Privacy Law Developments in California

MARGARET BETZEL*

ABSTRACT

This article discusses the privacy laws of California. The primary goal of the article is to assist businesses and organizations that operate on a national scope to know when and where the California privacy laws apply. Therefore, the article frequently compares California law with federal law. The article will address 5 major topics: (1) California's constitutional right to privacy, (2) California's law on the collection and management of information, (3) California's internet and computer privacy laws, (4) California's criminal law as it relates to privacy, and (5) California's Office of Privacy Protection.

I. INTRODUCTION

According to the Federal Trade Commission, California had 45,175 reported victims of identity theft in 2005.[1] This calculates to 125 victims per 100,000 people in California's population.[2] This statistic places California as the state with the third highest number of victims of identity theft, behind Nevada, and Arizona.[3] To counteract this growing problem, California has led the nation in the development of privacy laws. This article will address these new privacy laws. However, this article will go beyond merely describing these new laws. The goal of this article is to assist businesses and organizations that operate on a national scope by identifying when and where the California privacy laws apply.

This article is divided into five major sections:

1. The first section discusses California's constitutional right to privacy and how it relates to the right to privacy under the United States Constitution.

---

* The author received her J.D. from The Ohio State University Moritz College of Law in 2006. The author would like to thank Peter Swire for his assistance and guidance in this article.

[1] Office of the Attorney General, *Identity Theft*, http://ag.ca.gov/idtheft/ (last visited July 29, 2006).

[2] *Id.*

[3] *Id.*

2. The second section discusses California's law on the collection and management of information. This section will include three major subsections: (1) California's law on medical information and how it relates to federal law, (2) California's law on financial and banking institution information practices and how it relates to the federal law, and (3) California's law on government information collection.

3. The third section discusses California's new Internet and computer privacy laws and how they compare to the federal laws.

4. The fourth section discusses California's criminal law as it relates to privacy. This section will be divided into four subsections: (1) California's criminal law on the invasion of privacy and how it compares to the federal law, (2) California's criminal law on the protection of California citizens against identity theft and how it compares to federal law, (3) California's computer crimes statute and how it compares to the federal Computer Fraud and Abuse Act, and (4) California's criminal protection against unauthorized loan applications.

5. The fifth section discusses the Office of Privacy Protection. This office was created to promote and protect the privacy rights of California consumers.[4]

Following the paper will be an appendix containing Internet links to California's privacy laws and other California privacy information.

II. THE CONSTITUTIONAL RIGHT TO PRIVACY

Both the United States Constitution and the California Constitution contain a right to privacy. However, although the two rights have similar goals, they apply differently. The United States constitutional right to privacy and the California constitutional right to privacy will be discussed below.

---

[4] Office of Privacy Protection, http://www.privacy.ca.gov/ (last visited July 29, 2006).

A. THE UNITED STATES CONSTITUTIONAL RIGHT TO PRIVACY

The United States constitutional right to privacy is not written directly in the Constitution. Instead, it was first articulated by the United States Supreme Court in *Griswold v. Connecticut* in 1965.[5] In *Griswold*, the Supreme Court considered the constitutionality of a Connecticut statute that barred people from assisting others with the use of contraceptive devices.[6] In this case, the executive director of the Planned Parenthood League of Connecticut was charged with giving a married couple information, instruction, and medical advice on how to prevent conception, as well as providing the couple with a contraceptive device.[7] The Court held that this statute was unconstitutional because it violated the constitutional right to privacy.[8] The Court explained that even though a right to privacy is not specifically articulated in the Constitution, "[the] right to privacy [is] older than the Bill of Rights -- older than our political parties."[9] The Court then established that the right to privacy was a fundamental right under the Constitution and it came from penumbras of the Bill of Rights through the First, Fourth, Fifth and Ninth Amendments.[10]

In 1972, the Supreme Court reiterated the constitutional right to privacy in *Eisenstadt v. Baird*.[11] In this case, the Court struck down a law barring the distribution of contraceptives to unmarried persons because the law violated the right to privacy.[12] However, this time, the Supreme Court stated that the right to privacy came from the Fourteenth Amendment equal protection clause.[13]

---

[5] Griswold v. Connecticut, 381 U.S. 479 (1965).

[6] *Id.*

[7] *Id.* at 480.

[8] *Id.* at 484-86.

[9] *Id.* at 486.

[10] *Id.* at 484-85.

[11] Eisenstadt v. Baird, 405 U.S. 438 (1972).

[12] *Id.*

[13] *Id.* at 453.

Even though the source of the right to privacy is still unclear, it has become a solidified piece of constitutional jurisprudence. Under current law, a statute, regulation, or policy cannot be sustained if it infringes on the right to privacy unless the law is sufficiently narrowly tailored to serve a compelling state interest.[14] The Supreme Court has used the right to privacy to decide many controversial decisions, such as to overturn a law barring abortions[15] and to overturn a law barring two person of the same sex from engaging in sexual conduct.[16] However, even though the right has been broadly construed by the Supreme Court in recent years, the federal right to privacy can only be used to challenge government actions and cannot be used against a private corporation.[17]

B. CALIFORNIA'S CONSTITUTIONAL RIGHT TO PRIVACY

Unlike the United States constitutional right to privacy, California's constitutional right to privacy is specifically written into the state's constitution. The right to privacy was adopted as a result of a ballot initiative in 1972.[18]

The provision states,

> All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, *and privacy*.[19]

---

[14] Lawrence v. Texas, 539 U.S. 558, 593 (2003) (Scalia, J.,dissenting).

[15] Roe v. Wade, 410 U.S. 113 (1973).

[16] Lawrence, 539 U.S. at 558.

[17] *See* Virginia v. Rives, 100 U.S. 313, 318 (1880) (in which the Court states, "The provisions of the Fourteenth Amendment of the Constitution...all have reference to State action exclusively, and not to any action of private individuals.").

[18] Scott A. Baxter, *Review of Selected 1998 California Legislation: Public Entities, Officers and Employees: Informational Privacy and the California Public Records Act*, 30 MCGEORGE L. REV. 778, 780 (1999).

[19] CAL. CONST., art. I, § 1 (emphasis added).

Unlike the federal constitutional right to privacy, the California constitutional right to privacy protects individuals against privacy infringement from both public and private entities.[20]

The California Supreme Court outlined the elements and defenses of a constitutional privacy cause of action in *Hill v. National Collegiate Athletic Association*.[21] In this case, the plaintiffs, student athletes, argued that random drug testing programs administered by the National Collegiate Athletic Association ("NCAA") violated their right to privacy under the California Constitution. The court stated that the decision of whether the constitutional right to privacy has been violated is a balancing test between the interests of the plaintiff and the defendant.[22]

The first essential element to an invasion of privacy claim under the California Constitution "is the identification of a specific, legally protected privacy interest."[23] The court stated that "[j]ust as the right to privacy is not absolute, privacy interests do not encompass all conceivable assertions of individual rights."[24] The court listed two types of legally protected privacy interests: "(1) interests in precluding the dissemination or misuse of sensitive and confidential information (called informational privacy) and (2) interests in making intimate personal decisions or conducting personal activities without observation, intrusion, or interference (called autonomy privacy)."[25] If the interest alleged by the plaintiff falls into either of these categories, then it is a "legally protected privacy interest."[26]

The second essential element to a claim of invasion of privacy under the California Constitution is a reasonable expectation of privacy. The court stated that "[t]he extent of a privacy interest is not independent of the circumstances."[27] According to the California

---

[20] Am. Acad. of Pediatrics v. Lungren, 16 Cal. 4th 307, 326 (Cal. 4th 1997).

[21] Hill v. Nat'l Collegiate Athletic Ass'n, 7 Cal. 4th 1 (Cal. 4th 1994).

[22] *Id.* at 26-27.

[23] *Id.* at 35.

[24] *Id.*

[25] *Id.*

[26] *Id.*

[27] *Hill*, 7 Cal. 4th at 36 (quoting Plante v. Gonzalez, 575 F.2d 1119, 1135 (5th Cir. 1978)).

Supreme Court, "[e]ven when a legally cognizable privacy interest is present, other factors may affect a person's reasonable expectation of privacy."[28] The court listed a variety of factors that should be used in assessing whether there is a reasonable expectation of privacy, including customs, practices, physical setting, whether there was advance notice of the intrusion, and whether there was "the presence or absence of opportunities to consent voluntarily" to the activities affecting privacy interests.[29] A reasonable expectation of privacy is to be decided on the basis of "widely accepted community norms."[30]

Next, the California Supreme Court stated that "[a]ctionable invasions of privacy must be sufficiently serious in their nature, scope, and actual or potential impact to constitute an egregious breach of the social norms underlying the privacy right."[31] The court said that the "extent and gravity of the invasion" must be considered in assessing whether there is a violation of the right to privacy.[32]

The California Supreme Court said that the identified privacy interests must be balanced against the competing interests.[33] The court said that "[i]nvasion of a privacy interest is not a violation of the state constitutional right to privacy if the invasion is justified by a competing interest. Legitimate [competing] interests derive from the legally authorized and socially beneficial activities of the government and private entities."[34] The relative importance of the competing interests is "determined by their proximity to the central functions" of the enterprise.[35] The court said that "conduct alleged to be an invasion of privacy" must be "evaluated based on the extent to which it furthers legitimate and important competing interests."[36]

---

[28] *Id.* at 36.

[29] *Id* at 36-37.

[30] *Id* at 37.

