Chapter 5

State Privacy Laws

Scott P. Cooper,
Navid Soleymani & Clifford S. Davidson
Proskauer Rose LLP

Tanya L. Forsheit*
InfoSecCompliance LLC

§ 5:1 Introduction
  § 5:1.1 Overview: Role of State Governments
  § 5:1.2 Origins of State Privacy Laws
    [A] Judicial—Torts and Crimes
    [B] Constitutional
    [C] Statutory
    [C][1] The California Invasion of Privacy Standard
  § 5:2 Online Privacy
    § 5:2.1 State Online Privacy Protection Statutes
      [A] California Online Privacy Protection Act (OPPA)
      [B] Other States
      [C] Related State Legislation Affecting Online Businesses
  § 5:3 Spyware
    § 5:3.1 California
    § 5:3.2 Other States Following California’s Approach
    § 5:3.3 Other States with More Limited Spyware Statutes
  § 5:4 Spam
    § 5:4.1 The Federal Statute and Preemption
    § 5:4.2 State Regulation of Spam

* The authors thank Adam Rottenberg for his assistance in the updating of this chapter.
§ 5:5 Identity Theft
§ 5:5.1 Laws Criminalizing Identity Theft
§ 5:5.2 Laws Allowing Victims to Initiate Investigations and/or Clear Their Names
§ 5:5.3 Rights of Action Against Perpetrators
§ 5:5.4 Protections and Rights of Action Against Debt Collectors
§ 5:5.5 Notice of Security Breach Legislation
[A] The California Framework
[B][1] “Material” Breach Necessary to Trigger Notification
[B][2] Expanded Definition of “Personal Information”
[B][3] Necessity to Notify Customers of a Breach of Non-Computerized Data
[B][4] Notification Procedures
[B][5] Duty to Notify Other Entities
[B][6] Duty of Non-Owners Maintaining Data
[B][7] Exemption from Notification for Entities in Compliance with GLBA
[B][8] Exemption from Notification for Encrypted Information
[B][9] Penalties for Violation
[B][11] State Credit Freeze Laws
§ 5:5.6 Data Security and Destruction Requirements
§ 5:6 Financial Privacy
§ 5:6.1 California Financial Information Privacy Act
§ 5:6.2 Other States
§ 5:6.3 Preemption
§ 5:6.4 Credit Card Transactions
[A] Restrictions on Merchants
[B] Prohibition on Disclosure of Marketing Information
§ 5:7 Privacy of Insurance-Related Information
§ 5:7.1 The National Association of Insurance Commissioners (NAIC) Model Acts
§ 5:7.2 Definitions of “Personal Information” and Similar Terms
§ 5:7.3 The GLBA Joint Marketing Exception and 2003 Model Act States
§ 5:8 Laws Governing Disclosure and Use of Social Security Numbers
§ 5:8.1 The California Framework
[A] Jurisdictional Modification to the California Framework
[A][1] Prohibiting SSNs in Customer Mailings
§ 5:1 Introduction

§ 5:1.1 Overview: Role of State Governments

This chapter provides an overview of the many and varied privacy laws enacted by the fifty states. It also identifies some of the areas in which the states’ efforts to enact legislation regarding privacy have conflicted with federal schemes, and have been preempted.

Of the fifty states, California has been far and away the most active in its efforts to enact laws protecting the privacy of its citizens, to enforce those laws, and to educate the public about individual privacy issues. California’s Office of Privacy Protection (COPP), created by statute in 2000,\footnote{1} describes its mission as promoting and protecting the privacy rights of California consumers.\footnote{2} In conjunction with the California Office of Information Security and Privacy Protection,\footnote{3} COPP maintains a website designed to educate citizens regarding their privacy rights under existing California law.\footnote{4} COPP also recommends best practices and other resources for businesses.

\footnote{1}{CAL. BUS. & PROF. CODE § 350 (West 2002, 2004).}
\footnote{2}{Id. §§ 350 & 352.}
\footnote{3}{The California Office of Information Security and Privacy Protection (OISPP) was established through S.B. 90 (2007), which took effect on January 1, 2008. See CAL. GOV’T CODE §§ 11549–11549.6. The OISPP website is located at www.oispp.ca.gov.}
\footnote{4}{See www.privacy.ca.gov. In October 2005, the California Department of Consumer Affairs issued a series of audio public service announcements (PSAs) as part of its ongoing efforts to combat identity theft and an expanded personal information and privacy protection public awareness campaign. See www.dca.ca.gov/press_releases/publications/2005/1017_copp.htm.}
Three other states—Colorado, New York, and Wisconsin—also have offices dedicated to information privacy and security. Colorado’s Office of Cyber Security was created by the governor and focuses on threats to electronic information systems. New York’s Office of Cyber Security and Critical Infrastructure Coordination has a similar focus. The Wisconsin Office of Privacy Protection was created by Governor Jim Doyle and focuses on issues of identity theft and consumer protection.

