (5) health insurance information. Personal information does not include information publicly available from federal, state, or local government records. State agencies and businesses must provide

notice to consumers using either written notice, electronic notice, or substitute notice, as specified.[12] [California Civil Code Sections 1798.29 and 1798.82.]

Personal Information: Reasonable Security Procedures

California Law

Under state law, a business that owns or licenses personal information about a California resident must implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the 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. [California Civil Code Section 1798.81.5.]

The statute defines "personal information" to mean an individual's first name or first initial and last name in combination with one of the following, when either the name or the data elements are not encrypted: (1) social security number, (2) driver's license or California identification card number, (3) account, credit, or debit card number in combination with a security code or password that would permit access to the individual's financial account, or (4) medical information. Personal information does not include information that is publicly available from federal, state, or local government records. The section does not apply to financial institutions, health care providers, or other specified entities. [California Civil Code Section 1798.81.5.]

---

[12] Although there is no federal statutory law specifically on this issue, several federal agencies have issued guidance on security breaches under the "Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice." The guidance is intended to clarify the responsibilities of financial institutions under federal laws and interpret requirements of Gramm–Leach–Bliley. The guidance addresses "unauthorized access to, or use of, customer information that could result in substantial harm or inconvenience to a customer." The guidance also includes standards for when a financial institution should provide notice to customers when sensitive information is accessed without authorization. State laws not inconsistent with Gramm–Leach–Bliley are not preempted. [Office of the Comptroller of the Currency, 12 C.F.R. Part 30; Federal Reserve System, 12 C.F.R. Parts 208 and 225; Federal Deposit Insurance Corporation, 12 C.F.R. Part 364; and Office of Thrift Supervision, 12 C.F.R. Parts 568 and 570, http://www.occ.treas.gov/consumer/Customernoticeguidance.pdf.] Gramm–Leach–Bliley generally provides that state laws that are more protective of consumers' privacy are not "inconsistent." [15 U.S.C. 6807.]

Financial Privacy and Related Issues

Overview

- California led the nation in enacting the Financial Information Privacy Act, which gives consumers more control over their personal financial information than what is currently granted by federal law.

  The act gives consumers the ability to control the sharing of their nonpublic personal information by requiring a financial institution to obtain a consumer's consent before it may share the information with a nonaffiliated third party. This is commonly known as an "opt in" because a financial institution may not share a consumer's information unless he or she opts to share it. Federal law, however, subjects the sharing of personal information with nonaffiliated third parties to an "opt out" so that, as long as the consumer does not opt out, a financial institution may share his or her information with nonaffiliated third parties. Federal law allows states to provide consumers with greater privacy protections; therefore, with respect to sharing with nonaffiliated third parties, California law controls.

- California law also subjects the sharing of nonpublic personal information with affiliates to an opt out, whereas federal law does not place restrictions on affiliate sharing. The validity of this section of California's financial privacy law is presently before the courts and is described in more detail on page 53.

- Both state and federal law regulate the practice of debt collection and impose restrictions on threatening or harassing behavior.

Account Numbers

California Law

State law prohibits a financial institution from reusing a checking or savings account number until at least three years have passed since a previous account using that same number was closed. [California Financial Code Section 4100.]

Debt Collection

California Law

California's Rosenthal Fair Debt Collection Practices Act regulates third-party debt collectors in a manner similar to the federal law described below. 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. The protections of this act also apply to businesses. [California Civil Code Section 1788 et seq.]

Federal Law

The business practices of third-party debt collectors are regulated under the federal Fair Debt Collection Practices Act. Among other things, the act requires 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. Federal 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. The federal act specifically allows for state regulation regarding debt collection practices, provided that state laws are not inconsistent with federal law. State laws may give consumers greater protection than federal law. [Fair Debt Collection Practices Act, 15 U.S.C. 1692 et seq.]

Financial Privacy

California Law

California's Financial Information Privacy Act places restrictions on the sharing of consumers' nonpublic personal information by financial institutions. "Nonpublic personal information" does not include publicly available information; it 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.
   [California Financial Code Section 4052(a).]

A financial institution must first obtain a consumer's consent before it may disclose or share the consumer's nonpublic personal information with any nonaffiliated third party (an "opt in").[13] [California Financial Code Section 4053(a)(1).] Before disclosing nonpublic personal information to an affiliate, a financial institution must give a consumer an opportunity to direct that his or her information may not be disclosed (an "opt out"). [California Financial Code Section 4053(b)(1).] The preemptive effect of the Fair Credit Reporting Act on this restriction is a matter currently before the courts.[14]

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. [California Financial Code Section 4053(b)(2).] The unrestricted sharing of nonpublic personal information

---

[13] For descriptions of "opt in" and "opt out," see page 51.

[14] The restriction on sharing with affiliates was challenged by the American Bankers Association, Financial Services Roundtable, and Consumer Bankers Association on the basis that it was preempted by the Fair Credit Reporting Act (FCRA). The U.S. Court of Appeals for the Ninth Circuit agreed and directed the U.S. District Court to determine the scope of the preemption. [*Am. Bankers Ass'n v. Gould*, 412 F.3d 1081.] In October 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 FCRA. The court made clear in its ruling, however, that other provisions of California's financial privacy law still stand. [*Am. Bankers Ass'n v. Lockyer,* 2005 U.S. Dist. LEXIS 22437.] In November 2005 the attorney general's office filed a notice of appeal with the U.S. Court of Appeals for the Ninth Circuit. This appeal is pending.

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 Section 4053(c).]

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).]

Federal Law

Federal law prohibits a financial institution, under the Gramm–Leach–Bliley Act (GLB) of 1999 (Pub. L. 106-102, 113 Stat. 1338), 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 the financial institution's specified privacy policies and practices, (2) gives the consumer the opportunity to stop the disclosure before the information is initially disclosed (an "opt out"), and (3) provides the consumer with an explanation of how to exercise his or her right to opt out. [15 U.S.C. 6802(b)(1).] The act contains specified exceptions. [15 U.S.C. 6802(e).]

Under 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 GLB's provisions (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. [15 U.S.C. 6802(b)(2).]

GLB also specifically invites states to enact greater privacy protections than those contained in the federal act. [15 U.S.C. 6807.]

In 2006 Congress passed the Financial Services Regulatory Relief Act of 2006 (Pub. L. 109-351, 120 Stat. 1966), which amended GLB to require federal agencies to jointly develop a model privacy form for financial institutions to use for GLB-required disclosures to consumers. The act requires the agencies to develop a form that is succinct and comprehensible and allows consumers to easily identify and compare the sharing and privacy practices of financial institutions. Under the act, a financial institution that uses the model form is deemed to have satisfied the notice requirements of GLB (a "safe harbor"). In March 2007, pursuant to the act, eight federal regulators issued a notice of proposed rulemaking regarding a model privacy form.[15] Public comments were due by May 29, 2007. A final rule has not yet been issued.

Insurance Information and Privacy Protection Act

California Law

State law governs the collection, use, and disclosure of information gathered in connection with insurance transactions. The act generally limits disclosure of personal information by insurers and agents without the written consent of the individual. [California Insurance Code Section 791 et seq.]

[15] Interagency Proposal for Model Privacy Form Under the Gramm–Leach–Bliley Act, 72 Fed. Reg. 14940 (2007) (to be codified at 12 C.F.R. Part 40, 12 C.F.R. Part 573, 12 C.F.R. Part 216, 12 C.F.R. Part 332, 12 C.F.R. Part 716, 16 C.F.R. Part 313, 17 C.F.R. Part 160, and 17 C.F.R. Part 248) (proposed March 29, 2007).

Insurers: Genetic Testing

California Law

State law prohibits insurers from requiring a genetic test for the purpose of determining insurability, except for policies contingent on review or testing for other diseases or medical conditions. If an insurer requires a genetic test to determine insurability, the insurer must comply with informed consent and privacy protection rules, as specified. [California Insurance Code Section 10148.]

Civil penalties may be assessed for the willful or negligent disclosure of genetic test results if those results are disclosed in a manner that identifies or provides identifying characteristics about the subject of the test. Any person who negligently or willfully discloses the results is also liable for actual damages, including damages for resulting economic, bodily, or emotional harm. [California Insurance Code Section 10149.1.]

Identity Theft

Overview

- For the seventh year in a row, identity theft topped the Federal Trade Commission's list of top 10 consumer complaints in 2006.[16] Of the 674,354 complaints filed with the commission during that year, 246,035—or 36 percent—related to identity theft.[17] The most common form of reported identity theft was credit card fraud (25 percent of complaints), followed by phone or utilities fraud (16 percent), bank fraud (16 percent), and employment fraud (14 percent).[18]

  Among the 50 states, California ranked third in identity theft victims per capita, after Arizona and Nevada.[19] Five of the top 10 major metropolitan areas with the highest per capita rates of reported identity theft were in California: Napa, Madera, Yuba City, Hanford–Corcoran, Vallejo–Fairfield.[20]

- Many Americans are concerned about the threat of identity theft. In a poll by Zogby International conducted on March 23–26, 2007, 91 percent of nationwide respondents said they are concerned their identity could be stolen and used to make unauthorized purchases. One in three surveyed said they are not confident that retailers, banks, and credit card companies are taking sufficient steps to safeguard their personal information.[21]

- Over the years, both California and Congress have enacted various statutes relating to identity theft. State and federal law, for example, both impose criminal penalties for the crime of identity theft. California law also allows an identity theft victim to petition a court for a finding of innocence when an identity thief has committed crimes in the victim's name. And California recently enacted a statute requiring county welfare departments to obtain a credit report on behalf of foster-care children to determine whether they have been a victim of identity theft.

---

16 Federal Trade Commission, "FTC Issues Annual List of Top Consumer Complaints," February 7, 2007, http://www.ftc.gov/opa/2007/02/topcomplaints.shtm.

17 Federal Trade Commission, Consumer Sentinel and Identity Theft Data Clearinghouse, "Consumer Fraud and Identity Theft Complaint Data, January–December 2006," February 2007, p. 5, http://www.consumer.gov/sentinel/pubs/Top10Fraud2006.pdf.

18 Id., p. 13.

19 Id., p. 18.

20 Id., p. 17.

21 Zogby International, "Zogby Poll: Most Americans Worry About Identity Theft," April 3, 2007.

Crime of Identity Theft

California Law

Under state law, it is unlawful to willfully use someone else's personal identifying information for an unlawful purpose, including to obtain or attempt to obtain credit, goods, services, or medical information in the name of the other person without that person's consent. [California Penal Code Section 530.5(a).]