[31] *Id.*

[32] *Id.*

[33] *Hill*, 7 Cal. 4th at 37.

[34] *Id.*

[35] *Id.*

[36] *Id.*

If a plaintiff is confronted with a defense based on a competing interest, the plaintiff may rebut this defense with a showing of "availability and use of protective measures, safeguards, and alternatives to the defendant's conduct that would minimize the intrusion on privacy interests."[37]

Finally, the court noted that judicial assessment of the balancing of interests may differ if the defendant is a government entity versus a private entity.[38] The court listed a variety of factors to consider in weighing the balance. The court noted that government intrusion into privacy typically has the capacity to be far more detrimental to personal privacy than an intrusion by a private entity because the government has more power and resources available to it than a private entity.[39] The court noted that an individual has greater choice in dealing with private actors than when dealing with the government.[40] However, if there is a monopoly, the individual can go to the legislature and seek a statutory remedy to the problem.[41] Finally, unlike interaction with the government, private individuals can choose how to communicate and associate with each other through mutually negotiated terms and conditions.[42] The court went on to note, however, that if a "private entity controls access to a vitally necessary item," it may tip the balance toward the plaintiff.[43]

Even though the California Supreme Court stated that the California constitutional right to privacy may not apply as stringently to private actors, it still should be a concern to corporations operating in California. The California constitutional right to privacy will apply to a corporation's interactions with California customers and employees. Corporations may be especially vulnerable under the realm of informational privacy (which the California Supreme Court defined as protecting interests in "precluding the dissemination or

---

[37] *Id.*

[38] *Id.*

[39] *Hill*, 7 Cal. 4th at 37.

[40] *Id.*

[41] *Id.* at 39.

[42] *Id.*

[43] *Id.*

misuse of sensitive and confidential information").[44] Therefore, corporations must be careful to protect California customer and employee information. This level of care, however, will not have to be exercised on a national scope because the federal constitutional right to privacy does not apply to private actors.

III. CALIFORNIA LAW ON THE COLLECTION AND MANAGEMENT OF INFORMATION

This section covers three major subjects: (1) the collection and management of medical information, (2) the regulation of financial and banking institutions, and (3) the regulation of government information collection. Each of these subjects is discussed below.

A. COLLECTION AND MANAGEMENT OF MEDICAL INFORMATION

California has enacted several medical privacy laws, including the Confidentiality of Medical Information Act and California Civil Code § 1798.91. In some cases, these laws go well beyond what is required under federal law. Each law and how it compares to federal law will be discussed below.

1. CALIFORNIA CONFIDENTIALITY OF MEDICAL INFORMATION ACT

The Confidentiality of Medical Information Act ("CMIA") regulates the release of medical information. The statute requires patient authorization for release of medical information unless the release is otherwise permitted or required by law.[45] The federal analogue of CMIA is the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").[46] HIPAA is composed of two major sections.[47] The first section, Title I, is designed to protect "health insurance coverage for workers and their families when they

---

[44] *Id.* at 35.

[45] CAL. CIV. CODE § 56.10 (West 2005).

[46] Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. §§ 1320d to 1320d-8 (2005).

[47] Wikipedia, Health Insurance Portability and Accountability Act, http://en.wikipedia.org/wiki/HIPAA (last visited Aug. 27, 2006).

change or lose their jobs."[48] The second section, Title II, contains the administrative simplification provisions.[49] The administrative simplification provisions only apply to "covered entities" under HIPAA.[50] The administrative simplification provisions regulate the protection of patient health information, the HIPAA electronic data interchange, and the implementation of security plans to control access to patient information.[51] This section will address how CMIA and HIPAA interact.

According to Clark Stanton, when determining whether state law or HIPAA applies, HIPAA functions as the baseline.[52] State law, such as California's CMIA, will be used rather than HIPAA in three situations: (1) "there is no HIPAA law on the issue; (2) [the] state law is more stringent than HIPAA;" or (3) the Secretary of Health and Human Services has created an exception and determines that the state law should apply rather than HIPAA.[53] The Secretary can create an exception in two situations. First, the Secretary can create an exception if the Secretary determines that the state law provision "is necessary—(I) to prevent fraud and abuse; (II) to ensure appropriate State regulation of insurance and health plans; (III) for State reporting on health care delivery or costs; or (IV) for other purposes."[54] Second, the Secretary can also create an exception if the state law provision "addresses controlled substances."[55] In general, exceptions will be created for "specific state laws, not entire state schemes."[56]

---

[48] *Id.*

[49] *Id.*

[50] A "covered entity" is a health plan, health care clearinghouse, or health care provider who transmits health information electronically. 42 U.S.C. § 1320d-5(a) (2005).

[51] Wikipedia, *supra* note 47.

[52] CLARK STANTON, FEDERAL PREEMPTION AND STATE LAW AND REGULATION: CALIFORNIA (HIPPA SUMMIT AUDIOCONFERENCE 2002) 4, http://www.ehcca.com/presentations/hipaaaudio20020710/stanton.ppt.

[53] *Id.*

[54] Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d-7 (2005).

[55] *Id.*

[56] STANTON, *supra* note 52, at 4.

Although preemption is complex and there have not been any direct rulings by the Secretary of Health and Human Services, it appears as though HIPAA will govern in certain situations. The following are such situations.

BUSINESS ASSOCIATES

HIPAA applies to covered entities. Covered entities include health care providers, health care plans, and health care clearinghouses.[57] HIPAA also applies to business associates. A business associate is "a person or organization, other than a member of a covered entity's workforce, that performs certain functions or activities on behalf of, or provides certain services to, a covered entity that involve the use or disclosure of individually identifiable health information."[58] In order for a covered entity to disclose information to a business associate, the covered entity must include certain protections for the information in the contract of agreement with the business associate.[59] The contract must contain written safeguards on the "individually identifiable health information used or disclosed by its business associates."[60] Furthermore, a covered entity cannot contractually authorize its business associate to use or disclose any health information in a way that a covered entity could not use or disclose the information under HIPAA rules.[61] In contrast, California law states that corporations organized for the primary purpose of maintaining medical information for providers must maintain the "same standards of confidentiality required of [the] provider" and are subject to the same penalties for improper use and disclosure of the information of the provider.[62] However, California law does not require that covered entities specifically contract with business associates before the covered entity

---

[57] U.S. Dep't of Health and Human Services, Summary of the HIPAA Privacy Rule 2-3, http://www.hhs.gov/ocr/privacysummary.pdf (last visited July 29, 2006) [hereinafter HHS].

[58] *Id.* at 3.

[59] *Id.*

[60] *Id.*

[61] *Id.*

[62] CAL. CIV. CODE § 56.06 (West 2005).

can release the information. Therefore, in this case, HIPAA will govern.[63]

MINIMUM NECESSARY

A major tenet of HIPAA is that covered entities should not use, disclose, or request more personal health information than is required for the purposes for which the use, disclosure, or request is sought.[64] California's CMIA does not have a similar requirement, so HIPAA will govern.[65]

NOTICE TO PATIENTS

HIPAA requires that covered entities give notice to patients on how the covered entity uses and handles personal health information.[66] The HIPAA rules require that the notice must state the "covered entity's duties to protect privacy, provide a notice of privacy practices, and abide by the terms of the current notice."[67] "The notice must [also] describe the individual's rights, including the right to complain to HHS [the Department of Health and Human Services] and to the covered entity if they believe their privacy rights have been violated."[68] California's CMIA does not require that notice be given to patients, so in this situation, HIPAA will govern.[69]

DISCLOSURE FOR RESEARCH PURPOSES

HIPAA allows disclosure and use of personal health information for research purposes without authorization as long as the covered entity obtains either:

---

[63] *See* STANTON, *supra* note 52, at 5.

[64] HHS, *supra* note 57, at 10.

[65] *See* STANTON, *supra* note 52, at 5.

[66] HHS, *supra* note 57, at 11.

[67] *Id.*

[68] *Id.*

[69] *See* STANTON, *supra* note 52, at 6.

> (1) documentation that an alteration or waiver of individuals' authorization for the use or disclosure of protected health information about them for research purposes has been approved by an Institutional Review Board or Privacy Board; (2) representations from the researcher that the use or disclosure of the protected health information is solely to prepare a research protocol or for similar purpose preparatory to research, that the researcher will not remove any protected health information from the covered entity, and that protected health information for which access is sought is necessary for the research; or (3) representations from the researcher that the use or disclosure sought is solely for research on the protected health information of decedents, that the protected health information sought is necessary for research, and, at the request of the covered entity, documentation of the death of the individuals about whom information is sought.[70]

The California CMIA is less stringent because it does not require an approval process.[71] The CMIA permits providers and plans to disclose medical information to several types of research institutions as long as the information is not disclosed in any way that would disclose the identity of any patient or otherwise violate the statute.[72] Because HIPAA is more stringent than the California law, HIPAA will govern for research purposes.[73]

DISCLOSURES TO AGENCIES

HIPAA allows covered entities to make disclosures of personal health information to:

> [a] health oversight agency for oversight activities authorized by law . . . [when use of the information is]

---

[70] HHS, *supra* note 57, at 8.

[71] *See* STANTON, *supra* note 52, at 12.

[72] CAL. CIV. CODE § 56.10(c)(7) (West 2005).

[73] *See* STANTON, *supra* note 52, at 12.