§ 5:1.2 Origins of State Privacy Laws

[A] Judicial—Torts and Crimes

The impetus for early state privacy protections, like much of privacy law, arose from the 1890 work of Samuel D. Warren and Louis D. Brandeis, The Right to Privacy. Prior to that time, the law only protected from intrusion or damage one’s physical self (assault and battery), one’s property (trespass), and one’s reputation (libel), but no specific legal basis existed for the protection of one’s privacy. Following the publication of Warren and Brandeis’s influential article, a number of judicial decisions involving causes of action for privacy violations were issued by state courts, starting in New York, that resulted in the eventual recognition of a tort-based right of privacy. These cases were in large part prompted by significant advances in the technologies of the day, such as photography and newspaper publication, and tended to involve tort claims arising from the publication of private facts or images by individuals or the news media.

In Roberson v. Rochester Folding Box Co., the New York Court of Appeals reversed a lower-court opinion finding that a complaint stated a cause of action based on the unauthorized use of the complainant’s likeness in a lithograph advertising. Chief Judge Parker’s majority found that the asserted “right to privacy” had “not as yet found an abiding place in our jurisprudence, and, as we view it, the doctrine cannot now be incorporated without doing violence to settled principles of law by which the profession and the public have long been guided.”

It was not until the 1905 Georgia Supreme Court case of Pavesich v. New England Life Insurance Co. that the highest court of any state

5. See www.colorado.gov/cybersecurity/ [last visited May 21, 2008].
6. See www.cscic.state.ny.us/ [last visited May 21, 2008].
7. See http://privacy.wi.gov/ [last visited May 21, 2008].
8. 4 HARV. L. REV. 193 (1890).
11. Id. at 447.
recognized a cause of action for invasion of privacy based on the unauthorized use of a likeness. The *Pavesich* court stated as follows:

The right of privacy within certain limits is a right derived from natural law, recognized by the principles of municipal law, and guaranteed to persons in this state both by the Constitutions of the United States and of the state of Georgia, in those provisions which declare that no person shall be deprived of liberty except by due process of law.

It therefore follows from what has been said that a violation of the right to privacy is a direct invasion of a legal right of the individual. It is a tort, and it is not necessary that special damages should have accrued from its violation in order to entitle the aggrieved party to recover.\(^{13}\)

After *Pavesich*, other state courts began to follow suit.\(^{14}\)

**[B] Constitutional**

The right to privacy achieved a constitutional footing with the Supreme Court’s landmark decision in *Katz v. United States*,\(^ {15}\) which confirmed a right to privacy in the context of Fourth Amendment searches and seizures. The *Katz* opinion is best known for Justice Harlan’s concurring opinion, which introduced the idea of reasonable expectation of privacy in the context of Fourth Amendment protection.

Following *Katz*, between 1968 and 1974, four states amended their constitutions to expressly incorporate the right of privacy into their search and seizure provisions.\(^ {16}\) For example, Hawaii amended its constitution to read: “The right of the people to be secure in their persons, houses, papers and effects against unreasonable searches, seizures and *invasions of privacy* shall not be violated. . . .”\(^ {17}\)

In addition to *Katz*, the Supreme Court’s decisions in *Griswold v. Connecticut*\(^ {18}\) and, later, *Roe v. Wade*\(^ {19}\) have had a significant effect on the development of privacy rights. Prior to these cases, privacy rights had been grounded upon more traditional notions, such as privacy in one’s home (that is, a “man’s home is his castle”) based on the Fourth Amendment.

---

13. *Id.* at 71, 73.
17. HAW. CONST. art. I, § 7 [emphasis added].
Amendment, privacy in thought associated with the First Amendment, and privacy against the disclosure of personal information founded in tort law. *Griswold* and *Roe* represented a significant expansion of privacy rights by finding a substantive right to privacy in the liberty clause of the Fourteenth Amendment.

*Griswold* and *Roe* prompted several states to amend their constitutions in the 1970s to include the right to privacy as a substantive right protected by the state constitution. The codification of privacy rights into state constitutions has allowed state courts, in certain circumstances, to expand the scope of privacy protections as compared to federal court interpretation of federal law. That state law may provide increased privacy protection was expressly contemplated by the Supreme Court in *Katz*, where Justice Stewart stated: “the protection of a person’s general right to privacy—his right to be let alone by other people—is, like the protection of his property and of his very life, left largely to the law of the individual States.”

Thus, for example, when the U.S. Supreme Court in *South Dakota v. Opperman* permitted warrantless inventory searches of impounded vehicles under the Fourth Amendment, state courts in South Dakota, Montana, and Alaska refused to interpret their state search and seizure analogues in the same fashion.

**[C] Statutory**

California’s reputation as a vanguard of the privacy field stems in part from article 1, section 1 of the state Constitution (the Declaration of Rights), which contains what is known as the Privacy Clause: “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.” The protections of the Privacy Clause are stronger than the privacy protections of the federal Constitution.

The words “and privacy” were amended to the Declaration of Rights by ballot initiative in 1972. According to electioneering materials, which are considered the authoritative source for interpreting the constitutional amendments, various ballot measures were approved by the voters in California, Montana, and Alaska.