State law also prohibits acquiring or retaining possession of personal identifying information with the intent to defraud. [California Penal Code Section 530.5(c).] Additional penalties are imposed if the violator has previously been convicted of identity theft or possesses the personal information of 10 or more people. [California Penal Code Sections 530.5(c)(2) and (c)(3).] Also prohibited is the sale, transfer, or conveyance of personal identifying information with actual knowledge that it will be used to commit identity theft. [California Penal Code Section 530.5(d)(2).]

"Personal identifying information" includes, among other things, name, address, telephone numbers, social security number, driver's license number, mother's maiden name, checking or savings account numbers, unique biometric data (such as a fingerprint), or credit card numbers. [California Penal Code Section 530.55.]

Federal Law

Federal law makes it a crime to knowingly transfer, possess, or use another person's means of identification with the intent to commit, aid, or abet an unlawful activity that violates federal law or constitutes a felony under state law. [18 U.S.C. 1028(a)(7).] Federal law also provides for "aggravated identity theft," requiring a mandatory sentence of two years imprisonment for knowingly transferring, possessing, or using another person's identification while committing a specified felony violation. [18 U.S.C. 1028A(a)(1).]

Debt Collection Activities

California Law

Under state law, debt collectors must 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 does not establish that the debtor is not responsible for the debt in question. These protections also apply to businesses. [California Civil Code Section 1788.18.]

Deceptive Identification Documents

California Law

State law provides that it is a misdemeanor to possess a document-making device with the intent to manufacture, alter, or authenticate a deceptive identification document. A deceptive identification document may include a driver's license, birth certificate, or passport that purports to be (or which might deceive an ordinary reasonable person into believing that it is) a document issued by a state or federal governmental agency. [California Penal Code Section 483.5.]

Department of Justice Identity Theft Victim Database

California Law

Under state law, the Department of Justice must create and maintain a database of identity theft victims and limit access to the database to criminal justice agencies, identity theft victims, and individuals and agencies authorized by the victims. [California Penal Code Section 530.7(c).]

Falsely Obtaining Department of Motor Vehicles' Documents

California Law

State law 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.[22] A person convicted of conspiracy to commit identity theft may be fined up to $25,000. [California Penal Code Section 182.]

[22] 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.

Identity Theft Victim's Right to Free Credit Reports

California Law

State law requires consumer credit reporting agencies to provide identity theft victims, upon request, 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 must first provide an identity theft police report or a similar report. [California Civil Code Section 1785.15.3(b).]

Federal Law

Federal law also requires nationwide consumer reporting agencies to provide free reports to identity theft victims under the Fair Credit Reporting Act (FCRA), as amended by the Fair and Accurate Credit Transactions Act of 2003 (FACTA). 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 obtain 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 38). [Fair Credit Reporting Act Sections 605A(a)(2) and (b)(2) and 612(d), 15 U.S.C. 1681c-1.]

Under the FACTA amendments to FCRA, Congress preempted state laws with respect to the conduct required by these sections. [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

California Law

Under state law, a magistrate in the county where an identity theft victim resides may issue a warrant to search a person or property in another county. [California Penal Code Section 1524(j).]

Judicial Determination of Innocence

California Law

State law 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, 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 Section 530.6(b).]

Jurisdiction for Prosecuting Identity Theft Crime

California Law

State law specifies that the jurisdiction of a criminal action for unauthorized use of personal identifying information includes 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

California Law

State law 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 a Creditor

California Law

Under state law, an identity theft victim may bring legal action against a creditor to establish that he or she is a victim of identity theft. The law requires the victim to prove by a preponderance of the evidence that, in the case of a particular debt, he or she is an identity theft victim. If the victim is able to do so, then he or she is entitled to a judgment declaring that he or she is not obligated to pay the creditor for the particular debt. The victim may obtain an injunction preventing the creditor from collecting the debt from the victim or enforcing any security interest in the victim's property for that claim. In addition, a victim may obtain actual damages, attorney's fees and costs, and any equitable relief deemed appropriate by the court. [California Civil Code Sections 1798.92 and 1798.93.]

The judgment may also include a civil penalty of up to $30,000 if the victim establishes by clear and convincing evidence that (1) at least 30 days prior to filing the action, the victim gave written notice to the creditor of the suspected identity theft as well as the basis for the belief that identity theft has taken place, (2) the creditor failed to diligently investigate the possible identity theft, and (3) the creditor continued to pursue the claim against the victim after being

presented with facts later held to entitle the victim to the previously described judgment. [California Civil Code Section 1798.93.]

An identity theft victim must bring an action against a creditor within four years of the date the victim knew or, in the exercise of reasonable diligence, should have known of the existence of facts that would give rise to the action. [California Civil Code Section 1798.96.]

Right to Obtain Records of Fraudulent Transactions or Accounts

California Law

State law provides that if an identity theft victim discovers that an unauthorized person has either filed an application or opened an account 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 and identifying information, as specified. [California Penal Code Section 530.8.] For possible preemptive effect of FCRA on this provision, see the federal law discussion on page 67.

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

Federal Law

Federal law also requires a business that has provided credit, goods, or services 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, under the Fair Credit Reporting Act (FCRA), as amended by the Fair and Accurate Credit Transactions Act of 2003 (FACTA).

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. 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 FCRA 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 imposing 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.]

Although this would appear to be a preemption standard with broader reach than the "conduct required" standard, whether it preempts the above-described state law is ultimately a matter to be decided by the courts. The extent of this preemption provision has not yet been tested in a court of law, and, as a result, the preemptive effect of this FCRA provision is not yet known.

Statute of Limitations

California Law

Under state law, 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.]

Youth in Foster Care: Request for Credit Report

California Law

State law requires a county welfare department to request a credit report on behalf of a foster-care child to determine whether an identity theft has occurred; the report must be requested when the youth reaches 16 years of age. If the report indicates that some form of identity theft has occurred, the department must refer the youth to an approved counseling organization that provides services to identity theft victims. [Welfare and Institutions Code Section 10618.6.]

Marketing

Overview

- Using personal information for marketing purposes continues to be an issue of particular interest. Consumers have overwhelmingly responded to opportunities to control the use of their personal information. One example is the nationwide "Do Not Call" Registry, in which consumers may include their telephone numbers to reduce unwanted telemarketing sales calls. This registry has been tremendously popular, and according to its administrator, the Federal Trade Commission, 145 million phone numbers have been placed on the list.[23]

- Both state and federal law restrict the sending of unsolicited commercial e-mail messages (spam). Federal law largely preempts state spam laws except that state laws may prohibit "falsity or deception in any portion" of a commercial e-mail message or attachment.

- California law also places various restrictions on marketing practices, including regulation of the following: offering gifts to college students for filling out credit card applications, using supermarket club cards, marketing to children under 16 years of age, acquiring medical information for marketing purposes unless certain disclosures are made, and sending unsolicited text messages.

- California requires businesses to disclose their information-sharing practices if they share customers' personal information with third parties for marketing reasons. According to the Privacy Rights Clearinghouse, California's law is the only one of its kind in the country.[24]

---

[23] Federal Trade Commission, "Enhancing FTC Consumer Protection in Financial Dealings, With Telemarketers, and on the Internet," testimony before the Subcommittee on Commerce, Trade, and Consumer Protection; Committee on Energy and Commerce; U.S. House of Representatives; October 23, 2007.

[24] Privacy Rights Clearinghouse, "'Shine the Light' on Marketers: Find Out How They Know Your Name," July 2005, http://www.privacyrights.org/fs/fs4a-shinelight.htm.

Affiliate Marketing

Federal Law

In October 2007 the Federal Trade Commission (FTC) issued a final rule regarding marketing by affiliated companies.[25] Under the Fair and Accurate Credit Transactions Act of 2003 (FACTA), a consumer has the right to restrict a company from using certain information about him or her obtained from an affiliated company to solicit the consumer for marketing purposes. [Fair Credit Reporting Act Section 624, 15 U.S.C. 1681s-3.] The final rule issued by the FTC implements this provision.

FACTA prohibits a company from using specified information it receives from an affiliate about a consumer for marketing its own products and services to the consumer unless the consumer is given clear and conspicuous notice that the information may be used by affiliates and an opportunity to opt out of that use. [Fair Credit Reporting Act Section 624(a), 15 U.S.C. 1681s-3.]

The consumer's opt out must be effective for at least five years and a company may not use the consumer's information when the five-year period expires, unless the consumer receives a notice and an opportunity to extend the opt out for another period of at least five years and the consumer does not opt out. [Fair Credit Reporting Act Section 624(a)(3), 15 U.S.C. 1681s-3.]

The consumer's right to opt out of an affiliate's use of information does not apply in certain instances, such as when the company making the solicitation has a "pre-existing business relationship"[26] with the consumer or when the information is used in response to a communication initiated by the consumer or in response to a solicitation authorized or requested by the consumer. [Fair Credit Reporting Act Section 624(a)(4), 15 U.S.C. 1681s-3.]

---

[25] Affiliate Marketing Rule, 72 Fed. Reg. 61424 (2007) to be codified at 16 C.F.R. Parts 680 and 698.
[26] The final rule issued by the FTC further defines "pre-existing business relationship" and provides examples.

The FTC's final rule became effective January 1, 2008, and compliance is mandatory by October 1, 2008. The rule also contains model opt-out and notice forms.

Cell Phone Directory: Opt in Required

California Law

State law 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 consent may be given on an Internet Web site; 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

California Law

Under state law, a consumer may request that his or her name be removed from any list a consumer credit reporting agency furnishes for credit card solicitations. [California Civil Code Section 1785.11.8.]

Direct Marketing: Medical Information

California Law

State law prohibits businesses from directly requesting any medical information from an individual, regardless of whether the information pertains to him or her, and using, sharing, or otherwise disclosing that information for

direct marketing purposes without taking the following 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

California Law

Under state law, the governing bodies and alumni associations of California State University (CSU), University of California (UC), and Hastings College of the Law may disclose the names, addresses, and e-mail addresses of alumni to businesses offering various commercial products and services, provided that specified privacy requirements are met. For example, alumni must be offered an opportunity to opt out of the sharing. These disclosure provisions sunset on January 1, 2011. [California Education Code Sections 89090 and 92630.]

Disclosure of Personal Information to Direct Marketers

California Law

State law requires a business that discloses personal information to third parties for marketing purposes to either (1) disclose to customers, upon request, a list of the categories of personal information (such as name, address, telephone number, social security number, e-mail address, or occupation) that the business has disclosed in the preceding calendar year to third parties for marketing purposes, as well as 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.

"Personal information" is defined as "any information that, when it was disclosed, identified, described, or was able to be associated with an individual." The statute does not apply to financial institutions in compliance with California's Financial Information Privacy Act, as enacted. [California Civil Code Section 1798.83.]