> necessary for appropriate oversight of: (i) [t]he health care system; (ii) [g]overnment benefit programs for which health information is relevant to beneficiary eligibility; (iii) [e]ntities subject to government regulatory programs . . . [if the] health information is necessary for determining compliance with program standards; or (iv) entities subject to civil rights laws [if the] health information is necessary for determining compliance.[74]

Alternatively, the CMIA allows health care providers and health care service plans to disclose information to agencies when the disclosure is necessary for licensing and when it is otherwise specifically authorized by law.[75] Because it appears that HIPAA's requirements are more restrictive, HIPAA will govern.

DISCLOSURE FOR PEER REVIEW PURPOSES

HIPAA requires that covered entities obtain patient consent before using or disclosing personal health information for health care operations, including credentialing, and peer review.[76] On the other hand, CMIA expressly allows health care providers and health care plans to use and disclose medical information to hospital medical staff and other entities for peer review purposes without obtaining patient consent.[77] Because HIPAA is more restrictive than the CMIA on use and disclosure of personal health information for peer review, HIPAA will govern.

There are certain situations where California's CMIA will govern because it is more stringent than HIPAA. The following are such situations.

---

[74] 45 C.F.R. § 164.512(d) (2005).

[75] CAL. CIV. CODE §§ 56.10(c)(5), 56.10(c)(14) (West 2005).

[76] 45 C.F.R. § 164.506 (2005). For a definition of health care operations, see 45 C.F.R. § 164.501 (2005).

[77] CAL. CIV. CODE § 56.10(c)(4) (West 2005).

SUBPOENAS AND OTHER DISCOVERY REQUESTS

HIPAA states that a covered entity may release personal health information when it is subpoenaed or otherwise requested without a court order in two situations: (1) when the "covered entity receives satisfactory assurance . . . from the party seeking the information that reasonable efforts have been made by the party to ensure that the individual who is the subject of the protected health information that has been requested has been given notice of the request" when personal health information is subpoenaed; or (2) "[t]he covered entity receives satisfactory assurance . . . from the party seeking the information that reasonable efforts have been made by such party to secure a qualified protective order that" prohibits the information from being used in any context other than the court proceeding for which it was requested and requires that the information be destroyed or returned to the covered entity at the end of the proceeding.[78] California's law is more stringent than HIPAA.[79] Unlike HIPAA, which allows medical records to be disclosed under subpoena without notifying the individual who the records concern, the CMIA requires that the requesting party serve a Consumer Notice to the individual whose records are being sought before those records can be disclosed.[80] Therefore, when operating in California, a covered entity must follow the California law because it is more stringent than the HIPAA requirements.[81]

DISCLOSURES FOR MARKETING AND FUNDRAISING PURPOSES

HIPAA permits disclosures for marketing and fundraising purposes in limited situations. Disclosures for marketing purposes are permitted under HIPAA when: (1) the marketing communications are used "to describe health-related products or services, or payment for them, provided by or included in a benefit plan of the covered entity making the communication;" (2) the marketing communications are about "participating providers in a provider or health plan network,

---

[78] 45 C.F.R. § 164.512(e) (2005).

[79] STANTON, *supra* note 52, at 8.

[80] CAL. CIV. PROC. CODE. § 1985.3 (West 2005).

[81] STANTON, *supra* note 52, at 8.

replacement of or enhancements to a health plan, or health-related products or services available only to a health plan's enrollees that add value to, but are not part of, the benefits plan;" (3) the marketing communications are "for treatment of the individual;" and (4) the marketing communications are for "case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or care settings to the individual."[82] On the other hand, the CMIA specifically prohibits health care providers, health care service plans, contractors, corporations, subsidiaries, and affiliates from intentionally using medical information for marketing purposes without the consent of the patient.[83] Because the CMIA is more restrictive than HIPAA, the CMIA will govern in this circumstance.

There are situations in which the interaction between the California CMIA and HIPAA is especially unclear. Therefore, it is uncertain which law would govern. The following are such situations.

DISCLOSURES TO LAW ENFORCEMENT

HIPAA allows disclosures to law enforcement in six circumstances: (1) when the disclosure is "required by law (including court orders, court-ordered warrants, subpoenas) and administrative requests;" (2) when the disclosure can be used to "identify or locate a suspect, fugitive, material witness, or missing person;" (3) when the disclosure is "in response to a law enforcement official's request for information about a victim or suspected victim of a crime;" (4) when the disclosure is to "alert law enforcement of a person's death, if the covered entity suspects that a criminal activity caused the death;" (5) when the disclosure would be because "a covered entity believes that protected health information is evidence of a crime that occurred on its premises;" and (6) when the disclosure is by "a covered health care provider in a medical emergency not occurring on its premises," and is "necessary to inform law enforcement about the commission and nature of a crime, the location of the crime or crime victims, and the

---

[82] HHS, *supra* note 57, at 9-10.

[83] CAL. CIV. CODE § 56.10(d) (West 2005).

perpetrator of the crime."[84] It is unclear whether all of these disclosures are permitted under California's CMIA.[85]

While there are situations when it is unclear whether California's CMIA or HIPAA will govern, in the case of penalties, it is possible that *both* HIPAA and CMIA can be applied concurrently if an entity or person is found to have violated both statutes.[86] The following discussion addresses penalties under HIPAA and the CMIA.

PENALTIES UNDER HIPAA

HIPAA provides two methods for punishing those who violate its provisions. If a covered entity generally does not comply with the provisions of HIPAA, the Secretary of Health and Human Services shall impose "a penalty of not more than $100 for each such violation, except that the total amount imposed on the person for all violations of an identical requirement or prohibition during a calendar year may not exceed $25,000."[87] However, if a covered entity or "person knowingly uses or causes to be used a unique health identifier" in violation of HIPAA, "obtains individually identifiable health information relating to an individual" in violation of HIPAA, or "discloses individually identifiable health information to another person" in violation of HIPAA, the covered entity or person can be fined up to $50,000, imprisoned for up to one year, or both.[88] "If the offense is committed under false pretenses," the covered entity or person can be fined up to $100,000, imprisoned up to five years, or both.[89] "If the offense is committed with the intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm," the covered entity or person can be fined up to $250,000, imprisoned up to ten years, or both.[90]

---

[84] HHS, *supra* note 57, at 7.

[85] *See* STANTON, *supra* note 52, at 9.

[86] *See supra* Part II.A.1.

[87] 42 U.S.C. § 1320d-5(a)(1) (2005).

[88] *Id.* § 1320d-6.

[89] *Id.*

[90] *Id.*

PENALTIES UNDER CMIA

Unlike HIPAA, under California's CMIA, a patient who is harmed through unlawful disclosure can receive monetary damages. The CMIA provides that

> [i]n addition to any other remedies available at law, a patient whose medical information has been used or disclosed in violation of [the CMIA] . . . and who has sustained economic loss or personal injury therefrom may recover compensatory damages, punitive damages not to exceed three thousand dollars ($3,000), attorneys' fees not to exceed one thousand dollars ($1,000), and the costs of litigation.[91]

Because HIPAA and CMIA provide for different penalty structures, with HIPAA providing for civil fines and jail time and CMIA calling for monetary damages to the patient, it is possible for a person or an entity to be forced to pay civil fines and monetary damages to the patient, as well as serve jail time. Therefore, entities regulated by HIPAA and CMIA should be careful to abide by both statutory schemes to avoid liability.

2. CALIFORNIA CIVIL CODE § 1798.91

California Civil Code § 1798.91 places restrictions on how and when businesses can obtain medical information from individuals for use in direct marketing purposes. Direct marketing purposes is defined as "the use of personal information for marketing or advertising products, goods, or services directly to individuals."[92] California Civil Code § 1798.91 states:

> A business may not orally request medical information directly from an individual regardless of whether the information pertains to the individual or not, and use, share, or otherwise disclose that information for direct marketing purposes without doing both the following prior to obtaining that information: (1) Orally disclosing to the individual in

---

[91] CAL. CIV. CODE § 56.35 (West 2005).

[92] *Id.* § 1798.91(a)(1).

> the same conversation during which the business seeks to obtain the information, that it is obtaining the information to market or advertise products, goods, or services to the individual[; and] (2) Obtaining the consent of either the individual to whom the information pertains or a person legally authorized to consent for the individual, to permit his or her medical information to be used or shared to market or advertise products, goods, or services to the individual, and making and maintaining for two years after the date of the conversation, an audio recording of the entire conversation.[93]

The statute places similar requirements on obtaining medical information for purposes of direct marketing through writing. The statute states:

> A business may not request in writing medical information directly from an individual regardless of whether the information pertains to the individual or not, and use, share, or otherwise disclose that information for direct marketing purposes, without doing both of the following prior to obtaining that information: (1) Disclosing in a clear and conspicuous manner that it is obtaining the information to market or advertise products, goods, or services to the individual[; and] (2) Obtaining the written consent of either the individual to whom the information pertains or a person legally authorized to consent for the individual, to permit his or her medical information to be used or shared to market or advertise products, goods, or services to the individual.[94]

The federal analogue to this California statute is HIPAA. HIPAA has similar requirements for disclosure of medical information. HIPAA requires that in order for a covered entity to be able to disclose personal health information to a third party to be used for marketing purposes, the covered entity must obtain authorization from the individual.[95] The authorization must contain the following core elements.

---

[93] *Id.* § 1798.91(b).

[94] *Id.* § 1798.91(c).

[95] 45 C.F.R. § 164.508(a)(3) (2005).