---


intended meaning of the Privacy Clause, voters intended to protect a wide range of rights:

The right to privacy is the right to be left alone. It is a fundamental and compelling interest. It protects our homes, our families, our thoughts, our emotions, our expressions, our personalities, our freedom of communion, and our freedom to associate with the people we choose. . . . The right of privacy is an important American heritage and essential to the fundamental rights guaranteed by the First, Third, Fourth, Fifth, and Ninth Amendments to the U.S. Constitution. This right should be abridged only when there is compelling public need. 27

Although the Privacy Clause has been interpreted to protect both autonomy and informational privacy, 28 the ballot initiative focused principally on informational privacy:

Fundamental to our privacy is the ability to control circulation of personal information. This is essential to social relationships and personal freedom. The proliferation of government and business records over which we have no control limits our ability to control our personal lives. 28.1

California courts’ interpretations of the Privacy Clause have adhered to the ballot initiative proponents’ concerns. For example, in its groundbreaking decision in In re Marriage Cases, 28.2 the California Supreme Court ruled that the availability of domestic partnerships to same-sex couples could not substitute for marriage equality because, among other reasons, the existence of separate statuses gave rise to an inference of sexual orientation in myriad situations where such information is irrelevant:

Plaintiffs point out that one consequence of the coexistence of two parallel types of familial relationship is that—in the numerous everyday social, employment, and governmental settings in which an individual is asked whether he or she “is married or single”—an individual who is a domestic partner and who accurately responds to the question by disclosing that status will (as a realistic matter) be disclosing his or her homosexual orientation, even if he or she

28.1. Id.
would rather not do so under the circumstances and even if that information is totally irrelevant in the setting in question. 28.3

The Court found that facilitating such disclosure through a separate scheme of relationships was unacceptable because ordinarily, information about one’s sexual orientation is private and protected by the Privacy Clause. 28.4 Information about one’s sexual orientation, as well as other sensitive information, is protected by the Privacy Clause because public disclosure of such information exposes one to stigma. 28.5

[C][1] The California Invasion of Privacy Standard

In Hill v. National Collegiate Athletic Ass’n, 28.6 the California Supreme Court articulated its test for the invasion of privacy tort in California. At issue in Hill was defendant’s tort claim that being required to urinate in front of an NCAA drug testing official violated, among other things, his right to privacy. The Court reiterated the standard articulated in prior cases concerning state invasions of privacy:

Where the case involves an obvious invasion of an interest fundamental to personal autonomy, e.g., freedom from involuntary sterilization or the freedom to pursue consensual familial relationships, a “compelling interest” must be present to overcome the vital privacy interest. If, in contrast, the privacy interest is less central, or in bona fide dispute, general balancing tests are employed. 28.7

The Court then ruled that Privacy Clause violations are actionable as torts among private actors, 28.8 and articulated a three-part test:

The first essential element of a state constitutional cause of action for invasion of privacy is the identification of a specific, legally protected privacy interest. Whatever their common denominator, privacy interests are best assessed separately and in context. . . .

28.3. Id. at *217.
28.4. Id. at *217–*18.
28.7. Id. at 34.
28.8. Id. at 20.
The second essential element of a state constitutional cause of action for invasion of privacy is a reasonable expectation of privacy on plaintiff’s part. . . . A ‘reasonable’ expectation of privacy is an objective entitlement founded on broadly based and widely accepted community norms. . . .

Actionable 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. Thus, the extent and gravity of the invasion is an indispensable consideration in assessing an alleged invasion of privacy.28.9

To the extent other states recognize the invasion of privacy tort, those states track the elements of Hill’s three-part test.28.10 New York is a significant example of a state that does not recognize the common law invasion of privacy tort.28.11

As California has recognized, there can be no privacy without control over the dissemination of personal information.28.12 The Internet and other technology, as facilitators of information transfer, therefore pose a great privacy challenge.28.13 For the most part, this challenge has been taken up by the states; there exists no comprehensive federal privacy framework. The remainder of this chapter therefore addresses the major themes in state privacy legislation: Online privacy, Spyware, Spam, Identity Theft, Notice of Security Breach,

28.9. Id. at 35–37.
28.10. See, e.g., RESTATEMENT (SECOND) OF TORTS § 652D. State common law generally has incorporated the four privacy torts Dean William L. Prosser proposed in his seminal work Privacy: (1) intrusion into private matters; (2) public disclosure of private facts; (3) publicity placing a person in a false light; and (4) misappropriation of a person’s name or likeness. William L. Prosser, Privacy, 48 CAL. L. REV. 383, 389 (1960). See Hill, 7 Cal. 4th at 24 (noting that the Restatement (Second) and California law have incorporated the Prosser categories).
28.11. Messenger ex rel. Messenger v. Gruner + Jahr Printing & Publ’g, 94 N.Y.2d 436, 441 (N.Y. 2000). Like most states, however, New York provides a statutory cause of action for commercial use of one’s likeness without consent. N.Y. CIV. RIGHTS LAW §§ 50, 51 (2008); CAL. CIV. CODE § 3344 (2008) [prohibiting knowing commercial use of voice, signature, photograph or likeness without consent]. California also permits recovery of enhanced damages when one is injured by paparazzi or other snoopers. CAL. CIV. CODE § 1708.8.
28.12. See Hill, 7 Cal. 4th at 36 (“A particular class of information is private when well-established social norms recognize the need to maximize individual control over its dissemination and use to prevent unjustified embarrassment or indignity.”); Ballot Pamp., supra, note 27.
Financial Privacy, Privacy of Insurance-Related Information, Unsolicited Telephone Marketing and Electronic Eavesdropping.