Marketing to Children Under 16 Years of Age

California Law

Under state law, it is 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. "Child" is defined as a person under 16 years of age. 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.

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

On-Campus Marketing: Credit Cards

California Law

A 2007 state law urges the Regents of the University of California and requires the Trustees of the California State University and the Board of Governors of the California Community Colleges to do the following:

1. Direct each campus every year to disclose all exclusive arrangements, excluding proprietary information, that allow banks or other commercial entities to engage in on-campus credit card marketing to students using tabling activities in public areas; and
2. Prohibit banks and other commercial entities from offering gifts to students for filling out credit card applications during on-campus tabling activities. [California Education Code Section 99040.]

Satellite and Cable Television Subscribers

California Law

State law prohibits satellite or cable television providers, without the subscriber's express 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

California Law

State law 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 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 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 written confidentiality agreement with the outside company stating that the outside company agrees not to sell or share the cardholder's information. [California Civil Code Section 1749.65(c).]

Telecommunications: Residential Subscriber Information

California Law

Under state law, telephone companies may not disclose, without the residential subscriber's written consent, the subscriber's personal calling patterns, credit

or other personal financial information, services purchased, or demographic information, subject to specified exceptions. [California Public Utilities Code Section 2891.]

Telemarketing: "Do Not Call" Registry

California Law

After federal implementation of the nationwide registry described below, 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, such as 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.]

Federal Law

Federal law 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. Federal law also places restrictions on when a telemarketer may call a consumer's residence, prohibiting phone calls at any time except between 8:00 a.m. and 9:00 p.m. (local time at the consumer's location). [Telemarketing Sales Rule, 16 C.F.R. Part 310, Telemarketing and Consumer Fraud and Abuse Prevention Act, 15 U.S.C. 6101 et seq.]

Telephone Consumer Protection Act of 1991

Federal Law

Federal law places some restrictions on the use of automated telephone equipment and pre-recorded messages. [Telephone Consumer Protection Act of 1991, 47 U.S.C. 227.]

Unsolicited Commercial E-mail Messages (Spam)

California Law

State law prohibits any person or entity from sending unsolicited commercial e-mail advertisements from California or to a California e-mail address.[27] [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 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 third party's permission;
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 specifically allows the attorney general, an e-mail service provider, or a recipient of an unsolicited commercial e-mail to bring an action against a

---

[27] Also see the preemptive effect of federal law outlined on page 80.

person or entity who violates the law. A successful plaintiff may recover actual damages and/or liquidated damages of $1,000 for each unsolicited commercial e-mail transmitted in violation of the law, with a cap of $1 million per incident. A violation of the statute is also a misdemeanor. [California Business and Professions Code Section 17529.5.]

The collection of e-mail addresses posted on the Internet is unlawful under state law if the purpose of the collection is to use the addresses to initiate or advertise in an unsolicited commercial e-mail advertisement sent from California or to a California e-mail address. It is also prohibited to use an e-mail address obtained from an automated system that randomly combines names, letters, and numbers for this same purpose. [California Business and Professions Code Section 17529.4.]

Registered users of e-mail service providers are prohibited from using the provider's equipment in violation of the provider's policy, which prohibits or restricts the sending of unsolicited e-mail advertisements. [California Business and Professions Code Section 17538.45.]

Federal Law

The federal Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM) regulates e-mail messages with the primary purpose of advertising or promoting a commercial product or service. [15 U.S.C. 7701 et seq. Also see 16 C.F.R. Part 316.] CAN-SPAM expressly preempts a state law that regulates the sending of unsolicited commercial e-mails except to the extent that the state law "prohibits falsity or deception in any portion" of a commercial e-mail message or attachment. [15 U.S.C. 7707.] California law may therefore regulate false or deceptive aspects of unsolicited commercial e-mail. [4 Witkin, Summary of Cal. Law (10th ed.) Sales, Section 336.]

CAN-SPAM 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.]

Unsolicited Text Messages

California Law

State law prohibits a person, business, candidate, or political committee from transmitting unsolicited text-message advertisements to a cellular telephone, pager, or two-way messaging device, except as specified. The statute covers messages with the principal purpose of promoting the sale of goods or services or a political purpose or objective. The law exempts text messages transmitted by a business, candidate, or political committee that has an existing relationship with the subscriber—if the subscriber is given the opportunity to opt out of receiving text messages from that entity. [California Business and Professions Code Section 17538.41.]

Medical Privacy

Overview

- In a February 2007 poll by UPI–Zogby International, more than half of U.S. respondents expressed concerns about the privacy of their medical records. The poll asked consumers to rate their privacy concerns on a scale of 1 to 5: 1 equals "not at all concerned" and 5 equals "highly concerned." Half rated their concerns as either a 5 (28.4 percent) or 4 (22.1 percent), and only 11.4 percent said they are "not at all concerned."[28]

- A 2005 survey by the California HealthCare Foundation found that 67 percent of national respondents are "very concerned" or "somewhat concerned" about the privacy of their personal medical records.

  The survey respondents also have opinions about hospitals and doctors' offices shifting to computer-based systems: 63 percent believe the computerization of records helps reduce medical errors, and most —93 percent—believe it gives doctors and nurses quicker and easier access to patient information.

  Data security issues are another concern: 72 percent of the survey respondents believe computerization "increases occurrence of unauthorized break-ins to computer systems/payment systems." And 66 percent believe that storing their medical records in paper format is "very secure" or "somewhat secure" compared with 58 percent who feel their records are more secure when stored in an electronic format.[29]

- In September 2007 the secretary of the California Health and Human Services Agency established the California Privacy and Security

[28] UPI–Zogby International, "UPI Poll: Concern on Health Privacy," February 21, 2007.
[29] California HealthCare Foundation, "National Consumer Health Privacy Survey 2005," November 9, 2005, conducted by Forrester Research, Inc., http://www.chcf.org/documents/ihealth/ConsumerPrivacy2005Slides.pdf.

Advisory Board (CalPSAB), noting that consumers have a lack of confidence and trust in existing protections for the electronic exchange of health information. CalPSAB is a collaboration of public and private stakeholders tasked with making recommendations on privacy and security standards and policies regarding the exchange of health information.[30]

- Both California and federal law regulate the privacy of patients' medical information. At the federal level, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) sets a national standard for the privacy of health information while California's Confidentiality of Medical Information Act (CMIA) provides state protections. HIPAA preempts contrary state laws but generally allows states to provide patients with stronger privacy protections than provided under HIPAA.

Medical Privacy

California Law

California's 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, a provider, plan, or contractor must disclose medical information if required by a court order, subpoena, or search warrant, among other things. [California Civil Code Section 56.10(b).] In other specified circumstances, a provider or plan may disclose medical

[30] For additional information on CalPSAB, see http://www.ohi.ca.gov/state/calohi/ohiHome.jsp.

information. For example, a provider or plan may disclose the information for purposes of diagnosis or treatment of the patient or to provide billing or other administrative services to the provider or plan. A provider or plan also may disclose medical information for certain other purposes or to particular individuals, as specified. [California Civil Code Section 56.10(c).]

"Medical information" is defined as any individually identifiable information, in electronic or physical form, concerning a patient's medical history, mental or physical condition, or treatment. [California Civil Code Section 56.05(g).] A recent state law applies the CMIA provisions to any business organized for the purpose of maintaining medical information in order to make the information available to an individual or health care provider for purposes of allowing the individual to manage his or her information or for the diagnosis and treatment of the individual. [California Civil Code Section 56.06(a).]

Unless expressly authorized by the patient, enrollee, or subscriber, CMIA prohibits health care providers, plans, and contractors from using a patient's medical information for marketing purposes or any other purpose not necessary to provide health care services to the patient. [California Civil Code Section 56.10(d).] "Marketing" means a communication about a product or service that encourages recipients to purchase or use the product or service, except that certain communications are specifically excluded. For example, marketing does not include communications in which the communicator does not receive direct or indirect remuneration.

Also excluded from CMIA's definition of marketing are communications that meet the following two requirements:

1. They are tailored to the patient's circumstances to educate or advise him or her about treatment options, and otherwise maintain his or her adherence to a prescribed course of treatment for a chronic and seriously debilitating or life-threatening condition, as defined; and
2. They are paid for, either directly or indirectly, by a third party. In this case, the patient must be notified that the provider, contractor, or health

plan has been remunerated, as specified, and he or she must be given the opportunity to opt out of future remunerated communications by receiving instructions describing how to opt out by calling a toll-free number. [California Civil Code Section 56.05(f).]

CMIA also requires health care providers, plans, contractors, and pharmaceutical companies to preserve the confidentiality of medical records they create, maintain, store, dispose of, or destroy. [California Civil Code Section 56.101.]

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 not to exceed $3,000. The cost of litigation and attorneys' fees (not to exceed $1,000) also may be recovered. [California Civil Code Sections 56.35 and 56.36.]

Federal Law

The federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) specifies minimum privacy protections for patients' personal medical information. [Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. 1320d et seq.] Pursuant to HIPAA, the U.S. Department of Health and Human Services issued the "Standards for Privacy of Individually Identifiable Health Information" ("Privacy Rule"), which created national privacy standards for patients' information (called "protected health information" under the Privacy Rule). [45 C.F.R. 164.500 et seq.]

The Privacy Rule applies to health plans, health care clearinghouses, and health care providers that transmit any health information in electronic form that pertains to a transaction covered by the rule.[31] Under the rule, patients

[31] U.S. Department of Health and Human Services, Office for Civil Rights, "Summary of the HIPAA Privacy Rule," May 2003, http://www.hhs.gov/ocr/privacysummary.pdf, p. 2.

have the right to see and request correction of their medical records, except as specified. [45 C.F.R. 164.524 and 45 C.F.R. 164.526.] Entities covered under the Privacy Rule must provide patients with a notice of their privacy practices, which must contain specified information including a description of how the entity uses and discloses patients' information. [45 C.F.R. 164.520.]

Under federal law, patients also have the right to an accounting of the disclosures of their medical information by a covered entity or its business associates during the prior six years. Certain kinds of disclosures are excluded from these accountings, such as when the information was disclosed for treatment, payment, or health care operations. [45 C.F.R. 164.528.]

In general, the Privacy Rule states that a covered entity may not use or disclose protected health information except as the rule permits or requires or as authorized by the patient in writing. [45 C.F.R. 164.502(a).] Certain uses or disclosures are specifically permitted, such as for treatment, payment, or health care operations or pursuant to a valid authorization for use or disclosure for marketing purposes. [45 C.F.R. 164.502(a)(1).] Covered entities are required to disclose health information in only two instances: (1) to a patient who has requested access to, or an accounting of disclosures of, his or her medical record, or (2) to the U.S. Department of Health and Human Services in connection with a compliance investigation. [45 C.F.R. 164.502(a)(2).]