> (i) A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion. (ii) The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure. (iii) the name or other specific identification of the person(s), or class of persons, to whom the covered entity may make the requested use or disclosure. (iv) a description of each purpose of the requested use or disclosure. The statement "at the request of the individual" is a sufficient description of the purpose when an individual initiates the authorization and does not, or elects not to, provide a statement of the purpose. (v) an expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure. The statement "end of the research study," "none," or similar language is sufficient if the authorization is for a use or disclosure of protected health information for research, including for the creation and maintenance of a research database or research repository. (vi) signature of the individual and date. If the authorization is signed by a personal representative of the individual, a description of such representative's authority to act for the individual must also be provided.[96]

In addition to these core elements, HIPAA requires that the authorization contain statements that allow the individual to be on notice of the following: (1) "[t]he individual's right to revoke the authorization in writing and . . . [t]he exceptions to the right to revoke and a description of how the individual may revoke the authorization;" (2) "[t]he ability or inability to condition treatment, payment, enrollment or eligibility for benefits on the authorization;" and (3) "[t]he potential for information disclosed pursuant to the authorization to be subject to redisclosure by the recipient and no longer be protected by this subpart."[97] HIPAA also requires that the authorization document be written in plain language and a copy of the signed authorization must be provided to the individual.[98]

---

[96] *Id.* § 164.508(c)(1).

[97] *Id.* § 164.508(c)(2).

[98] *Id.* §§ 164.508(c)(3), (4).

As previously stated, the general preemption rule when comparing HIPAA to any other statute that governs similar situations, is HIPAA is a baseline rule. It governs when there is no other state statute or when the state statute provides less stringent protections than HIPAA. However, the state statute governs instead of HIPAA in three situations: (1) there is no HIPAA law on the issue; (2) the state law is more stringent than HIPAA; and (3) the Secretary of Health and Human Services creates an exception and determines that the state law should apply rather than HIPAA.[99]

When HIPAA is compared to California Civil Code § 1798.91, it is clear that the California statute applies to a wider range of situations. Unlike HIPAA, the California statute applies when the business is obtaining health information from the individual directly and from all other sources, including "covered entities" under HIPAA. Under the general HIPAA preemption rules, California Civil Code § 1798.91 would apply when HIPAA does not. Therefore, § 1798.91 would apply when a business is trying to obtain medical information for marketing purposes from the individual and from all sources that do not qualify as "covered entities" under HIPAA.

Yet, it appears as though the authorization requirements under HIPAA are more stringent than the California authorization requirements. Therefore, HIPAA would govern when a business is trying to obtain medical information for marketing purposes from any covered entity.

Because of the complexity of interactions between HIPAA and California Civil Code § 1798.91, a business or corporation must be careful to do research on each specific situation.

B. FINANCIAL AND BANKING INSTITUTION INFORMATION LAW

California has enacted a wide variety of laws regulating privacy issues in financial and banking institutions. This topic will be divided into seven sections: (1) California Financial Information Privacy Act, (2) disclosure of breach insecurity by businesses maintaining computerized data that includes personal information, (3) destruction of consumer records, (4) confidentiality of social security numbers, (5) prohibited business disclosures, (6) background checks and issuing

---

[99] STANTON, *supra* note 52, at 4. For a discussion of exceptions under HIPAA, see the previous section on the California CMIA.

credit, and (7) prohibition of debt collection once evidence of identity theft is provided.

1. CALIFORNIA FINANCIAL INFORMATION PRIVACY ACT

The California Financial Information Privacy Act ("FIPA") was created to ensure that Californians have the ability to control the disclosure of "nonpublic personal information."[100] FIPA gives Californians more control over their personal information in several ways. First, FIPA requires financial institutions that want to share information with *non-affiliated third-parties and unrelated companies* "to seek and acquire affirmative consent of California consumers prior to sharing the information."[101] Second, FIPA provides that companies must provide customers the ability to prevent the sharing of financial information with *affiliated companies* through an opt-out mechanism.[102] Third, FIPA states that a financial institution may not share information with an affiliate unless the financial institution *annually* provides notice of such disclosure to consumers.[103]

FIPA interacts with several different federal statutes. One of these statutes is the Fair Credit Reporting Act ("FCRA"). The purpose of the FCRA is "to require that consumer reporting agencies adopt reasonable procedures for consumer credit, personnel, insurance, and other information in a manner which is fair and equitable to the consumer, with regard to the confidentiality, accuracy, relevancy, and proper utilization of [consumer credit reports.]"[104] With this goal in mind, Congress created the FCRA as a set of "standards for collecting and disseminating consumer information."[105] Under the FCRA, affiliates are allowed to share consumer information as long as the consumers receive notice of the sharing and the opportunity to opt out

---

[100] CAL. FIN. CODE § 4051.5(b)(1) (West 2005).

[101] *Id.* § 4051.5(b)(2).

[102] *Id.* § 4051.5(b)(3).

[103] *Id.* § 4053(b)(1).

[104] 15 U.S.C. § 1681(b) (2005).

[105] Jason Shroff, *California: A Privacy Statute Meets the GLBA & FCRA*, 9 N.C. BANKING INST. 223, 228 (2005).

of the sharing.[106] Unlike FIPA, this notice does not have to be an annual notice. The FCRA does not discuss the sharing of consumer information with non-affiliated third parties.

The FCRA was recently amended by the Fair and Accurate Credit Transactions Act ("FACT Act"). The FACT Act prohibits the sharing of information for marketing purposes unless it is both clearly and obviously disclosed to the consumer that their information can be shared with others for the purposes of soliciting the customer.[107] Furthermore, the customer must be given an opportunity to prevent the solicitations.[108]

FIPA also interacts with the Gramm-Leach-Bliley Act ("GLBA"). The GLBA was enacted to achieve "financial modernization" through better laws for financial holding companies.[109] However, to protect consumers, the GLBA also included additional information-sharing requirements.[110] The GLBA requires that financial holding companies and banks create policies on securing nonpublic personal information.[111] The GLBA states that these policies should protect "the privacy of its customers and . . . the security and confidentiality of those customers' nonpublic personal information."[112] The banks and financial holding companies also must notify the consumer of the policies that they are installing under the GLBA.[113]

Under the GLBA, financial institutions are prohibited from sharing nonpublic personal information with entities not affiliated with the financial institutions unless the financial institution provides the customer with appropriate notice.[114] If a consumer does not want this information to be disclosed to a nonaffiliated third party, he or she can

---

[106] 15 U.S.C. § 1681b(e) (2005).

[107] *Id.* § 1681s-3(a)(1).

[108] *Id.*

[109] Shroff, *supra* note 105, at 226.

[110] *Id.*

[111] 15 U.S.C. § 6801 (2005).

[112] *Id.* § 6801(a).

[113] *Id.* § 6803.

[114] *Id.* § 6802.

notify the financial institution in writing and, subsequently, the financial institution may not disclose the information. However, the GLBA still allows financial institutions to share information with its affiliates without prior notice.[115]

Until recently, the interaction between FIPA, FCRA, the FACT Act, and GLBA was unclear. Both the FCRA and the GLBA have preemption provisions within the statutes. The FCRA's express preemption provision states that "no requirement or prohibition may be imposed under the laws of any State . . . with respect to the exchange of information among persons affiliated by common ownership or common corporate control."[116] In contrast, the GLBA's preemption clause says that state laws that are not inconsistent with the provisions of the GLBA and "[a]fford any person . . . greater . . . protection" than that provided under the GLBA, are not preempted.[117] In 2005, the Ninth Circuit attempted to solve the dilemma over which law governs by taking up the case *American Bankers' Association v. Gould*.[118] In this case, the Ninth Circuit had to decide whether FCRA preempted FIPA "insofar as [FIPA] regulates the exchange of information among financial institutions and their affiliates."[119] The American Bankers' Association contended that FIPA's opt-out provisions for affiliate information-sharing, which required companies to provide annual notice to consumers of their opportunity to opt-out of the information-sharing, were preempted by the FCRA, which does not require annual notice to consumers.[120] The trial court held that FIPA was not preempted in any way and dismissed on summary judgment.[121] On appeal, the Ninth Circuit held that FIPA was partially preempted by FCRA. The court held that FIPA was preempted

---

[115] Chad C. Coombs & Keenen Milner, *New California Identity Theft Legislation*, 27 LOS ANGELES LAW. 21, 22 (2004).

[116] 15 U.S.C. § 1681t(2) (2005).

[117] *Id.* § 6807(b).

[118] Am. Bankers' Ass'n v. Gould, 412 F.3d 1081 (9th Cir. 2005).

[119] *Id.* at 1083.

[120] *Id.* at 1085.

[121] *Id.* at 1083.

> to the extent that it applies to information shared between affiliates concerning consumers' 'credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living' that is used, expected to be used, or collected for the purpose of establishing eligibility for 'credit or insurance,' employment, or other authorized purpose.[122]

The court then stated that even though GLBA allows for more restrictive state laws, the preemptive effect of FCRA is not affected by GLBA.[123] The court then remanded to the district court to determine what portion of FIPA should survive preemption.[124]

On remand, the district court found that no portion of FIPA's affiliate-sharing provision survived preemption and those portions were no longer good law.[125] The court refused to answer the question of severability, stating that the "[d]efendants are necessarily asking this Court to 'dissect an unconstitutional measure and reframe a valid one out of it by inserting limitations it does not contain. This is legislative work beyond the power and function of the court.'"[126] The court left the restructuring of FIPA to the California legislature.[127] As of now, it is unclear what remains of FIPA.