§ 5:2  **Online Privacy**

§ 5:2.1  **State Online Privacy Protection Statutes**

[A]  **California Online Privacy Protection Act (OPPA)**

The California Online Privacy Protection Act of 2003 (OPPA),\(^{29}\) became effective on July 1, 2004. It was the first state law in the nation requiring operators of commercial websites or online services to post a privacy policy.

OPPA’s reach extends beyond California’s borders to require any person or company in the United States (and conceivably the world) that operates a website that collects personally identifiable information from California consumers to post a conspicuous privacy policy on its website.\(^{30}\) The statute does not apply, however, to third parties that operate, host, or manage websites or online services on behalf of another party.\(^{31}\) Given the limitless reach of the Internet, OPPA effectively functions as a national law, potentially impacting every commercial website that collects personally identifiable information from consumers.

“Personally identifiable information” means information collected online about an individual consumer, such as a consumer’s first and last names, physical address, email address, telephone number, Social Security number, or any other identifying information that permits a California consumer to be contacted physically or electronically.\(^{32}\)

OPPA requires that website operators “conspicuously post” a privacy policy on the website, which is satisfied if:

- The privacy policy appears on the homepage of the website or the first significant page after entering the website; or
- The privacy policy is hyperlinked to the homepage by an icon or text link that contains the word “privacy,” and is in a color different from the background of the homepage.\(^{33}\)

The privacy policy must contain all of the following features:

- Identify the categories of personally identifiable information the operator collects;

---

30.  *Id.* § 22575[a].
31.  *Id.* § 22577[c].
32.  *Id.* § 22577[a].
33.  *Id.* § 22577[b].
• Identify the categories of third parties with whom the operator may share such personally identifiable information;

• Describe the process by which a consumer can review and request changes to his or her personally identifiable information collected by the operator, if such process exists;

• Describe the process by which the operator notifies consumers of material changes to the operator’s privacy policy; and

• Identify the effective date of the privacy policy.  

An operator has thirty days to post a privacy policy after being notified of its noncompliance.  

An operator who fails to post a privacy policy, or fails to comply with the terms of its posted policy, is in violation if its noncompliance is either [1] negligent and material, or [2] knowing and willful (that is, regardless of the materiality of the violation).  

OPPA does not contain any enforcement provisions. However, OPPA presumably could be enforced through California’s Unfair Competition Law (UCL), though there are no judicial decisions to date. Under the UCL, both private plaintiffs and government officials can file suit for unlawful, unfair, or fraudulent business practices. California courts have held that a business practice that violates another state law can serve as a predicate for a UCL claim. Private plaintiffs who are injured by the violation may state claims under the UCL and recover restitution and obtain injunctive relief. Government officials can also recover civil penalties. Claims under the UCL are often used as the basis for class actions.

[B] Other States

California is the only state that has enacted a statute requiring all website operators that collect personally identifiable information to post and comply with privacy policies.

Two states, Nebraska and Pennsylvania, have amended their unfair business practices statutes to provide that knowingly making a false or

34. Id. § 22575(b).
35. Id. § 22575(a).
36. Id. § 22576.
37. Id. § 17200 et seq.
37.1 The only case filed to date alleging an OPPA violation is Doe v. Network Solutions, LLC, No. 07-CV-05115 [JSW] [N.D. Cal. 2007]. The case was dismissed in January 2008 based on improper venue.
40. Id. § 17206.
misleading statement in a privacy policy gives rise to a claim under each state’s unfair business practices act.\footnote{41}

Two other states, Minnesota and Nevada, have enacted laws that impose confidentiality requirements on Internet service providers with respect to their subscribers. Minnesota requires Internet service providers to maintain the confidentiality of their customers’ personally identifiable information. Under the Minnesota statute, “personally identifiable information” means information that identifies:

1. a consumer by physical or electronic address or telephone number;
2. a consumer as having requested or obtained specific materials or services from an Internet service provider;
3. Internet or on-line sites visited by a consumer; or
4. any of the contents of a consumer’s data storage devices.\footnote{42}

A consumer who prevails in an action brought under this statute is entitled to an award of $500 or actual damages, whichever is greater, and may also recover costs and attorneys’ fees.\footnote{43}