The federal Privacy Rule requires covered entities to obtain a valid authorization from the patient before they may use or disclose the patient's health information for marketing. An authorization is not necessary if the communication is a face-to-face communication made by a covered entity to the patient or a promotional gift of nominal value provided by the covered entity. If the marketing involves direct or indirect remuneration to the covered entity from a third party, the authorization must state this fact. [45 C.F.R. 164.508(a)(3).]

Marketing is defined under the Privacy Rule as a communication about a product or service that encourages recipients to purchase or use the product

or service. The definition specifically excludes some communications if they are made (1) to describe a health-related product or service that is included in the covered entity's benefit plan, (2) for treatment of the individual, or (3) to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual. Marketing includes arrangements between a covered entity and a third party in which the covered entity discloses health information to the other party in exchange for direct or indirect remuneration, so that the other party may communicate with patients about its own products or services and encourage them to purchase or use those products or services. [45 C.F.R. 164.501.]

The Privacy Rule requires a covered entity to maintain appropriate administrative, technical, and physical safeguards to protect the privacy of a patient's health information. Covered entities must reasonably safeguard health information from intentional or unintentional uses or disclosures that violate the Privacy Rule, and they must limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure. [45 C.F.R. 164.530(c).]

A covered entity must also mitigate, to the extent practicable, any harmful effects it learns resulted from the use or disclosure of health information by the entity or its business associates that was in violation of either the entity's privacy policy or the Privacy Rule. [45 C.F.R. 164.530(f).]

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.] The Privacy Rule defines a contrary state law as one where either (1) a covered entity would find it impossible to comply with both the state and federal requirements, or (2) the state law provision stands as an obstacle to accomplishing and executing "the full purposes and objectives" of specified provisions of HIPAA. A state law is more stringent than HIPAA if it meets one or more of the following criteria:

1. The state law prohibits or restricts the use or disclosure of health information in circumstances where it would be permitted by HIPAA (unless the disclosure is either to the patient, who is the subject of the health information, or is required by the U.S. Department of Health and Human Services in determining whether a covered entity is in compliance with HIPAA);
2. The state law gives patients greater rights of access to, or amendment of, their medical records;
3. The state law provides patients with a greater amount of information concerning their rights and remedies or the use or disclosure of their health information;
4. The state law increases the privacy protections granted to patients with respect to the "form, substance, or the need for express legal permission" from the patient for use or disclosure of his or her health information. A state law is also more stringent if it narrows the scope or duration of the permission or reduces the coercive effect of the circumstances surrounding the permission;
5. The state law provides for recordkeeping or accounting-of-disclosure requirements that compel the retention or reporting of more detailed information than required by HIPAA. A state law is also more stringent if it imposes recordkeeping or accounting-of-disclosure requirements for a longer duration; or
6. The state law provides greater privacy protection for the patient with respect to any other matter. [45 C.F.R. 160.202.]

Under HIPAA, patients do not have a private right of action; instead, they may file a complaint with the U.S. Department of Health and Human Services, which may impose civil penalties of up to $100 per Privacy Rule violation. Civil penalties may not exceed $25,000 per calendar year for multiple violations of the same Privacy Rule requirement. [42 U.S.C. 1320d-5(a).] Penalties may not be imposed in certain cases, such as when a violation is due to a reasonable cause and not willful neglect and the entity corrected the violation within 30 days of when it knew or, by exercising reasonable diligence, would have known of the violation. [42 U.S.C. 1320d-5(b)(3).

Criminal penalties may be imposed for knowingly violating HIPAA. [42 U.S.C. 1320d-6(a).] Violators may be fined up to $50,000, imprisoned for up to one year, or both. If the wrongful conduct involves false pretenses, the criminal penalties increase to up to $100,000, up to five years in prison, or both. If the violator intended to sell, transfer, or use the health information for commercial advantage, personal gain, or malicious harm, the penalties increase to up to $250,000, up to 10 years in prison, or both. [42 U.S.C. 1320d-6(b).]

Office of HIPAA Implementation

California Law

State law establishes a separate office solely to deal with the implementation of HIPAA. [California Health and Safety Code Section 130300 et seq.] The Office of HIPAA Implementation was created in 2001 to, among other things, "assume statewide leadership, coordination, direction, and oversight responsibilities for determining which provisions of state law concerning personal medical information are preempted by HIPAA."[32] [California Health and Safety Code Section 130311.5.] The provisions creating the office become inoperative on July 1, 2010, and are repealed on January 1, 2011. [California Health and Safety Code Section 130317.]

Patient Access to Medical Records

California Law

State law gives a patient the right to request, inspect, and copy his or her records maintained by a health care provider upon payment of reasonable

[32] For additional information from the California Office of HIPAA Implementation, including HIPAA preemption analyses, see http://www.calohi.ca.gov/state/calohi/ohiHome.jsp.

clerical costs. [California Health and Safety Code Section 123110.] A patient who has been denied access to his or her records may bring an action against the health care provider. [California Health and Safety Code Section 123120.]

An adult patient has the right to include a limited 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.]

Retention of Patient Records

California Law

State law requires optometrists to retain a patient's records for a minimum of seven years from the date the patient's treatment was completed. If the patient is a minor, the optometrist must retain the patient's records for a minimum of seven years from the date the patient completed treatment and at least until the patient reaches 19 years of age. [California Business and Professions Code Section 3007.]

California law also requires licensed psychologists to retain a patient's health service records for a minimum of seven years from the date the patient is discharged. If the patient is a minor, the patient's health service records must be retained for a minimum of seven years from the date the patient reaches 18 years of age. [California Business and Professions Code Section 2919.]

Online Privacy and Related Issues

Overview

- Nationwide, consumers have grown increasingly concerned about online privacy and the protection of their personal information. In fact, 30 percent of respondents to a May 2006 poll by Wall Street Journal Online/Harris Interactive said they limit online purchases because of identity theft concerns. Another 24 percent said they limit online banking transactions.[33]

- An October 2005 Consumer Reports WebWatch survey found that nearly nine out of 10 Internet users (86 percent) have "made at least one change in their behavior because of fears about identity theft" and slightly more than half (53 percent) say "they have stopped giving out personal information on the Internet." Furthermore, 88 percent of those surveyed say that "keeping personal information safe and secure is very important for a Web site they visit."[34] In another survey, 63 percent of Americans indicated they are "very worried" and "somewhat worried" about providing personal information on Web sites.[35]

- California is one of several states that has enacted various statutes to help consumers protect their privacy online. For example, California law requires companies to conspicuously post their privacy policies on their Web sites and identify their information-collection and sharing practices. Other states impose restrictions on Web site operators that prohibit them from making false or misleading statements in their privacy policies.[36]

---

[33] Wall Street Journal Online/Harris Personal Finance Poll, "Most Americans Are Taking Steps to Prevent Identity Theft, Poll Shows," May 11, 2006.

[34] Consumer Reports WebWatch, "Leap of Faith: Using the Internet Despite the Dangers; Results of a National Survey of Internet Users for Consumer Reports WebWatch," October 26, 2005, conducted by Princeton Survey Research Associates International, http://www.consumerwebwatch.org/pdfs/princeton.pdf.

[35] Ipsos/Queen's University, "Seven Countries Ponder Online Privacy," November 19, 2006, http://www.angus-reid.com/polls/index.cfm/fuseaction/viewItem/itemID/13849.

[36] National Conference of State Legislatures, "State Laws Related to Internet Privacy," February 3, 2006, http://www.ncsl.org/programs/lis/privacy/eprivacylaws.htm.

- Some states, including California, have also prohibited the unauthorized installation of spyware on a user's computer, which allows an individual to secretly collect, monitor, and transmit the user's personal information. California and other states have also outlawed the practice of phishing (when an identity thief uses e-mail or the Internet to impersonate a legitimate company to obtain an unsuspecting consumer's personal information, account number, or password). Federal legislation has been introduced on these issues as well.

Anti-Phishing Act of 2005

California Law

State law makes it unlawful 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.]

Children's Online Privacy Protection Act

Federal Law

Federal law requires the Federal Trade Commission (FTC) to issue a privacy rule regarding the collection of personal information from a child under the age of 13 by operators of Web sites or online services directed at children. [Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501 et seq.]

In November 1999 the FTC issued the Children's Online Privacy Protection Rule, which requires operators to post a notice on their Web sites outlining what

personal information is collected and how it is used and disclosed. The rule also generally requires operators to obtain parental consent prior to collecting, using, or disclosing a child's personal information. Operators must provide parents with access to their children's personal information and the ability to (1) review the information, (2) request its deletion, and (3) opt out of future collection or use of the information. Operators may not make the disclosure of more information than is reasonably necessary a condition of a child's participation in a game or prize offering, and they must establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children. [Children's Online Privacy Protection Rule, 16 C.F.R. Part 312.]

Computer Spyware

California Law

Among other things, state law prohibits an unauthorized person or entity from causing, as specified, computer software to be copied onto another person's computer if the software, through intentionally deceptive means, modifies the user's computer settings to use or access the Internet or collects personally identifiable information. [California Business and Professions Code Section 22947.2.]

Online Privacy Policy

California Law

Under state law, commercial Web site operators and online services that collect personally identifiable information about California residents are required 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, including identifying the categories of personally identifiable information collected by the operator and the categories of third parties with whom the operator shares that information. If an operator offers

consumers a process to review and request changes to their personally identifiable information, it must provide a description of that process. The policy must also describe the process by which the operator notifies consumers of material changes to the policy and identify its effective date. [California Business and Professions Code Section 22575.]

An operator is in violation if, after being notified of noncompliance, its privacy policy is not posted within 30 days. An operator who fails to comply with these requirements or the provisions of its posted privacy policy is in violation if it does so either knowingly and willfully or negligently and materially. [California Business and Professions Code Sections 22575 and 22576.]

"Personally identifiable information" is defined as individually identifiable information about a consumer collected online by the operator from that individual and maintained by the operator in an accessible form, including name, address, e-mail address, or social security number. [California Business and Professions Code Section 22577(a).]

Posting Personal Information on the Internet

California Law

State law places restrictions on posting the personal information of certain individuals on the Internet. For example, state and local agencies are prohibited from posting the home address or telephone number of any elected or appointed official, including state constitutional officers, members of the Legislature, judges, district attorneys, public defenders, and city council members, without first obtaining the official's written permission. [California Government Code Section 6254.21.]