2. DISCLOSURE OF BREACH INSECURITY BY BUSINESSES MAINTAINING COMPUTERIZED DATA THAT INCLUDES PERSONAL INFORMATION: CALIFORNIA CIVIL CODE § 1798.29

On July 1, 2003, Senate Bill 1386 went into effect.[128] The enactment of Senate Bill 1386, or California Civil Code § 1798.29, was one of the most significant changes to California privacy law.

---

[122] *Id.* at 1087.

[123] *Id.* at 1088.

[124] *Am. Bankers' Ass'n*, 412 F.3d at 1087.

[125] Am. Bankers' Ass'n v. Lockyer, No. 04-0778, 2005 U.S. Dist. LEXIS 22437, at *2 (E.D. Cal. Oct. 4, 2005).

[126] *Id.* at 4 (quoting Hill v. Wallace, 259 U.S. 44, 70 (1922)).

[127] *Id.*

[128] Coombs & Milner, *supra* note 115, at 21.

California Civil Code § 1798.29 requires businesses to provide prompt notice to California resident customers of any breach of security involving unencrypted personal data.[129] "The law applies to any person or business that does business in California . . . and [any business] that owns or licenses computerized data that includes personal information" of California residents.[130] Sufficient notice under the statute must be provided directly to the individual whose information has been disclosed.[131] Sufficient notice can be either written notice or electronic notice.[132] However, if the business entity "demonstrates that the cost of providing notice would exceed . . . $250,000, or that the affected class of persons to be notified exceeds 500,000 persons, or the agency does not have sufficient contact information," substitute notice can be used.[133] Substitute notice consists of all of the following: "(A) E-mail notice when the agency has an e-mail address for the subject persons[;] (B) [c]onspicuous posting of the notice on the agency's Web site page, if the agency maintains one[; and] (C) [n]otification to major statewide media."[134] If the business or person fails to act in compliance with this law, any customer injured may institute a civil proceeding to recover damages.[135]

California Civil Code § 1798.29 has created a bevy of news due to its notification requirements. One news story involved data theft from ChoicePoint, in which ChoicePoint had to notify the public that the personal data of 145,000 customers was stolen from the company's database.[136] Another incident involved LexisNexis, in which LexisNexis had to notify 310,000 customers that a database had been

---

[129] CAL. CIV. CODE § 1798.29(a) (West 2005).

[130] Coombs & Milner, *supra* note 115, at 21.

[131] CAL. CIV. CODE § 1798.29 (West 2005).

[132] *Id.* at (g)(1)-(2).

[133] *Id.* at (g)(3).

[134] *Id.* at (g)(3)(A)-(C).

[135] *Id.* § 1798.84.

[136] Bob Sullivan, *Data Theft Affects 145,000 Nationwide: Suspect Arrested in ChoicePoint Case Agrees to a Plea Deal*, MSNBC.com, Feb. 18, 2005, http://www.msnbc.msn.com/id/6979897.

breached.[137] In the LexisNexis breach, the thieves accessed the customers' social security numbers, driver's license information, and addresses.[138] Yet another incident involved a breach of information at Bank of America and Wachovia, in which the banks had to notify over 670,000 customers that employees illegally sold the customers' account information.[139] The number of accounts affected could top more than 1,000,000.[140]

California Civil Code § 1798.29 was the first bill of its kind enacted in the United States.[141] However, as of July 18, 2006, thirty-four states have enacted security breach laws.[142] Currently, there is not a federal analogue to this law.

3. DESTRUCTION OF CONSUMER RECORDS: CALIFORNIA CIVIL CODE §§ 1798.80 – 1798.81

California Civil Code §§ 1798.80-1798.81 requires that businesses take reasonable steps to destroy customer records that contain personal information when the business is finished using them.[143] This statute applies to all businesses that have or maintain California "customer's records."[144] The records that must be destroyed include "any material, regardless of physical form, on which information is recorded or preserved by any means, including written or spoken words,

---

[137] Heather Timmons, *Security Breach at LexisNexis Now Appears Larger*, N.Y. TIMES, Apr. 13, 2005, *available at* http://www.nytimes.com/2005/04/13/technology/13theft.html?ei=5090&en=408eeb16d6d5ca34&ex=1271044800&adxnnl=1&partner=rssuserland&adxnnlx=1137430827-uXQ05PZNzFYysIGq+fAk/g.

[138] *Id.*

[139] *Bank Security Breach May be Biggest Yet: Account Info at Bank of America, Wachovia Sold by Employees; More Arrests Expected, N.J. Police Say*, CNNMONEY.COM, May 23, 2005, http://money.cnn.com/2005/05/23/news/fortune500/bank_info/.

[140] *Id.*

[141] The State Public Interest Research Group, State PIRG Summary of State Security Freeze and Security Breach Notification Laws, July 18, 2006, http://www.pirg.org/consumer/credit/statelaws.htm#breach.

[142] *Id.*

[143] CAL. CIV. CODE § 1798.81 (West 2005).

[144] *Id.* §§ 1798.80-1798.81.

graphically depicted, printed, or electromagnetically transmitted."[145] Personal information that must be protected under the statute include

> any information that identifies, relates to, describes, or is capable of being associated with, a particular individual, including, but not limited to, his or her 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.[146]

Currently, there is not a federal analogue to this statute.

4. CONFIDENTIALITY OF SOCIAL SECURITY NUMBERS: CALIFORNIA CIVIL CODE § 1798.85

California Civil Code § 1798.85 prohibits the use of social security numbers in any of the following situations: (1) an individual's social security number cannot be publicly posted or publicly displayed in any manner; (2) an individual's social security number cannot be printed on any card "required for the individual to access products or services provided by the person or entity;" (3) an individual cannot be required to "transmit his or her social security number over the Internet, unless the connection is secure or the social security number is encrypted;" (4) an individual cannot be required to "use his or her social security number to access an Internet Web site, unless a password or unique personal identification number or other authentication device is also required to access the Internet Web site;" and (5) an individual's social security number cannot be printed on any materials that are mailed to the individual, unless state or federal law requires the social security number to be on the document to be mailed.[147] This statute applies to persons and entities, so businesses that operate in California must be

---

[145] *Id.* § 1798.80(b).

[146] *Id.* § 1798.80(e).

[147] *Id.* § 1798.85.

careful not to use or disclose social security numbers in an illegal manner under the statute.[148] Currently, there is not a federal analogue to this statute.

5. PROHIBITED BUSINESS DISCLOSURES: CALIFORNIA CIVIL CODE §§ 1798.83-1798.84 AND 1799.1

California has enacted a set of statutes that require businesses to give notice to customers of any disclosures of information to a third party for direct marketing purposes upon the request of the customer.[149] This statute applies to all businesses that disclose California customer information to third parties for direct marketing purposes. If a customer is injured due to a violation of this provision, the customer can institute a civil action against the business.[150] A prevailing customer can obtain monetary damages, injunctive relief, costs, and attorney's fees.[151] Furthermore, if a business is found to have willfully, intentionally, or recklessly violated this provision, a customer may receive a civil penalty up to $3000 per violation.[152] However, if the business is not found to have willfully, intentionally, or recklessly violated the provision, the customer can receive a civil penalty up to $500 per violation.[153] Currently, there is not a similar federal statute.

California has also enacted a law that prohibits any business entity that performs bookkeeping services from disclosing

> in whole or in part the contents of any record, including the disclosure of information in the record in any composite of information, which is prepared or maintained by such business entity to any person, other than the individual or business entity which is the subject of the record, without the

---

[148] *Id.* §1798.85(a).

[149] CAL. CIV. CODE § 1798.83.

[150] *Id.* § 1798.84(b).

[151] *Id.* § 1798.84 (a)-(g).

[152] *Id.* § 1798.84 (c).

[153] *Id.*

> express written consent of such individual or business entity.[154]

Currently, there is not a federal law that is similar to this California statute.

6. BACKGROUND CHECKS AND ISSUING CREDIT: CALIFORNIA CIVIL CODE § 1785.20.3

California has enacted a statute that requires all persons and entities to take reasonable steps to verify the identity of a California credit applicant if the information provided by the applicant, including the applicant's first and last name, address, and social security number, does not reasonably match the information in the credit report.[155] The statute also says that if the credit report has been flagged, showing that the applicant has been a victim of identity theft, the person or entity may not extend credit or lend money without taking reasonable steps to verify a California consumer's identity.[156]

If a consumer suffers damages as a result of a person or entity violating this provision, the consumer can bring a civil action against the person or entity and recover actual damages, court costs, attorney's fees, and punitive damages up to $30,000 per violation.[157]

Federal law does overlap with this California provision. In 2003, Congress enacted the Fair and Accurate Credit Transactions Act ("FACT Act").[158] The FACT Act primarily regulates consumer credit reporting agencies. This Act provides that consumer credit reporting agencies must provide a mechanism for consumers to correct errors in their credit reports and to be able to flag their credit reports to show that the consumer is a victim of identity theft.[159] However, the Act

---

[154] *Id.* § 1799.1(a).

[155] Coombs & Milner, *supra* note 115, at 21.

[156] CAL. CIV. CODE § 1785.20.3(b) (West 2005).

[157] *Id.* § 1785.20.3(c).

[158] Jennifer Lynch, *Identity Theft in Cyberspace: Crime Control Methods and Their Effectiveness in Combating Phishing Attacks*, 20 BERKELEY TECH. L.J. 259, 278 (2005). For more discussion of the FACT Act, see the section on California's Financial Information Privacy Act.