Nevada requires Internet service providers to maintain the confidentiality of “all information” concerning their subscribers.\footnote{44} Providers must also maintain the confidentiality of a subscriber’s email address upon the subscriber’s request. The statute requires the Internet service provider to provide notice of these requirements, including a conspicuous statement that the subscriber may request to have his or her email address be kept confidential. Internet service providers who violate this section can be fined $50 to $500 for each violation.\footnote{45}

[C] Related State Legislation Affecting Online Businesses

California and Utah have enacted legislation that, though not specifically targeted to online businesses, require businesses to notify

\footnote{41. NEB. REV. STAT. § 87-302(14) (a person engages in a deceptive trade practice when he or she “[k]nowingly makes a false or misleading statement in a privacy policy, published on the Internet or otherwise distributed or published, regarding the use of personal information submitted by members of the public”); 18 PA. CONS. STAT. § 4107(a)(10) (“A person commits an offense if, in the course of business, the person . . . knowingly makes a false or misleading statement in a privacy policy, published on the Internet or otherwise distributed or published, regarding the use of personal information submitted by members of the public.”).}

\footnote{42. MINN. STAT. ANN. § 325M.01(5) (2006).}

\footnote{43. Id. § 325M.07.}

\footnote{44. NEV. REV. STAT. ANN. § 205.498 (2006).}

\footnote{45. Id.}
consumers whenever they intend to disclose personal information about the consumer to a third party for direct marketing purposes or for compensation. The Utah statute provides that a business may not disclose nonpublic personal information about a consumer to a third party for compensation, unless it provides a notice to the consumer that reads substantially as follows: “We may choose to disclose nonpublic personal information about you, the consumer, to a third party for compensation.” Businesses that violate this statute can be held liable for $500 for each occurrence and court costs.

The California statute, informally known as the Shine the Light law, requires covered businesses to disclose to California customers, upon request, the categories of personal information disclosed to third parties for direct marketing purposes, as well as the names and addresses of the third parties. As an alternative, a company can comply with the statute by implementing a privacy policy that allows consumers to opt-in or opt-out of information sharing. The statute also contains an exception for certain disclosures between financial institutions and businesses with co-branded credit cards. Consumers who are harmed by violations of this statute may sue to recover damages, civil penalties of between $500 and $3,000 per occurrence, and attorneys’ fees.

§ 5:3 Spyware

As defined by the California State Senate, spyware is “as an executable computer software program installed without a computer user’s knowledge by a software manufacturer, software controller, or web site operator which either: (1) gathers and transmits personal information or data regarding computer usage; or (2) operates in a manner that is intended to confuse or mislead the user concerning the identity of the person or entity responsible for the performed functions or contents displayed.” A number of states, including California, have passed laws to combat spyware.

§ 5:3.1 California

The California Consumer Protection Against Computer Spyware Act prohibits an unauthorized user from willfully loading software

47. Id. § 13-37-203.
49. Id.
49.1. Id. § 1798.83(d)(5).
50. Id. § 1798.84.
onto the computer of a California resident and using the software to do any of the following:

- Modify, through intentionally deceptive means, certain settings related to the computer’s access to or use of the Internet;
- Collect, through intentionally deceptive means, certain types of personally identifiable information;
- Prevent, through intentionally deceptive means, an authorized user’s reasonable efforts to block the installation of or disable software;
- Intentionally misrepresent that the software will be uninstalled or disabled by an authorized user’s action;
- Remove, disable, or render inoperative, through intentionally deceptive means, antispyware, or antivirus software installed on the computer;
- Take control of the computer by
  1. causing emails or viruses to be transmitted or relayed from the computer;
  2. causing the authorized user to incur charges for unauthorized services;
  3. using the computer as part of an activity performed by a group of computers for purpose of causing damage to another computer (such as a denial-of-service attack); or
  4. allowing multiple, sequential, stand-alone advertisements to be opened on the computer such that a reasonable user cannot close the advertisements without turning off the computer or closing the Internet browser.52

The law also prohibits inducing computer users to install a software component by intentionally misrepresenting that it is necessary for security or privacy or in order to open, view, or play a particular type of content.53

There are no enforcement provisions in the California Consumer Protection Against Computer Spyware Act. Presumably, the statute can be enforced through actions under the California Unfair Competition Law,54 though no judicial decision applying it has been published to date.

52. CAL. BUS. & PROF. CODE §§ 22947.2, 22947.3 (2006).
53. Id. § 22947.4.
54. Id. § 17200 et seq.
§ 5:3.2 Other States Following California’s Approach

Thirteen states at the time of publication have enacted statutes that mirror the core provisions of the California Consumer Protection Against Computer Spyware Act.  

A key difference between the California statute and the statutes of these states is that some of the other statutes contain specific enforcement provisions. For example, Arizona law provides that the state Attorney General may seek injunctive relief and recover the greater of actual damages or $100,000 for each violation. Computer software providers and website and trademark owners affected by a violation of law also may bring suit.

Arkansas’ Consumer Protection Against Computer Spyware Act provides that violations will be punished by the Attorney General under the state’s deceptive trade practices act, with any penalties and fines deposited into the Spyware Monitoring Fund and used for enforcement and educational activities.