The law also prohibits any person from knowingly posting on the Internet the home address or telephone number of a public official or his or her residing

spouse or child with the intent to cause, or threaten to cause, imminent great bodily harm to the individual. [California Government Code Section 6254.21(b).]

Similar provisions restrict the public posting of personal information and photographic images of providers, employees, volunteers, and patients of reproductive health services facilities. [California Government Code Section 6218(a).]

State Agency Collection of Personal Information on the Internet

California Law

Under state law, state agencies are required, when electronically collecting personal information on the Internet, to indicate 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 written permission, except as specified. "Electronically collected personal information" is any information maintained by an agency that identifies or describes an individual user. [California Government Code Section 11015.5.]

Unauthorized Access to Computers, Computer Systems, and Data

California Law

State law 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.]

U.S. SAFE WEB Act

Federal Law

The federal "Undertaking Spam, Spyware, and Fraud Enforcement With Enforcers beyond Borders Act of 2006" (U.S. SAFE WEB Act of 2006) provides the Federal Trade Commission with the authority to protect consumers from unfair or deceptive acts or practices perpetrated from outside the United States. The act extends the commission's authority to include acts or practices that involve foreign commerce and "cause or are likely to cause reasonably foreseeable injury within the United States." [U.S. SAFE WEB Act of 2006, Section 3, Pub. L. 109-455.]

Wireless Network Security

California Law

Under state law, a wireless network device, which allows a consumer to connect wirelessly to an Internet service provider, must be manufactured to include one of several security measures in the product or its packaging. Such measures include a consumer warning on how to protect the wireless network connection from unauthorized access. The law applies only to devices manufactured after October 1, 2007, that are sold as new for use in a small office, home office, or residential setting. [California Business and Professions Code Sections 22948.5 and 22948.6.]

Public Records

Overview

- State law largely governs the collection, use, and disclosure of personal information contained in public records. For example, California law places restrictions on the maintenance and release of birth and death indices and records to safeguard personal information contained within those records, such as social security numbers and mothers' maiden names.

- California also imposes limitations on the collection and disclosure of personal information by state agencies and permits individuals to inspect and, if necessary, request correction of their records maintained by the agency. Federal law imposes similar restrictions on federal agencies.

- California is one of 19 states with an address-confidentiality program that allows participants to request that a substitute address be used as their address of record in public records.[37] Victims of domestic violence and stalking, as well as providers, employees, volunteers, and patients of reproductive health care facilities, may participate in the program. California recently strengthened this law by adding victims of sexual assault to the program.

- Other public records are also protected under California law. For example, court records, Department of Motor Vehicle records, and voter records all receive some protections. Social security numbers contained in certain public records are protected as well. See "Social Security Numbers" on page 121 for more details.

[37] National Conference of State Legislatures, "States With Address Confidentiality Programs for Domestic Violence Survivors," http://www.ncsl.org/programs/cyf/dvsurvive.htm.

Birth and Death Record Indices

California Law

Under state law, the state registrar must 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, except as necessary for official government business, 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; and
3. Noncomprehensive birth and death indices containing the mother's maiden name and social security numbers, as specified, must be made available for purposes of 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(a)-(c).]

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(b)(4).]

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

The above-described provisions are to be implemented only to the extent that funds are appropriated by the Legislature.[38] [California Health and Safety Code Sections 102230(i) and 102231(g).]

---

[38] The California Department of Public Health's Center for Health Statistics, Office of Health Information and Research, indicates that it currently produces and maintains the three types of indices specified in Health and Safety Code Section 102230. Only governmental agencies and fraud-prevention organizations may obtain confidential versions of the indices; the public may obtain nonconfidential indices.

Violation of the restrictions relating to birth and death record indices is a misdemeanor. [California Health and Safety Code Section 102232.]

Birth and Death Records: Confidential Information

California Law

State law 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 the medical and social information contained in the second section of a birth certificate—such as birth weight, pregnancy history, and race and ethnicity of the mother and father—confidential, and 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 Sections 102425, 102430, and 103025.]

Birth and Death Records: Release of Records

California Law

State law controls the access to and release of 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." Informational certified copies may only be printed from the state registrar's single statewide database and signatures must be electronically redacted. This requirement becomes operative on July 1, 2007, but only after the statewide database becomes operational.[39] [California Health and Safety Code Section 103526.]

Court Records: Personal Information of Victims and Witnesses

California Law

State law protects confidential personal information that relates to a witness or victim contained in a police, arrest, or investigative report. "Confidential personal information" is defined to include, among other things, address, telephone number, driver's license number, social security number, and date of birth. [California Penal Code Section 964.]

Court Records: Sealing Information Regarding Financial Assets and Liabilities

California Law

Under state law, a party to a dissolution of marriage, an annulment, or a legal separation may request that the court seal from public view information

[39] The California Department of Public Health's Center for Health Statistics, Office of Vital Records, indicates that the "Informational, Not A Valid Document To Establish Identity" statement is currently included on all copies issued to those who are not authorized to receive a regular certified copy. For additional information, see http://www.cdph.ca.gov/certlic/birthdeathmar/Pages/default.aspx.

concerning the party's financial assets and liabilities. [California Family Code Section 2024.6.]

Department of Motor Vehicles' Records

California Law

State law prohibits the Department of Motor Vehicles from disclosing personal information about a person unless the disclosure is in compliance with the federal Driver's Privacy Protection Act of 1994 (this act is described in more detail on page 110). [California Vehicle Code Section 1808(e).] Existing law also 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 Sections 1808.21 and 1808.22.]

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 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.] 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 also 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 or information pertaining to the driver's physical characteristics is prohibited. [California Vehicle Code Section 12800.5.]

Driver's License Information: "Swiping" Licenses

California Law

Under state law, businesses may "swipe" 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

Federal Law

Federal law prohibits a state's Department of Motor Vehicles and its employees from knowingly disclosing, or otherwise making available, 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. Federal law imposes criminal penalties for certain violations, and a driver may bring a civil action against a person who knowingly obtains, discloses, or uses personal information from the driver's motor vehicle record for an impermissible purpose. [Driver's Privacy Protection Act of 1994, 18 U.S.C. 2721 et seq.]

Information Practices Act of 1977

California Law

California's Information Practices Act of 1977 imposes limitations on the collection and disclosure of personal information by state agencies. The act declares that the right to privacy is a personal and fundamental right protected by both the California and U.S. Constitutions and that all individuals have a right of privacy regarding information about them. [California Civil Code Section 1798 et seq.]

The act defines "personal information" as any information maintained by an agency that identifies or describes an individual, including name, social security number, physical description, home address, home telephone number, financial matters, and medical and employment history. Personal information also includes statements made by, or attributed to, the individual. [California Civil Code Section 1798.3(a).]

The Information Practices Act requires, among other things, that state agencies maintain in their records only personal information relevant and necessary to accomplish an authorized purpose. [California Civil Code Section 1798.14.] State agencies also must permit individuals to inspect and, if necessary, request correction of their records maintained by the agency. [California Civil Code Sections 1798.34 and 1798.35.]

Under state law, an agency may not disclose any personal information in a manner that would link the information to the individual it pertains to 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, (4) pursuant to a subpoena or 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 the individual's behalf. [California Civil Code Section 1798.24.]

Marriage License Information

California Law

Under state law, a marriage license applicant, or a witness to a marriage, may request that the marriage certificate or license show the business address or a post office box number for that applicant or witness instead of the person's residential address. [California Family Code Section 351.5.]

Privacy Act of 1974

Federal Law

The federal Privacy Act regulates the collection, maintenance, use, and disclosure of personal information by federal executive branch agencies. Individuals are granted some limited rights to access their personal information and request a correction if necessary. [5 U.S.C. 552a.]

Public Records: Address Confidentiality

California Law

State law provides that certain individuals may request a substitute address, designated by the secretary of state, to be used as their address of record in public records. State and local agencies must use this alternate address when creating, modifying, or maintaining public records, except as specified. The programs apply to victims of domestic violence, stalking, and sexual assault,

as well as providers, employees, volunteers, and patients of reproductive health care facilities. These provisions sunset on January 1, 2013. [California Government Code Sections 6205 et seq. and 6215 et seq.]

Public Records Act

California Law

California's Public Records Act provides that public records are open to inspection, unless exempt. [California Government Code Section 6250 et seq.] The act may not be construed to require the disclosure of various records, including (1) personnel, medical, or similar files if the disclosure would constitute an unwarranted invasion of personal privacy, (2) records pertaining to pending litigation that the public agency is a party to, until the pending litigation or claim has been finally adjudicated or otherwise settled, and (3) records in which disclosure is exempted or prohibited pursuant to state or federal law. [California Government Code Section 6254.]

Some information contained in certain public records—social security numbers, for example—is exempt from disclosure under the Public Records Act. See "Social Security Numbers" on page 121 for more details.

In November 2004, Proposition 59 amended the California Constitution to grant Californians the right of public access to meetings of government bodies and writings of government officials and agencies. Statutes furthering public access must be interpreted broadly, and, if they limit access, 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 I, Section 3.]

The California Supreme Court ruled in August 2007 that the names, salaries, hiring dates, and termination dates of certain public employees must be disclosed under the Public Records Act, although information concerning particular employees—in this case, peace officers—may be exempt from disclosure if the safety of the officers would be threatened. [*Commission on Peace Officer Standards and Training v. Superior Court* (2007) 42 Cal. 4th 278; *International Federation of Professional and Technical Engineers, Local 21, AFL-CIO v. Superior Court*, (2007) 42 Cal. 4th 319.]

State Agencies: Mailing Personal Information

California Law

State law prohibits state agencies from sending U.S. mail to an individual that contains personal information about that individual unless the information is sealed and cannot be viewed from the outside of the envelope. Personal information includes, but is not limited to, the individual's social security number, telephone number, driver's license number, and credit card account number. This restriction also applies to correspondence sent via a common carrier, such as an express delivery or courier service. A "state agency" in this instance includes the California State University. [California Government Code Section 11019.7.]

State Agencies' Privacy Policies

California Law

State law 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. Any subsequent use of the information must not be inconsistent with these identified purposes. [California Government Code Section 11019.9.]

State Agency Databases: Researcher Access

California Law

Under state law, state agencies may 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

California Law

State law requires that specified information regarding the permissible use of voter information must 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.]

The following information contained on voter registration cards is confidential: (1) home address, (2) telephone number, (3) e-mail address, (4) precinct number, and (5) prior registration information. [California Government Code Section 6254.4(a) and Elections Code Section 2194(a)(1).]