[159] 15 U.S.C. §§ 1681c-1, 1681i (2005).

also regulates users of consumer credit reports. The Act states that if a business or entity obtains a credit report that has a substantially different address from the address of the applicant, the business or entity must act to "form a reasonable belief" that the identity of the applicant is the same as the person in the credit report.[160] The FACT Act overlaps with California Civil Code § 1785.20.3 because they both state that businesses and entities must verify the identity of the applicant if the credit report shows a discrepancy in the applicant's address. However, California Civil Code § 1785.20.3 goes further than the FACT Act in that if the credit report shows a discrepancy in the applicant's first or last name or social security number, California Civil Code § 1785.20.3 requires that businesses take action to verify the identity of the applicant, while the FACT Act does not require businesses to take any action if there is a discrepancy in the applicant's first or last name or social security number.

The FACT Act also provides that if a credit report is flagged showing that the consumer is a victim of identity theft, a business or entity cannot extend credit to that applicant "unless the [business or entity] utilizes reasonable policies and procedures to form a reasonable belief that the [business or entity] knows the identity of the [applicant]."[161] In this case, the FACT Act is virtually identical to California Civil Code § 1785.20.3.

Like California Civil Code § 1785.20.3, if a business or entity violates the provisions of the FACT Act, the consumer can file a civil suit against the business or entity. If the business or entity is found to have *willfully* violated the FACT Act, the court can award the consumer "actual damages sustained by the consumer . . . of not less than $100 and not more than $1000," punitive damages, costs of the court action and reasonable attorney's fees.[162] If the business or entity is found to have *negligently* violated the FACT Act, the court can award the consumer actual damages sustained by the consumer, court costs, and reasonable attorney's fees.[163]

The FACT Act does not completely preempt state law. The FACT Act states:

---

[160] *Id.* § 1681c(h).

[161] *Id.* § 1681c-1(h).

[162] *Id.* § 1681n.

[163] *Id.* § 1681o.

> [It] does not annul, alter, affect, or exempt any person . . . from complying with the laws of any State with respect to the . . . use of any information on consumers, or for the prevention or mitigation of identity theft, except to the extent that those laws are inconsistent . . . and then only to the extent of the inconsistency.[164]

Because the FACT Act and California Civil Code § 1785.20.3 are not inconsistent, California Civil Code § 1785.20.3 is not preempted. Therefore, businesses and entities that extend credit to California customers must comply with both the FACT Act and California Civil Code § 1785.20.3 to avoid civil liability under both statutes.

7. PROHIBITION OF DEBT COLLECTION ONCE EVIDENCE OF IDENTITY THEFT IS PROVIDED: CALIFORNIA CIVIL CODE § 1788.18 AND CALIFORNIA CIVIL CODE §§ 1798.92-1798.97

California law requires that debt collectors cease all collection activities once the debt collector receives a copy of a police report alleging that the debt is due to identity theft and a written statement from the debtor that he or she believes that he or she is a victim of identity theft with respect to the debt being collected.[165]

California law also enables victims of identity theft to bring a civil action against "claimants" in order to alleviate the damages due to identity theft.[166] A claimant is a "person who has or purports to have a claim for money or an interest in property in connection with a transaction procured through identity theft."[167] Under this statute, if the victim can prove by a preponderance of the evidence that he or she is a victim of identity theft, as defined in California Penal Code § 530.5, then he or she can obtain the following relief:

> (1) A declaration that he or she is not obligated to the claimant [on the claims arising from identity theft]. (2) A

---

[164] *Id.* § 1681t(a).

[165] CAL. CIV. CODE § 1788.18 (West 2005).

[166] *Id.* §§ 1798.92-1798.97.

[167] *Id.* § 1798.92.

> declaration that any security interest or other interest the claimant had purportedly obtained in the victim's property in connection with that claim is void and unenforceable. (3) An injunction restraining the claimant from collecting or attempting to collect from the victim on that claim, from enforcing or attempting to enforce any security interest or other interest in the victim's property in connection with that claim, or from enforcing or executing on any judgment against the victim on that claim. (4) If the victim has filed a cross-complaint against the claimant, the dismissal of any cause of action in the complaint filed by the claimant based on a claim which arose as a result of the identity theft. (5) Actual damages, attorney's fees, and costs, and any equitable relief that the court deems appropriate.[168]

The claimant can also be subjected to a civil penalty of up to $30,000 if all of the following is shown.

> (A) [The victim of identity theft] provided written notice to the claimant at the address designated by the claimant for complaints related to credit reporting issues that a situation of identity theft might exist and explaining the basis for that belief. (B) The claimant failed to diligently investigate the victim's notification of a possible identity theft. (C) The claimant continued to pursue its claim against the victim after the claimant was presented with facts that were later held to entitle the victim to a judgment pursuant to this section.[169]

There are federal provisions that are similar to these California laws. However, the federal provisions operate differently than the California provisions. As previously discussed, the FACT Act primarily regulates consumer credit reporting agencies.[170] However, the FACT Act also regulates the collection of debt and therefore enters

---

[168] *Id.* § 1798.93.

[169] *Id.* §1798.93(6).

[170] For more discussion of the FACT Act, see the sections on California's Financial Information Privacy Act and Background Checks and Issuing Credit.

the same regulatory sphere as California Civil Code § 1788.18. But, the FACT Act does not regulate debt collection in the same way as California Civil Code § 1788.18. Under the FACT Act, "no person shall sell, transfer for consideration, or place for collection a debt that such person has been notified . . . has resulted from identity theft."[171] Unlike the California provisions, the FACT Act does not require debt collectors to cease *all* debt collection activities once the debtor has notified the debt collector of the identity theft. Therefore, if a debt collector collects debt from California consumers, the debt collector must comply with the FACT Act as well as California Civil Code §1788.18 to avoid civil liability under both statutes.[172]

C. GOVERNMENT INFORMATION COLLECTION: INFORMATION PRACTICES ACT OF 1977

The California Legislature created the Information Practices Act of 1977 because they felt that "the right to privacy[as guaranteed by the California Constitution was] . . . was being threatened by the indiscriminate collection, maintenance, and dissemination of personal information and the lack of effective laws and legal remedies."[173]

Under this Act, California agencies are required to minimize the amount of information that California agencies maintain about individuals.[174] Furthermore, the Act mandates that the information that agencies use should be collected, "to the greatest extent possible, directly from the individual who is the subject of the information."[175]

The Act also limits California agencies' ability to disclose the information. The Act states that disclosures can be made to the individual, within the government, under statutory authority, or with

---

[171] 15 U.S.C. § 1681m(f)(1) (2005).

[172] For a discussion of civil liability under FACTA, see the previous section on Background Checks and Issuing Credit.

[173] CAL. CIV. CODE § 1798.1(a) (West 2005).

[174] *Id.* § 1798.14.

[175] *Id.* § 1798.15.

the consent of the individual.[176] Agencies are required to keep detailed records of the disclosures that it makes.[177]

The Act makes clear that individuals "have the right to inquire and be notified" as to what information agencies maintain about him or her.[178] Agencies must permit the individual to inspect the records about himself or herself.[179] Agencies also must amend the records upon the request of an individual if the record contains incorrect information.[180]

If an agency refuses to comply with any provision under this Act, an individual can bring a civil action against the agency.[181] The plaintiff can obtain an injunction.[182] The plaintiff can also obtain actual damages sustained by the individual, including damages for mental suffering, and the costs of the action with attorney's fees.[183]

IV. CALIFORNIA INTERNET AND COMPUTER PRIVACY LAW

California has recently enacted several computer privacy laws. This section will address the following laws and how they compare to applicable federal provisions: (1) The Online Privacy Protection Act, (2) The Consumer Protection Against Computer Spyware Act, and (3) The Anti-Phishing Act of 2005.

---

[176] *Id.* § 1798.24.

[177] *Id.* § 1798.25.

[178] *Id.* § 1798.32.

[179] CAL. CIV. CODE § 1798.34.

[180] *Id.* § 1798.35(a).

[181] *Id.* § 1798.45.

[182] *Id.* § 1798.47.

[183] *Id.* § 1798.48.

A. CALIFORNIA ONLINE PRIVACY PROTECTION ACT: CALIFORNIA BUSINESS AND PROFESSIONAL CODE §§ 22575-22579

The California Online Privacy Protection Act ("OPPA") became operative on July 1, 2004.[184] California was the first state in the nation to enact a law of this kind governing online privacy policies.[185] This statute says that operators of commercial web sites and online services "that collects personally identifiable information through the Internet about individual consumers residing in California" must conspicuously post the website's privacy policy.[186]

The privacy policy must do all of the following.

> (1) Identify the categories of personally identifiable information that the operator collects through the Web site . . . about individual consumers who use or visit its commercial Website . . . and the categories of third-party persons or entities with whom the operator may share that personally identifiable information. (2) If the operator maintains a process for an individual consumer who uses or visits its commercial Web site to . . . review and request changes to any of his or her personally identifiable information that is collected through the Web site or online service, provide a description of that process. (3) Describe the process by which the operator notifies consumers who uses or visits its commercial Web site . . . of material changes to the operator's privacy policy for that Web site or online service. (4) Identify its effective date.[187]

If an operator fails to post a privacy policy that complies with the statute, the web site operator will be open to civil lawsuits.[188] A web

---

[184] CAL. BUS. & PROF. CODE § 22579 (West 2005).