The Georgia Computer Security Act of 2005 is similar to California’s statute, but it authorizes the Attorney General to bring a civil action to recover between $100 and $100,000 for each violation. Internet service providers and telecommunications carriers damaged as a result of the unlawful conduct may bring private causes of action. The statute also provides for criminal penalties.

The Indiana statute provides that a provider of computer software, the owner of a website, or the owner of a trademark who is adversely affected by reason of the violation may bring a civil action against a person who violates the statute to enjoin further violations and recover the greater of actual damages or $100,000.

The Iowa statute provides for criminal penalties, but does not explicitly provide for a private right of action.


58. Id. § 4-111-105.


60. Id. § 16-9-155 to -156.


The Louisiana statute provides for criminal penalties, but allows for civil relief. The Attorney General, a computer software provider, a trademark owner, or an Internet service provider may bring an action against a person who violates the statute for actual damages and injunctive relief.\textsuperscript{63}

Under the New Hampshire statute, violations are Class A misdemeanors.\textsuperscript{64}

Texas allows the following particular groups of injured persons to bring private suits against violators: computer software providers, webpage or trademark owners, telecommunications carriers, cable operators, and Internet service providers. Such plaintiffs can recover the greater of actual damages or $100,000 for each violation, as well as injunctive relief and attorneys’ fees. The Attorney General can recover civil penalties in the amount of $100,000 for each violation.\textsuperscript{65}

Finally, the Washington statute\textsuperscript{66} provides that the Attorney General, or a computer software provider or a website owner, may bring an action against a person who violates the statute and recover either actual damages or $100,000, whichever is greater. The court can increase the damages by three times if the person has engaged in a pattern and practice of violating the statute.\textsuperscript{67}

\section*{§ 5:3.3 Other States with More Limited Spyware Statutes}

At least two other states, Alaska and Utah, have enacted statutes that are intended only to ban spyware that causes “pop-up advertisements.”

Alaska law defines a pop-up advertisement as “material offering for sale or advertising the availability or quality of a property, good, or service that is displayed on a user’s computer screen, without any request or consent of the user, separate from an Internet site that a user intentionally accesses.”\textsuperscript{68} The Alaska statute prohibits using spyware to cause a pop-up advertisement to appear on the computer screen of a user if the pop-up advertisement is displayed in response to a user accessing a specific website address or mark, unless it is done with the consent of the owner of the Internet site or the mark.\textsuperscript{69}

\begin{flushright}
\textsuperscript{63} \textit{LA. REV. STAT. ANN.} §§ 51:1441 to :1449 (2006). \\
\textsuperscript{64} \textit{N.H. REV. STAT. ANN.} §§ 359-H:2 to :3 (2006). \\
\textsuperscript{65} \textit{TEX. BUS. & COM. CODE ANN.} §§ 48.101, 48.102 (2006). \\
\textsuperscript{66} \textit{WASH. REV. CODE ANN.} §§ 19.270.010 et seq. (2006). \\
\textsuperscript{67} \textit{Id.} § 19.270.060. \\
\textsuperscript{68} \textit{ALASKA STAT.} § 45.45.798 (2005). \\
\textsuperscript{69} \textit{Id.} § 45.45.792.
\end{flushright}
Violations of this statute are actionable under the state’s unfair business practices statute.70 Utah law defines a pop-up advertisement as material:

(a) offering for sale or advertising the availability or quality of a commercial property, good, or service; and

(b) that is displayed:

[i] separate from an Internet website;

[ii] as a result of a user accessing an Internet website;

[iii] in a manner that covers paid advertising or other content on an Internet website in a way that interferes with the user’s ability to view the advertising or other content that the user attempted to originally access; and

[iv] without the authority of the operator of the Internet website.71

The Utah statute prohibits using spyware to cause pop-up advertisements if the advertisement is displayed in response to a user accessing a specific website address or mark, unless it is done with the consent of the owner of the Internet site or the mark. There is no violation of the statute if the spyware purveyor first requests information about the user’s state of residence and the user indicates a residence outside Utah.72 Private plaintiffs may recover the greater of actual damages or up to $500 for each violation, as well as treble damages and attorneys’ fees if the defendant willfully or knowingly violated the law.73

§ 5:4 Spam

The term “spam” refers to unsolicited emails, typically sent by online marketers in mass quantities for advertising purposes. Spam has also been linked with fraudulent business schemes, chain letters, and offensive sexual and political messages. The problems associated with spam range from the inconvenience and annoyance they cause to email users, to damage to the hardware and networks that make up the Internet. Spam has been widely criticized as being the cause of a significant drain on time and money, clogging available bandwidth, and damaging confidence in email as an effective communication tool. Fraudulent and pornographic spam messages also pose risks

70. Id. § 45.50.471[b].
72. Id. § 13-40-201.
73. Id. § 13-40-301.
to the elderly and children, and anyone who may be vulnerable to email scams.\(^4\)*

Responding to these concerns, state and federal lawmakers have acted to regulate or ban spam. Prior to enactment of the federal anti-spam law, commercial email was regulated by a collection of state laws. Nevada became the first state to pass an anti-spam law in 1997. Thirty-seven states now have such laws. The specific provisions in these laws vary widely, but most of the statutes share the common goals of eliminating fraud in commercial email and reducing the overall volume of spam received by email users.\(^5\)*

Congress passed the federal Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM),\(^6\) after several states enacted more restrictive, and sometimes conflicting, statutes. As discussed below, CAN-SPAM preempts the state laws in many (but not all) respects.