Under state law, the above-described information must be provided to any candidate for federal, state, or local office; any committee for or against an initiative or referendum measure; and any person for election, scholarly, journalistic, or political purposes; or for governmental purposes, as determined by the secretary of state. [California Elections Code Section 2194(a)(3).]

State law provides that a voter's driver's license number, identification card number, and social security number are confidential and may not be disclosed to any person. The signature of a voter shown on a voter registration card is confidential as well and may not be disclosed to any person unless a person's vote is challenged. [California Elections Code Section 2194(b)-(c).]

A recently enacted state law provides that certain information on a voter registration card—the applicant's driver's license number, identification card number, and social security number—is confidential and may not be disclosed by an individual or organization that distributes voter registration cards. [California Elections Code Section 2138.5.]

Additionally, certain individuals may request that their residence address, telephone number, and e-mail address contained on a voter registration card be kept confidential. For example, victims of domestic violence, stalking, and sexual assault, as well as providers, employees, volunteers, and patients of reproductive health care facilities who participate in the secretary of state's address-confidentiality program described under "Public Records: Address Confidentiality" on page 112, may request confidentiality. This provision sunsets on January 1, 2013. [California Elections Code Section 2166.5.]

Public safety officers may request similar confidentiality and the county elections official must comply, if authorized by the county board of supervisors. The confidentiality terminates two years after commencement and may be renewed. [California Elections Code Section 2166.7.]

Voter Information: Outsourcing

California Law

State law 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 specified. [California Elections Code Section 2188.5.]

Social Security Numbers

Overview

- Although originally created to track workers' earnings and eligibility for social security programs,[40] social security numbers are now used for many purposes wholly unrelated to the social security system. The identification number has been called the most frequently used recordkeeping number in the United States.

- Because a social security number is unique to each individual to whom it is assigned, it is often used to verify identity. But in the wrong hands a social security number can be used by an identity thief to assume another person's identity, access his or her bank account, or establish new credit or utility accounts in that person's name, among other things. The social security number—along with a name and birth date—is one of the "three pieces of information most often sought by identity thieves."[41]

- California is one of several states that has taken legislative action to protect against the misuse of individuals' social security numbers. After California enacted its statute restricting the public display of social security numbers, at least 13 other states adopted similar measures.[42]

- Provisions in federal laws also restrict disclosure of an individual's social security number. For example, the Fair Credit Reporting Act requires consumer reporting agencies to, upon request, truncate a consumer's social security number when the consumer requests a copy of his or her credit report.

---

[40] General Accounting Office, "Social Security Numbers: Federal and State Laws Restrict Use of SSNs, Yet Gaps Remain," September 15, 2005, http://www.gao.gov/new.items/d051016t.pdf.
[41] Id., p. 3.
[42] General Accounting Office, "Social Security Numbers: More Could Be Done to Protect SSNs," March 30, 2006, http://www.gao.gov/new.items/d06586t.pdf.

- Nevertheless, despite these and other protections, the General Accounting Office concluded in a March 2006 report that "more could be done" to protect social security numbers.[43] It found that social security numbers are widely available in public records held by states and local governments and are most often found in court and property records.[44] The report also noted the lack of restrictions placed on "information resellers" who "resell" social security numbers in the course of their business.[45]

- In response to concerns about the widespread availability of social security numbers in court and county recorders' records, California enacted two measures in 2007 restricting the display of social security numbers in publicly available records.

Confidentiality

California Law

State law places restrictions on the use of social security numbers and prohibits the following:

1. Publicly 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

---

[43] General Accounting Office, "Social Security Numbers: More Could Be Done to Protect SSNs."
[44] Id., p. 6., Also see General Accounting Office, "Social Security Numbers: Governments Could Do More to Reduce Display in Public Records and on Identity Cards," November 2004, http://www.gao.gov/new.items/d0559.pdf.
[45] General Accounting Office, "Social Security Numbers: More Could Be Done to Protect SSNs," p. 14.

5. Printing an individual's social security number on any materials mailed to him or her unless required by state or federal law. [California Civil Code Section 1798.85(a).]

This state law does not prevent the use of a social security number for internal verification or administrative purposes and does not apply to documents required to be open to the public. It prohibits any person or entity from encoding or embedding a social security number in a barcode, chip, magnetic strip, or other technology, instead of removing the social security number as required. [California Civil Code Section 1798.85.]

County Recorders' Records

California Law

State law, enacted in 2007, requires county recorders to establish a Social Security Number Truncation Program. Under the program, county recorders must create public-record versions of official records dating back to January 1, 1980, by truncating any social security number contained in the records so only the last four digits are displayed. [California Government Code Sections 27300 and 27301.] The statute contains provisions regarding implementation of the program for records recorded between January 1, 1980, and December 31, 2008, and records recorded on or after January 1, 2009. [California Government Code Section 27301.]

Once a public version is created, the county recorder may only disclose the original version in response to a subpoena or court order. Otherwise, the county recorder may only release the public-record version. [California Government Code Section 27303.] The original record is exempt from disclosure under the California Public Records Act if a "public record" version is available. [California Government Code Section 6254.27.]

A county recorder is deemed to be in compliance with these truncation requirements and is not 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 them in the public-record version. Using an automated program with a high rate of accuracy is deemed to be due diligence. [California Government Code Section 27302(a).] If a county recorder fails to truncate a social security number, any person may request that the number be truncated and—if the request identifies the exact location of the untruncated social security number—the county recorder must comply with that request within 10 business days. [California Government Code Section 27302(b).]

Unless otherwise required by state or federal law, no person, entity, or government agency may present—for recording or filing with a county recorder's office—a document containing more than the last four digits of a social security number if that document is required to be open to the public. [California Civil Code Section 1798.89.]

Court Records

California Law

A state law enacted in 2007 eliminated the requirement that an individual's full social security number must be provided on a tax lien filing or an abstract of judgment requiring the payment of money. Instead, only the last four digits of the social security number are required. [California Code of Civil Procedure Section 674 and Revenue and Taxation Code Section 2191.3.]

Drivers' Licenses

California Law

State law requires a driver's license applicant to include his or her social security number (or other appropriate number) on the application. The social

security number, however, may not be included on a magnetic tape or strip used to store data on the license. [California Vehicle Code Section 12801.]

Employee Compensation

California Law

Under state law, by January 1, 2008, all employers may only use 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(a).]

Family Court Records

California Law

State law 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 the collection of child or spousal support. [California Family Code Section 2024.5.]

Franchise Tax Board Liens

California Law

A 2007 state law requires the Franchise Tax Board—before disclosing records to the public—to truncate social security numbers (by redacting the first five digits) on lien abstracts and any other records created by the board that are disclosable under the California Public Records Act. This requirement applies unless the truncation is prohibited by federal law. [California Government Code Section 15705.]

Local Agencies' Records

California Law

State law, enacted in 2007, expresses the intent of the Legislature that, to protect against the risk of identity theft, local agencies shall redact social security numbers from records before disclosing them to the public under the California Public Records Act. The law also exempts social security numbers from the information required to be disclosed by local agencies under the Public Records Act. These provisions do not apply to records maintained by county recorders, who are covered under a separate section of the law (see "County Recorders' Records" on page 123). [California Government Code Section 6254.29.]

Powers of Attorney

California Law

A recent state law deleted the line on the statutory power-of-attorney form that required a social security number and added a notice on the form stating that a third party may require additional identification. [California Probate Code Section 4401.]

Secretary of State Filings

California Law

State law, enacted in 2007, requires the secretary of state and other filing offices to create a public version of an official filing that contains only a truncated social security number. Once a public-filing version is created, the filing office may only release the public-filing version; the filing office may only disclose the official filing in response to a subpoena or court order. [California

Commercial Code Section 9526.5.] The official filing is exempt from disclosure under the California Public Records Act if a "public filing" version is available. [California Government Code Section 6254.28.]

A filing office is deemed to be in compliance with these truncation requirements and is not liable for failure to truncate a social security number if it uses due diligence to locate social security numbers in official filings and truncate them in the public filing. Using an automated program with a high rate of accuracy is deemed to be due diligence. [California Commercial Code Section 9526.5(f).] If a filing office fails to truncate a social security number, any person may request that the number be truncated and—if the request identifies the exact location of the untruncated social security number—the filing office must comply with that request within 10 business days. [California Commercial Code Section 9526.5(g).]

Filing offices are required to post a notice on their Web site informing filers not to include social security numbers in their filings, and a filing office's online system may not contain a field requesting a social security number. [California Commercial Code Section 9526.5(c).] The secretary of state is also required to produce and make available financing statements that do not provide a space for a social security number; producing or making available forms that include a space for the social security number is prohibited. [California Commercial Code Section 9526.5(h) and (i).]

These provisions do not apply to county recorders who are covered under a separate section of the law (see "County Recorders' Records" on page 123).

Use by Colleges and Universities

California Law

A 2007 state law requires the Office of Privacy Protection to establish a task force to review the use of social security numbers by colleges and universities and recommend practices for minimizing the collection, use, storage, and retention of social security numbers. The task force must submit a report on its findings to the Legislature by July 1, 2010. [California Education Code Section 66018.55.]

Use in Credit Reports

Federal Law

Federal law requires 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.]

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

Other Key Statutes

Overview

- There are a variety of other significant statutes relating to consumer privacy and identity theft and California has been at the forefront of many of these issues. For example, in 2000 California became the first state to establish an Office of Privacy Protection charged with protecting the privacy of individuals' personal information.[46] In 2007 the Office of Privacy Protection was transferred to the new Office of Information Security and Privacy Protection, an agency-level office created to ensure the confidentiality and integrity of state systems and promote and protect consumer privacy.

- In 2004 California became the first state to enact a law requiring automobile manufacturers to notify consumers if "event data recorders" (commonly known as "black boxes") are installed in vehicles.[47] And California is one of two states to impose restrictions on a rental car company's ability to use electronic surveillance technology or a Global Positioning System (GPS) to track a renter for the purpose of imposing fines or surcharges.[48]

- Recently enacted laws in California and at the federal level restrict a type of "pretexting" in which individuals use deceptive methods to obtain consumers' telephone records. Both laws impose criminal penalties for the fraudulent acquisition of confidential phone records. Federal law also prohibits pretexting to obtain a customer's financial information.

---

[46] For additional information on the Office of Information Security and Privacy Protection, see http://www.privacy.ca.gov.

[47] National Conference of State Legislatures, "2006 Privacy Legislation Related to Event Data Recorders ("Black Boxes") in Vehicles," October 2006, http://www.ncsl.org/programs/lis/privacy/blackbox06.htm.

[48] Id.

- California joined several other states in 2007 when it enacted a law prohibiting any person from forcing another to be implanted with an identification device that transmits personal information using such technology as radio frequency identification (RFID).