[185] Matthew A. Goldberg, *The Googling of Online Privacy: GMail, Search-Engine Histories and the New Frontier of Protecting Private Information on the Web*, 9 LEWIS & CLARK L. REV. 249, 254 (2005).

[186] CAL. BUS. & PROF. CODE § 22575(a) (West 2005).

[187] *Id.* § 22575(b).

[188] Stefanie Olsen, *California Privacy Law Kicks In*, CNET NEWS.COM, July 6, 2004, http://news.com.com/California+privacy+law+kicks+in/2100-1028_3-5258824.html.

site operator will be deemed to have violated the statute if he or she fails to post the policy either "knowingly and willfully" or "negligently and materially."[189] OPPA does not specify what type of damages are available to those who file civil lawsuits.

This law has sweeping ramifications because of the borderless nature of the Internet. Because the statute holds any company or web site conducting business with California citizens accountable for installing a privacy policy and any California citizen can access any web site at anytime, this means that all websites that collect information from its visitors and users must install a privacy policy whether or not the business operates out of California.[190] There is no comparable federal statute.

B. CALIFORNIA CONSUMER PROTECTION AGAINST COMPUTER SPYWARE ACT: CALIFORNIA BUSINESS AND PROFESSIONAL CODE § 22947.3

The California Consumer Protection Against Computer Spyware Act became effective on January 1, 2005.[191] This statute prohibits a person or entity that is not an authorized user from knowingly, "with conscious avoidance of actual knowledge, or willfully" copying computer software onto the computer of a consumer in the state and use the software to do any of the following acts: (1) modify the computer's Internet settings; (2) collect personally identifiable information about the user; (3) prevent an authorized user's reasonable efforts to install, or to disable software; (4) "intentionally misrepresent that software will be uninstalled or disabled by an authorized user's action;" or (5) "remove, disable, or render inoperative security, antispyware, or antivirus software installed on the computer."[192]

The Act also bans a person or entity that is not an authorized user from knowingly, "with conscious avoidance of actual knowledge, or willfully" copying computer software "onto the computer of a consumer in the state and using the software to do any of the following acts:" (1) to take control of the consumer's computer to (a) send

---

[189] CAL. BUS. & PROF. CODE § 22576 (West 2005).

[190] Olsen, *supra* note 188.

[191] Michael L. Baroni, *Spyware Beware*, 47 ORANGE COUNTY L. 36, 38 (2005).

[192] CAL. BUS. & PROF. CODE § 22947.2 (West 2005).

commercial electronic mail or a computer virus, (b) "access[] or [use] the consumer's modem or Internet service to cause damage to the consumer's computer" or to cause an "authorized use to incur financial charges for a service that is not authorized by the authorized user," (c) [use] the consumer's computer to cause damage to another computer, (d) "opening multiple, sequential . . . advertisements in the consumer's Internet browser without the authorization of an authorized user"; (2) to modify the computer's security settings; or (3) to prevent the authorized user's "reasonable efforts to block the installation of, or to disable, software."[193]

Although the passing of this Act has been widely applauded, some experts believe that the Act "does not do enough to curb . . . spyware."[194] Experts say that the Act "doesn't actually *prohibit* spyware."[195] Instead, it "merely requires notice to the computer user that the spyware is being installed."[196] Others say that the "Act's definition of spyware is too limited" because it "only targets software that has . . . [a] 'wrongful' effect" on the user's computer.[197] Instead, they think that the Act should have banned spyware from being installed "without the user's fully-informed knowledge and consent."[198] Finally, critics claim that the requirement that the Spyware perpetrator have willfully and deceptively installed the Spyware is too high of a burden to prove.[199]

Although not everyone is an ardent supporter of the Act, this law will have sweeping ramifications because the Internet does not have any borders. Therefore, any web site that conducts business with California citizens will be accountable if it unlawfully installs Spyware onto computers even if the website is not operated out of California. To date, there is not a federal analogue to this statute.

---

[193] *Id.* § 22947.3.

[194] Baroni, *supra* note 191, at 39.

[195] *Id.*

[196] *Id.*

[197] *Id.*

[198] *Id.*

[199] *Id.*

C. CALIFORNIA ANTI-PHISHING ACT OF 2005

The California Anti-Phishing Act was approved by the California Governor on September 30, 2005.[200] It became effective on January 1, 2006.[201] The statute states that it is "unlawful for any person, by means of a Web page, electronic mail message, or otherwise through use of the Internet, to solicit, request, or take any action to induce another person to provide identifying information by representing itself to be a business without the authority or approval of the business."[202]

Those who violate the statute can be subject to both criminal and civil penalties.[203] Both the business whose name or trademark is being used to phish for information and the person who has been phished may bring a civil action against the perpetrator.[204] The business may seek to recover "the greater of actual damages" or $500,000.[205] The person who has been phished may seek to enjoin further phishing attempts and to recover "the greater of three times the amount of actual damages" or $5,000 per violation.[206] Furthermore, the court can grant the prevailing plaintiff costs of the suit and attorney's fees.[207]

The California Attorney General or a district attorney can bring a criminal action against those who violate the statute.[208] Those who are found to have violated the statute may be fined up to $2,500 per violation.[209]

---

[200] CAL. BUS. & PROF. CODE § 22948 (West 2006).

[201] *Id.*

[202] *Id.* § 22948.2.

[203] *Id.* § 22948.3.

[204] *Id.* §§ 22948.3(a)(1), (2).

[205] *Id.* § 22948.3(a)(1).

[206] CAL. BUS. & PROF. CODE § 22948.3(a)(2).

[207] *Id.* § 22948.3(c)(2).

[208] *Id.* § 22948.3(b).

[209] *Id.*

The statute applies to any phisher that unlawfully interacts with California consumers or uses a California business's name or trademark to induce the consumers to provide their identifying information. To date, there is not a federal law that is similar.

V. CALIFORNIA CRIMINAL LAW AS IT RELATES TO PRIVACY

California has enacted several criminal statutes to aid in the protection of privacy. This section adresses the following topics: (1) invasion of Privacy Act, (2) protection of California citizens against identity theft: California Penal Code § 530.5, (3) computer crimes statute: California Penal Code § 502, and (4) criminal protection against unauthorized loan applications: California Penal Code § 530.8.

A. INVASION OF PRIVACY ACT: CALIFORNIA PENAL CODE §§ 630-637.9

The California Legislature enacted the Invasion of Privacy Act to "protect the right of privacy of the people of this state" and to prevent the use of "new devices and techniques for the purpose of eavesdropping upon private communications."[210] The Act bars unauthorized wiretaps,[211] the use of recording devices or unauthorized amplifying devices,[212] eavesdropping on cellular and cordless phones,[213] trespassing on property with the intent to commit any of the acts under banned under the statute,[214] selling or making eavesdropping equipment,[215] and the use of electronic tracking devices to determine a person's location.[216]

California cases have construed the Act broadly. California courts have held that the Act prohibits the recording of information without consent from all parties if the call includes a confidential

---

[210] CAL. PENAL CODE § 630 (West 2005).

[211] *Id.* § 631.

[212] *Id.* § 632.

[213] *Id.* §§ 632.6, 632.7.

[214] *Id.* § 634.

[215] *Id.* § 635.

[216] CAL. PENAL CODE § 637.7.

communication.[217] A "confidential communication" is a conversation in which a party to that conversation has an "objectively reasonable expectation that the conversation is not being overheard or recorded."[218] Furthermore, California courts have held that there does not have to be proof of actual damages to recover under the Act.[219] A plaintiff may recover up to $5000 for each incident.[220]

This Act is similar to the federal wiretapping statute called Title III of the Omnibus Crime Control and Safe Streets Act of 1968.[221] The federal wiretapping statute prohibits the intentional interception of wire, oral, or electronic communications.[222] It also prohibits the intentional or attempted use of devices to engage in interception of wire, oral, or electronic communications.[223] Finally, it bars the disclosure or use of unlawfully intercepted wire, oral, or electronic communications.[224] The federal wiretapping statute allows those people whose communications were unlawfully intercepted to file a civil suit and collect monetary damages, including punitive damages, and attorney's fees.[225]

Although the federal statute overlaps California's Invasion of Privacy Act, the federal statute does not preempt the Invasion of Privacy Act. The Supreme Court of California has held, "the federal act was not intended to occupy the entire field of wire communications and electronic surveillance to the exclusion of state regulation, and [where the state statute] does not impair the attainment of federal objectives, but rather aids in fulfilling the purposes of federal law," it

---

[217] Flanagan v. Flanagan, 41 P.3d 575, 576 (Cal. 2002); Turnbull v. ABC, No.03-3554, 2004 U.S. Dist. LEXIS 24351 (C.D. Cal. 2004).

[218] *Id.*

[219] Lieberman v. KCOP Television, 1 Cal. Rptr. 3d 536, 543 (Cal. Ct. App. 2003).

[220] *Id.*

[221] James X. Dempsey, *Communications Privacy in the Digital Age: Revitalizing the Federal Wiretap Laws to Enhance Privacy*, 8 ALB. L.J. SCI. & TECH. 65, 71 (1997).

[222] 18 U.S.C. § 2511 (2005).

[223] *Id.*

[224] *Id.*

[225] 18 U.S.C. § 2520 (2005).

should not be preempted by the federal law.[226] Therefore, both the federal wiretapping statute and California's Invasion of Privacy Act can be used to impose civil liability on violators.