§ 5:4.1 The Federal Statute and Preemption

Relevant to the present discussion of state law, CAN-SPAM contains a preemption section intended to supersede analogous state laws in many respects. The preemption section states as follows:

\(^1\) IN GENERAL
This Act supersedes any statute, regulation, or rule of a State or political subdivision of a State that expressly regulates the use of electronic mail to send commercial messages, \(\text{except to the extent that any such statute, regulation, or rule prohibits falsity or deception in any portion of a commercial electronic mail message or information attached thereto.}\)

\(^2\) STATE LAW NOT SPECIFIC TO ELECTRONIC MAIL.
This Act shall not be construed to preempt the applicability of—

(A) State laws that are not specific to electronic mail, including State trespass, contract, or tort law; or

(B) other State laws to the extent that those laws relate to acts of fraud or computer crime.\(^7\)

There is some uncertainty with respect to the scope of federal preemption. On the one hand, the first clause of subsection \(^1\) purports to supersede all state laws that expressly regulate the use of emails to send commercial messages. On the other hand, the

---

\(^5\) Id. at 976–77; see also COLO. REV. STAT. § 6-1-702.5 (2008).
\(^7\) 15 U.S.C. § 7707[b] [emphasis added].
subsequent clause of subsection (1) provides that state laws prohibiting “falsity or deception” in email messages are not preempted. The practical impact of the Act’s preemptive scope is unclear in the absence of judicial interpretation of these two clauses and the effects of specific state laws. It also is unclear whether, under subsection (2), Internet Service Providers and/or spam recipients can state claims under state trespass, contract, or tort law against spam purveyors. The scope of CAN-SPAM’s preemption is significant, among other reasons, because the Act does not authorize suit by consumers and businesses who receive spam, as many state laws permit; rather, the Act authorizes suit only by a provider of “Internet access service.”

A number of federal district courts have addressed CAN-SPAM’s preemptive scope. In Gordon v. Impulse Marketing Group, Inc., the Eastern District of Washington concluded that the Washington anti-spam statute is not preempted to the extent that the statute prohibits falsity and deception in sending unsolicited commercial emails. The plaintiff in that case was a Washington resident and the registered user of an Internet domain name. He alleged that the defendant sent unsolicited commercial emails to various addresses at his domain. He sued under Washington’s Commercial Electronic Mail Act, which, among other things, prohibits using a third party’s Internet domain name without permission, misrepresenting any information in identifying the point of origin or the transmission path of the email, and using false or misleading information in the subject line. The court held that because these provisions prohibit falsity or deception, they are not

78. A series of federal court decisions, beginning with CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015 (S.D. Ohio 1997), has approved the use of trespass to chattels as a basis on which Internet service providers (but not email recipients) can recover against purveyors of spam, based upon evidence that the vast quantities of email sent by spammers overburdened the ISP’s computer system and made the computer system harder to use for the ISP’s customers. See also Hotmail Corp. v. Van$ Money Pie, Inc., 1998 WL 388389 (N.D. Cal. Apr. 16, 1998); Am. Online, Inc. v. IMS, 24 F. Supp. 2d 548 (E.D. Va. 1998); Am. Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444 (E.D. Va. 1998). On the other hand, the California Supreme Court rejected a trespass to chattel claim asserted by Intel against a former employee who sent numerous emails criticizing Intel to numerous current employees. Intel v. Hamidi, 71 P.3d 296 (Cal. 2003). The court distinguished the cases cited above on the ground that Intel had not shown that unsolicited emails from one employee impaired or damaged its computer system. Trespass to chattels “does not encompass, and should not be extended to encompass, an electronic communication that neither damages the recipient computer system nor impairs its functioning.” Id. at 1347.

preempted by federal law and the plaintiff could state a claim under the state law.

The Northern District of California also took up the issue in Facebook, Inc. v. ConnectU LLC. Facebook alleged that ConnectU unlawfully collected email addresses of Facebook’s registered users and then sent them commercial email, encouraging them to switch to ConnectU. Among its claims, Facebook alleged that ConnectU violated California Business and Professions Code sections 17529.4 and 17538.45—two state statutes that regulate the transmission of unsolicited commercial emails. The court held that the California statutes are preempted by CAN-SPAM because they do not “purport to regulate false or deceptive email, or require such falsity or deception as an element of the statutory violation.”