Criminal Investigation Information

California Law

State law makes it unlawful for a peace officer, law enforcement employee, attorney, or trial court employee to disclose or solicit—for financial gain—any information obtained in the course of a criminal investigation if disclosure of the information is prohibited by law. [California Penal Code Section 146g.]

Eavesdropping on Confidential Communications

California Law

State law 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

Federal Law

The federal Electronic Communications Privacy Act of 1986 prohibits an individual from intentionally intercepting any wire, oral, or electronic communication. Specified oral communications are exempt from this prohibition. There also are several exceptions to the prohibition, including intercepts where one of the parties to the communication consents. [Electronic Communications Privacy Act of 1986, 18 U.S.C. 2511.]

Electronic Surveillance Technology: Rental Cars

California Law

State law prohibits a rental car company from using, accessing, or obtaining 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, including 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 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

California Law

State law makes it unlawful to use an electronic tracking device attached to a vehicle or other movable thing 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.]

Identification Devices: Forced Human Implants

California Law

State law prohibits any person from requiring, coercing, or compelling another individual to undergo the implantation on or under the skin of an identification device that transmits personal information using such technology as radio frequency identification (RFID). Violators are subject to civil penalties, and any person who is unlawfully implanted with a device may bring an action to recover damages. [California Civil Code Section 52.7.]

Office of Information Security and Privacy Protection

California Law

State law, enacted in 2007, provides for the Office of Information Security and Privacy Protection in the State and Consumer Services Agency to ensure the confidentiality, integrity, and availability of state systems and promote and protect consumer privacy. [California Government Code Section 11549.] The

office must establish an information security program that creates, updates, and publishes policies, standards, and procedures for state agencies regarding information security, privacy, and incident notification. Every state agency, department, and office is required to comply with these policies, standards, and procedures. [California Government Code Section 11549.3.]

This newly enacted statute transferred the Office of Privacy Protection—which was created in 2000—and all of its responsibilities from the Department of Consumer Affairs to the new Office of Information Security and Privacy Protection. [California Government Code Sections 11549.2 and 11549.5.]

The statutory purpose of the Office of Privacy Protection 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 in adherence with the Information Practices Act." The office is required to inform consumers about ways to protect 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. Where appropriate, the office is authorized to promote voluntary and mutually agreed-upon nonbinding arbitration and mediation of privacy-related disputes. [California Government Code Section 11549.5.]

Personal Information: Domestic Violence, Sexual Assault, and Stalking

California Law

State law prohibits any person or entity, in the course of awarding grants, from requesting or requiring that a victim-service provider—such as a rape

crisis center or domestic violence shelter—supply personally identifying information regarding any individuals to whom it is providing, has provided, or may provide services. This provision applies to victim-service providers who provide services to victims of domestic violence, dating violence, sexual assault, or stalking and the children of such victims. [California Civil Code Section 1798.79.9.]

"Personally identifiable information" includes an individual's first and last name or last name only, home address, e-mail address, telephone number, social security number, date of birth, Internet protocol address or host name that identifies an individual, and any other information that, in combination with other nonpersonally identifying information, would identify the individual. [California Civil Code Section 1798.79.8.]

Personal Information: Inmate Access

California Law

Under state law, the secretary of the Department of Corrections and Rehabilitation may not assign a prison inmate to employment that provides the inmate with access to the personal information of private individuals. Personal information includes, among other things, addresses, telephone numbers, social security numbers, mothers' maiden names, credit card numbers, or checking account numbers. [California Penal Code Section 5071(a).]

Similar restrictions apply to any person confined in a county jail, industrial farm, road camp, or city jail and any person performing community service in lieu of a fine or custody or who is assigned to work furlough. [California Penal Code Section 4017.1(a).]

Pretexting

California Law

State law addresses one kind of "pretexting" in which individuals use deceptive methods to obtain consumers' telephone records. Existing law makes it unlawful to purchase, sell, offer to purchase or sell, or conspire to purchase or sell a record or list of a subscriber's telephone calling patterns without his or her written consent. It is also unlawful for any person to procure or obtain through fraud or deceit a subscriber's telephone calling pattern record or list. [California Penal Code Section 638(a).]

In February 2007 the California Supreme Court also considered another type of pretexting in which an academic researcher was alleged to have misrepresented her position to obtain sensitive personal information. In this case, the court held that the researcher could be held liable in an invasion-of-privacy lawsuit for improperly intruding into private matters. [*Taus v. Loftus* (2007) 40 Cal. 4th 683.]

Federal Law

Federal law also addresses the use of pretexting to obtain consumers' telephone records under the "Telephone Records and Privacy Protection Act of 2006." This recently enacted federal law provides for criminal penalties for the fraudulent acquisition of confidential phone records. The law also restricts the sale, transfer, and purchase of a customer's confidential phone records without his or her prior authorization or with the knowledge that the information was obtained fraudulently. These provisions apply only to violations that occur in interstate or foreign commerce. [Telephone Records and Privacy Protection Act of 2006, Pub. L. 109-476.]

Federal law also restricts pretexting with respect to financial information. The Gramm–Leach–Bliley Act (GLB) prohibits obtaining a customer's financial

information by making false, fictitious, or fraudulent statements to a financial institution's employees. It is also unlawful to obtain a customer's financial information by providing a document to a financial institution knowing that it is forged, counterfeit, lost, stolen, was fraudulently obtained, or contains a false, fictitious, or fraudulent statement or representation. [15 U.S.C. 6821(a).] The statute contains various exceptions; for example, its provisions do not apply to a law enforcement agency performing its official duties or a licensed private investigator collecting court-ordered child support. [15 U.S.C. 6821(c) and (g).]

GLB imposes criminal penalties for knowing and intentional violations. [15 U.S.C. 6823.] The act also provides that states may grant consumers greater protections than those provided by federal law. [15 U.S.C. 6824.]

Real ID Act of 2005

Federal Law

The federal Real ID Act of 2005 provides that, unless a state meets specified requirements, a federal agency may not accept a driver's license or identification card issued by the state for an "official purpose," such as entering a federal building or boarding a commercial airplane. [Real ID Act of 2005, Pub. L. 109-13, 119 Stat. 231.] Such requirements relate to the information contained on state drivers' licenses and identification cards and the minimum standards for issuance of those documents. [Real ID Act Section 202.]

In March 2007 the Department of Homeland Security (DHS) issued proposed regulations implementing the requirements of Real ID.[49] The proposed rule interprets Real ID to provide that, effective May 11, 2008, federal officials may

---

[49] Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes, 72 Fed. Reg. 10820 (2007) (to be codified at 6 C.F.R. Part 37). Public comments on the proposed rule were due May 8, 2007. At press time, a final rule had not yet been issued although Department of Homeland Security officials have indicated that the final rule is expected by the end of 2007 or early 2008. [*Federal Computer Week*, "Real ID Standards Expected in Two to Three Months, Says DHS Official," October 17, 2007, http://www.fcw.com/online/news/150547-1.html.]

not accept state-issued drivers' licenses or identification cards for an official purpose unless the state has submitted the required certification or extension application (lasting until December 31, 2009) to DHS and DHS has determined that the state is meeting the requirements of Real ID. DHS will certify a state under this section if the state has established a program that ensures the state will begin issuing Real ID-compliant licenses and identification cards beginning May 11, 2008.

Under the proposed rule, states will have a five-year phase-in period in which to replace noncompliant licenses and identification cards: all drivers' licenses and identification cards must be Real ID-compliant by May 11, 2013, or they will not be accepted by federal agencies for an official purpose.[50]

With respect to the information contained on state drivers' licenses and identification cards, the act requires the documents to meet certain minimum requirements, including that the license or card contain, among other things, (1) the person's full legal name, date of birth, and gender, (2) a digital photograph of the person, (3) physical security features designed to prevent tampering, counterfeiting, or duplication of the document for fraudulent purposes, and (4) a common machine-readable technology, with defined minimum data elements. [Real ID Act Section 202(b).]

In its consideration of the proposed rule, DHS reviewed several types of machine-readable technology and determined the 2D bar code as the best option (DHS rejected optical stripes, contact integrated circuit chips, integrated contactless chips, e.g., using RFID, and the 1D bar code).[51] As a result, the proposed rule requires states to use the "PDF417 2D bar code" standard with the following defined minimum data elements, which must be included in the bar code: (1) expiration date, (2) holder's name, including full legal name and all name changes, (3) issue date, (4) date of birth, (5) gender, (6) address, (7) unique identification number, (8) revision date, and (9) inventory control number of the physical document.[52]

---

[50] 72 Fed. Reg. at 10822, 10824, 10851.
[51] 72 Fed. Reg. at 10837.
[52] 72 Fed. Reg. at 10854.

Real ID also imposes requirements for the issuance of drivers' licenses and identification cards, such as the minimum information an individual must present before a state may issue him or her a license or identification card. [Real ID Act Section 202(c)(1).] Such "identity source" information includes proof of birth date, principal residence, and social security number or verification that the person is not eligible for a social security number. [Real ID Act Section 202(c)(1)(A)-(D).] States also must verify the issuance, validity, and completeness of this information. [Real ID Act Section 202(c)(3).] The proposed rule provides that states must require applicants to submit at least one of several listed documents, such as a valid, unexpired U.S. passport, certified copy of a birth certificate, consular report of birth abroad, or a U.S. certificate of citizenship or naturalization.[53]

A state must use technology to capture digital images of "identity source documents" and retain paper copies of these documents for at least seven years or digital images for at least 10 years. [Real ID Act Section 202(d)(1) and (2).]

For its drivers' licenses and identification cards to be accepted by a federal agency for an official purpose, a state must provide all other states with electronic access to information contained in the state's motor vehicle database. [Real ID Act Section 202(d)(12).] This database must contain all data fields printed on drivers' licenses and identification cards and drivers' histories, including motor vehicle violations, suspensions, and points on licenses. [Real ID Act Section 202(d)(13).]

[53] 72 Fed. Reg. at 10827, 10851.

Student Records

California Law

California law addresses the confidentiality of student records. [California Education Code Section 49060 et seq.] The statute gives parents of students currently or formerly enrolled in elementary or secondary schools the right to access their children's student records maintained by the school district or private school. [California Education Code Section 49069.] Parents may also request the correction of information contained in a record, as specified. [California Education Code Section 49070.] State law generally restricts access to student records without written parental consent or a court order, except as specified. [California Education Code Sections 49075 and 49076.]