B. PROTECTION OF CALIFORNIA CITIZENS AGAINST IDENTITY THEFT: CALIFORNIA PENAL CODE § 530.5

California has enacted a criminal provision to protect its citizens from identity theft. It states,

> [e]very person who willfully obtains personal identifying information, of another person, and uses that information for any unlawful purpose, including to obtain, or attempt to obtain, credit, goods, services, or medical information in the name of the other person without the consent of that person, is guilty of a public offense.[227]

The statute defines "personal identifying information" broadly, including everything from name and address, to credit card numbers, to unique biometric identifying information.[228]

If a person is convicted of violating this provision, that person can be punished with up to a year of county jail time, a fine of up to $1000, or both. If the offense is especially egregious, a person can be imprisoned in the state prison, fined up to $10,000, or both.[229]

This provision also tries to combat those who buy personal identifying information with the intent to do harm by making it a crime as well. The statute states, "[e]very person who, with the intent to defraud, acquires, transfers, or retains possession of the personal identifying information of another person is guilty of a public offense."[230] If a person is convicted of violating this provision, he or

---

[226] Tavernetti v. Superior Court of San Diego, 583 P.2d 737, 739 (Cal. 1978) (internal citation omitted).

[227] CAL. PENAL CODE § 530.5 (West 2005).

[228] *Id.*

[229] *Id.*

[230] *Id.*

she can be imprisoned in a county jail for up to a year, fined $1,000, or both.[231]

One court case interpreting this statute held that there does not have to be an intent to defraud to be found guilty under the statute.[232] Instead, the court said that "willfulness, coupled with use for an unlawful purpose, was sufficient mens rea" under the statute.[233] There is not a similar federal statute.

C. COMPUTER CRIMES STATUTE: CALIFORNIA PENAL CODE § 502

California created the computer crimes statute "to expand the degree of protection afforded to individuals, businesses, and governmental agencies from tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems."[234] The statute criminalizes many different acts of unauthorized computer access, including: (1) accessing a computer and altering or damaging it in an attempt to obtain money, (2) accessing a computer and stealing data, (3) accessing a computer altering computer data without the permission of the authorized user, and (4) accessing a computer and causing the computer to access the internet without the permission of the authorized used.[235]

A person convicted of crimes under this statute can be punished with fines and jail time.[236] The severity of the punishment depends on the severity of the crime committed.[237] A victim of these crimes also has the ability to bring a civil suit against the violator and can collect monetary damages and attorney's fees.[238]

---

[231] *Id.*

[232] People v. Hagedorn, 25 Cal. Rptr. 3d 879 (Cal. Ct. App. 2005).

[233] *Id.* at 887-888.

[234] CAL. PENAL CODE § 502(a) (West 2005).

[235] *Id.* § 502.

[236] *Id.*

[237] *Id.*

[238] *Id.*

This law is very similar to the federal Computer Fraud and Abuse Act.[239] This statute bars many acts of unauthorized access to computers including accessing computer records to: (1) obtain information, (2) accessing a computer in a way that would affect the U.S. government, (3) accessing a computer and altering the computer that causes damage to the computer or affects public safety or national security, and (4) accessing a computer with an attempt to commit fraud through internet commerce.[240]

Like the California provision, those convicted for violating these criminal provisions can be fined and sentenced to jail time.[241] The severity of the punishment varies with the severity of the offense. Also like the California provision, a victim can sue a violator in civil court.[242]

Although there have not been any court cases interpreting the preemptive effect of the Computer Fraud and Abuse Act, the California provision probably will not be preempted and those who act in ways that are illegal under both statutes may be subject to prosecution under both.

D. CRIMINAL PROTECTION AGAINST UNAUTHORIZED LOAN APPLICATIONS: CALIFORNIA PENAL CODE § 530.8

California Penal Code § 530.8 states that people who have unauthorized loan or credit applications in their names due to identity theft have the right to obtain information on the unauthorized transaction.[243] The victim of identity theft has the right to learn what types of information were used to open the account.[244] The victim also has the right to all paper records, records of telephone authorizations, and records of electronic authorizations.[245]

---

[239] 18 U.S.C. § 1030 (2005).

[240] *Id.*

[241] *Id.*

[242] *Id.* § 1030(g).

[243] CAL. PENAL CODE § 530.8 (West 2005).

[244] *Id.*

[245] *Id.*

If a business fails to comply, the victim can file a civil action and receive damages, injunctive relief, a penalty of up to $100 per day of noncompliance, and attorney's fees.[246]

Businesses that accept loan and credit applications from California residents will have to comply with this statute. There is no comparable federal statute.

VI. CALIFORNIA'S OFFICE OF PRIVACY PROTECTION

California was the first state to have an agency dedicated to promoting and protecting the privacy rights of consumers.[247] The California Office of Privacy Protection began in 2001.[248] The Office of Privacy Protection has four main goals: (1) to "assist individuals with identity theft and other privacy-related concerns;" (2) to "provide consumer education and information on privacy issues;" (3) to "coordinate with local, state and federal law enforcement on identity theft investigations;" and (4) to "recommend policies and practices that protect individual privacy rights."[249]

VII. CLOSING

In summary, this article has addressed five major topics: (1) California's constitutional right to privacy; (2) California's law on the collection and management of information in the medical field, in financial and banking institutions, and in the government; (3) California's new Internet and computer privacy laws; (4) California criminal law as it relates to privacy; and (5) California's Office of Privacy Protection. As I have discussed, the interplay between California's privacy laws and federal privacy laws is complex. Sometimes federal laws have a preemptive effect and sometimes they do not. Although this article has attempted to take a comprehensive view of California's privacy law and how it relates to federal privacy

---

[246] *Id.* § 530.8(d)(2).

[247] Office of Privacy Protection, About Us, http://www.privacy.ca.gov/cover/about.htm (last visited July 29, 2006).

[248] *Id.*

[249] *Id.*

law, it is not exhaustive.[250] Furthermore, this is not an exhaustive list of all types of preemption that may occur between the California privacy statutes and the federal privacy statutes as the law is continually and rapidly changing. For this reason, I would encourage readers, if they think that a statute may apply in a certain situation, to look to the statutes and case law for a more detailed analysis.

APPENDIX ON CALIFORNIA'S PRIVACY LAWS

CONSTITUTIONAL PROVISIONS

California Constitutional Right to Privacy
- http://www.leginfo.ca.gov/.const/.article_1

PROTECTION OF MEDICAL INFORMATION

Confidentiality of Medical Information Act (CMIA)
- http://www.privacy.ca.gov/code/cc56.htm?codesection=civ&codebody=&hits=20

California Civil Code § 1798.91
- http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1798.91

REGULATION OF BANKING AND FINANCIAL INSTITUTIONS

California Financial Information Privacy Act (FIPA)
- http://www.leginfo.ca.gov/cgi-bin/displaycode?section=fin&group=04001-05000&file=4050-4060

California Civil Code § 1798.29
- http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1798.25-1798.29

California Civil Code §§ 1798.80-1798.81
- http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1798.80-1798.84

California Civil Code § 1798.85
- http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&

---

[250] For an exhaustive list of California privacy provisions, visit the California Office of Privacy Protection at California Office of Privacy Protection, Privacy Laws, http://www.privacy.ca.gov/lawenforcement/laws.htm (last visited July 29, 2006).

group=01001-02000&file=1798.85-1798.86

California Civil Code §§ 1798.83-1798.84

- http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1798.80-1798.84

California Civil Code § 1799.1

- http://www.leginfo.ca.gov/cgi-bin/waisgate?WAISdocID=8460014315+21+0+0&WAISaction=retrieve

California Civil Code § 1785.20.3

- http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1785.20-1785.22

California Civil Code § 1788.18

- http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1788.10-1788.18

California Civil Code §§ 1798.92-1798.97

- http://www.leginfo.ca.gov/cgi-bin/waisgate?WAISdocID=8460674433+0+0+0&WAISaction=retrieve

REGULATION OF GOVERNMENT INFORMATION COLLECTION

Information Practices Act of 1977

- http://www.privacy.ca.gov/code/ipa.htm

PROTECTION OF ONLINE PRIVACY

Online Privacy Protection Act (OPPA)

- http://www.leginfo.ca.gov/cgi-bin/displaycode?section=bpc&group=22001-23000&file=22575-22579

Consumer Protection Against Computer Spyware Act

- http://www.leginfo.ca.gov/cgi-bin/displaycode?section=bpc&group=22001-23000&file=22947-22947.6

Anti-Phishing Act of 2005

- http://www.leginfo.ca.gov/cgi-bin/displaycode?section=bpc&group=22001-23000&file=22948-22948.3

CRIMINAL PROTECTION OF PRIVACY

Invasion of Privacy Act

- http://www.leginfo.ca.gov/cgi-bin/displaycode?section=pen&group=00001-01000&file=630-637.9

California Penal Code § 530.5

- http://www.leginfo.ca.gov/cgi-bin/displaycode?section=pen&group=00001-01000&file=528-539

California Penal Code § 502

- http://www.leginfo.ca.gov/cgi-bin/waisgate?WAISdocID=8455753634+1+0+0&WAISaction=retrieve

California Penal Code § 530.8

- http://www.leginfo.ca.gov/cgi-bin/displaycode?section=pen&group=00001-01000&file=528-539

OFFICE OF PRIVACY PROTECTION

Office of Privacy Protection

- http://www.privacy.ca.gov/index.html