Federal Law

Under the federal Family Educational Rights and Privacy Act of 1974 (FERPA), parents are granted certain privacy rights regarding their children's education records. For example, parents may inspect and review their children's education records maintained by the school and request correction of any inaccuracies contained within the records. In general, schools may not release any information from a student's education record without parental consent, except as specified. These rights are transferred from the parents to the student when the student reaches 18 years of age or is attending an institution of postsecondary education. FERPA applies to all schools that receive federal funding from the U.S. Department of Education; federal funds are denied to schools that do not comply with FERPA. [Family Educational Rights and Privacy Act of 1974, 20 U.S.C. 1232g.]

Taxpayer Information

California Law

State law 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 as specified, (2) the disclosure is expressly authorized by state or federal law or is necessary to prepare a return, or (3) the disclosure is pursuant to a court order. [California Business and Professions Code Section 17530.5(a).]

Unfair Competition Law

California Law

State 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 county counsel, 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 a separate cause of action, and the unfair competition law has therefore been used as a means for consumers to obtain relief for violations. A statute that declares a particular act or type of practice unlawful, but does not contain its own independent cause of action, may be independently actionable under the unfair competition law. [13 Witkin, Summary of Cal. Law (10th ed.) Equity, Section 107.]

Vehicle Event Data Recorders

California Law

State law 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. Such devices retrieve data after an accident, including the vehicle's speed, braking performance, and whether the driver was wearing a seatbelt. 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 Image Evidence: Parking Enforcement

California Law

A 2007 state law permits the City and County of San Francisco to install automated devices on city-owned public transit vehicles to capture video images of parking violations occurring in transit-only traffic lanes. The parking control devices must face forward and be angled and focused to capture video images of parking violations—they may not unnecessarily capture identifying images of other drivers, vehicles, or pedestrians. [California Vehicle Code Section 40240(a).]

Citations may be issued based on the video images; in this case, video-image evidence may be retained for up to six months from the date the information was first obtained or 60 days after final disposition of the citation, whichever is later. After that time the images must be destroyed. [California Vehicle Code

Section 40240(c) and (e)(1).] Video images that do not contain evidence of a parking violation must be destroyed within 15 days after the information was first obtained. [California Vehicle Code Section 40240(e)(2).]

State law provides that these video images are confidential, and public agencies may use and allow access to the images only for authorized purposes. [California Vehicle Code Section 40240(f).] These provisions of law sunset on January 1, 2012. [California Vehicle Code Section 40243.]

Video Sale or Rental

California Law

State law prohibits any person who provides video-cassette sales or rental services from disclosing personal information (including sales or rental information) to another person without the written consent of the individual to whom the information pertains, except in specified instances. [California Civil Code Section 1799.3.]

Federal Law

The federal Video Privacy Protection Act of 1998 provides that any business engaged in the interstate 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 (an "opt out"), and (2) the disclosure does not identify the title, description, or subject matter of the video tapes. The subject matter may be disclosed, however, 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.]

Index

birth and death records
confidential information 107
indices 106
release of records 107

breach notification 46

California Community Colleges
marketing on college campuses 76

California State University
marketing of alumni personal information 74
marketing on college campuses 76

CAN-SPAM 79

cell phone directory 73

children
foster care youth, request for credit report 68
marketing 75
online privacy 98
school records 141

Children's Online Privacy Protection Act 98

Confidentiality of Medical Information Act (CMIA) 86

constitutional right to privacy 12

constructive invasion of privacy 14

county recorders' records
social security numbers 123

court records
family court, social security numbers 125
personal information of victims and witnesses 108
sealing information regarding financial assets and liabilities 108
social security numbers 124

credit cards
activation process required for substitute credit cards 21
change of address and credit card requests 22
credit card numbers printed on receipts 24

disclosure of minimum payment amount 25
fraudulent use of information on credit cards ("skimming") 26
marketing on college campuses 76
preprinted checks, disclosures 26
recording credit card numbers on checks 27
recording personal information on credit card transaction forms 27
solicitations 73
verification of credit applicant's address 27

credit reporting
California Consumer Credit Reporting Agencies Act 34
foster care youth, request for credit report 68
identity theft victim, right to free credit reports 63
investigative consumer reporting agencies 37
security alerts 38
security freezes 40
use of social security numbers in credit reports 128

criminal investigation
disclosure of information 132

data security
destruction of business and medical records 44
notification of breach in data security 46
reasonable security procedures 47

debit cards
debit card numbers printed on receipts 24
fraudulent use of information on debit cards ("skimming") 26

debt collection 52

Department of Motor Vehicles
home address information 109
Real ID Act of 2005 138
records 109, 110

destruction of business and medical records 44

"Do Not Call" Registry 78

driver's license information
Department of Motor Vehicles' records 109, 110
Real ID Act of 2005 138

social security numbers 124
"swiping" licenses 110

Driver's Privacy Protection Act of 1994 110

eavesdropping 132

Electronic Communications Privacy Act of 1986 133

electronic surveillance technology
rental cars 133

electronic tracking devices
vehicles 134

Fair Credit Reporting Act
affiliate marketing 72
change of address and credit card requests 22
credit card or debit card numbers printed on receipts 24
credit reporting 34
destruction of business records 44
identity theft victim, records of fraudulent transactions or accounts 66
identity theft victim, right to free credit reports 63
preemption 16, 22, 24, 27, 38, 44, 53, 63, 66, 128
security alerts 38
social security numbers in credit reports 128
verification of credit applicant's address 27

Fair Debt Collection Practices Act 52

Family Educational Rights and Privacy Act of 1974 (FERPA) 141

federal agencies
personal information 112

financial information
disclosure 53

financial privacy
account numbers 52
privacy of financial information 53

forced human implants
identification devices 134

Franchise Tax Board
social security numbers 125

Health Insurance Portability and Accountability Act (HIPAA) 86, 92

identification devices
forced human implants 134

identity theft
crime of 60
debt collection 61
deceptive identification documents 61
Department of Justice identity theft victim database 62
falsely obtaining Department of Motor Vehicles' documents 62
foster care youth, request for credit report 68
judicial determination of innocence 64
jurisdiction for prosecuting identity theft 64
law enforcement investigation 65
right to bring legal action against a creditor 65
right to obtain records 66
search warrants 64
security alerts 38
security freezes 40
statute of limitations 67
victim's right to free credit reports 63

Information Practices Act of 1977 111

inmate access to personal information 136

insurance information
disclosure 55, 56

Insurance Information and Privacy Protection Act 55

insurers
genetic testing 56

Internet
children 98
phishing 98
posting personal information 100
state agency collection of personal information 101
wireless network security 102

invasion of privacy
common law tort 14
penal code 15
pretexting 137

investigative consumer reporting agencies 37

marketing
affiliate marketing 72
alumni personal information 74
cell phone directory 73
children 75
college campuses 76
credit card solicitations 73
medical information 73, 86
personal information, disclosure to direct marketers 75
satellite and cable television subscribers 76
spam (unsolicited commercial e-mail messages) 79
supermarket club cards 77
telemarketing, "Do Not Call" Registry 78
Telephone Consumer Protection Act of 1991 79
telephone subscriber information 77
unsolicited text messages 81

marriage license information 112

medical privacy
destruction of medical records 44
disclosure of medical information 86
medical information, marketing 73
Office of HIPAA Implementation 92
patient access to medical records 92
retention of patient records 93

Office of Information Security and Privacy Protection 134

Office of Privacy Protection (see Office of Information Security and Privacy Protection)

online privacy
children 98
privacy policy 99

patient access to medical records 92

phishing 98

preemption 16, 22, 24, 25, 26, 27, 38, 44, 53, 63, 66, 79, 86, 92, 128

pretexting 137

Privacy Act of 1974 112

public records
address confidentiality, victims of domestic violence, stalking and sexual assault 112
birth and death record indices 106
birth and death records 107
county recorders' records, social security numbers 123
court records 108
court records, social security numbers 124
Department of Motor Vehicles' records 109, 110
family court records, social security numbers 125
Franchise Tax Board, social security numbers 125
Information Practices Act of 1977 111
local agencies, social security numbers 126
marriage license information 112
Privacy Act of 1974 112
Public Records Act 113
secretary of state, social security numbers 126
state agency databases, researcher access 115
voter information 115

Public Records Act 113

Real ID Act of 2005 138

retention of patient medical records 93

Rosenthal Fair Debt Collection Practices Act 52

San Francisco, city and county of
video image evidence 143

satellite and cable television subscriber information 76

secretary of state
social security numbers 126

social security numbers
confidentiality 122
county recorders' records 123
court records 124
driver's license information 124
employee compensation 125
family court records 125
Franchise Tax Board 125
local agencies' records 126
power of attorney form 126
secretary of state filings 126
truncation 123, 124, 125, 126, 128
use by colleges and universities 128
use in credit reports 128

spam
unsolicited commercial e-mail messages (spam) 79
U.S. SAFE WEB Act 102

spyware
spyware 99
U.S. SAFE WEB Act 102

state agencies
collection of personal information on the Internet 101
databases, researcher access 115
mailing personal information 114
Office of Information Security and Privacy Protection 134
personal information 111
privacy policies 114

supermarket club cards 77

taxpayer information 142

telemarketing 78

telephone records
pretexting 137
residential subscriber information 77

telephone subscriber information 77

unauthorized access to computers, computer systems, and data ... 101

Unfair Competition Law 142

University of California
marketing of alumni personal information 74
marketing on college campuses 76

unsolicited text messages 81

vehicle event data recorders 143

victims of domestic violence, sexual assault, and stalking
victim-service providers, personal information 135
address confidentiality 112

video image evidence
parking enforcement 143

Video Privacy Protection Act of 1998 144

video sale or rental
personal information 144

voter information
outsourcing 117
personal information 115

wireless network security 102

California Senate Office of Research

Established in 1969 by the Senate Rules Committee, the California Senate Office of Research is a nonpartisan office charged with serving the research needs of the California State Senate and helping with the development of policy for Senate members and committees. For more information and copies of this report, please visit www.sen.ca.gov/sor.

Saskia Kim

Since 2005, Saskia Kim has worked for the California Senate Office of Research as a senior policy consultant specializing in judiciary, privacy, and business and professions issues. Prior to that she was counsel to the California Assembly Judiciary Committee and a legislative aide in the U.S. Congress. In 2006 she was awarded an Ian Axford Fellowship in Public Policy and was based at the Ministry of Justice and Office of the Privacy Commissioner in Wellington, New Zealand.

1399-S
Additional copies of this publication may be purchased for $20.00 per copy
(includes shipping and handling), plus current California sales tax.

Senate Publications & Flags
1020 N Street, Room B-53
Sacramento, CA 95814
(916) 651-1538

Make checks or money orders payable to Senate Rules Committee.
Credit cards not accepted.
Please include stock # 1399-S when ordering.