In a separate case, the Northern District dismissed (with leave to amend) claims against Reunion.com brought under California’s anti-spam law because the plaintiff failed to allege with sufficient particularity that “forward-to-a-friend” emails were fraudulent or deceptive. In the absence of a cause of action for fraud or deceit, the complaint had to be dismissed because CAN-SPAM pre-empted the California anti-spam statute to the extent it applied to non-fraudulent or non-deceptive emails.

Most recently as of May 1, 2009, the Southern District of Ohio held that Ohio’s anti-spam statute was pre-empted to the extent that it included penalties for inadvertent misstatements in advertisements, but was not pre-empted to the extent that it penalized “falsity and deception” in email and other commercial activities.

The District of Maryland utilized a different approach to analyze the preemption question in Beyond Systems, Inc. v. Keynetics, Inc. Unlike the approach in Gordon and Facebook, the court in Beyond Systems, Inc. did not base its decision on whether the state statute prohibited falsity or deception. Rather, the court held that the state statute was not preempted at all because its goals were “in no way inconsistent with CAN-SPAM. At most it supplements the federal law... Given that sort of compatibility between state and federal law, the preemption doctrine does simply does not apply.”

81.1. Id. at 1094.
81.5. Id. at 538.
It is unclear whether courts will adopt the reasoning in *Beyond Systems, Inc.* and conclude that state anti-spam statutes are not prohibited to the extent their aims are consistent with CAN-SPAM, or whether the courts will follow the approach taken by the courts in *Gordon* and *Facebook* and conclude that the only state statutes that survive the CAN-SPAM preemption provision are those that require falsity or deception as an element of the statutory violation. As of May 1, 2009, the Ninth Circuit Court of Appeals was considering whether CAN-SPAM preempts California’s anti-spam law (discussed below), which bans unsolicited commercial email containing falsified or misrepresented header information. On January 28, 2009, the circuit court stayed the appeal and asked the California Supreme Court to determine whether California’s anti-spam statute, Business and Professions Code section 17529.5(a)(2), prohibits email marketers from sending emails from multiple domain names in order to bypass spam filters. On June 27, 2010, the California Supreme Court held that it is not unlawful to send commercial email advertisements from multiple domain names for the purpose of bypassing spam filters.

§ 5:4.2 State Regulation of Spam

This section summarizes the categories of substantive anti-spam rules that states have enacted, and the likelihood that these categories are likely to be found to be preempted by the federal statute.


Opt-in provisions require a recipient to specifically assent to receiving email advertising messages. Enacted thus far by California and Delaware, they are considered the strongest anti-spam provisions because, in essence, they prohibit receiving unsolicited bulk commercial emails. They are preempted by CAN-SPAM, however, as they “expressly regulate[ ] the use of electronic mail to send commercial messages” and do not fall within the exception for laws prohibiting falsity or deception.


Opt-out provisions are far more common and require that spam senders include a mechanism allowing recipients to opt-out of receiving subsequent messages. These provisions exist in over twenty states,

---

83. DEL. CODE ANN. tit. 11 § 937 (2005).
84. 15 U.S.C. § 7707(b).
though different states have different opt-out mechanisms. Like the opt-in provisions, they, too, appear to be preempted by CAN-SPAM.

[C] Subject-Line Labeling Requirements

Some states have enacted provisions that require particular labels in the subject line of the messages (for example, ADV for advertisements or ADV:ADLT for adult messages). These labeling provisions appear to be preempted by CAN-SPAM. Although CAN-SPAM does not itself have a labeling requirement, it grants the Federal Trade Commission rule-making authority to implement the Act. FTC rules require that sexually explicit spam be labeled “SEXUALLY-EXPLICIT” in the subject line.

[D] Provisions Prohibiting False or Misleading Practices

Provisions that prohibit false or misleading practices in sending spam are not preempted by CAN-SPAM because they fall squarely within the preemption section’s “falsity or deception” savings clause. Recent cases are split as to whether this savings clause applies only to common-law fraud claims.


86. ALASKA STAT. § 45.50.479 (2005); ARIZ. REV. STAT. ANN. § 44-1372.01 (2006); ARK. CODE ANN. § 4-88-603 (2005); COLO. REV. STAT. § 6-1-702.5 (2008) [effective Aug. 5, 2008]; CONN. GEN. STAT. § 52-570c(b) (2006); 815 ILL. COMP. STAT. 511/10 (2005); IND. CODE § 24-5-22-8 (2005); KAN. STAT. ANN. § 50-6,107 (2005); LA. REV. STAT. ANN. § 51:1741.1 (2005); ME. REV. STAT. ANN. tit. 10, § 1497 (2005); MICH. COMP. LAWS § 445.2503 (2005); MO. REV. STAT. § 407.1138 (2005); NEV. REV. STAT. § 41.730 (2004); N.M. STAT. ANN. § 57-12-23 (2005); N.D. CENT. CODE § 51-27-04 (2005); OHIO REV. CODE ANN. § 2307.64 (2005); OKLA. STAT. tit. 15, § 776.6 (2006); 73 PA. CONS. STAT. § 2250.3 (2005); R.I. GEN. LAWS § 6-47-2 (2004); TENN. CODE ANN. § 47-18-2501 (2005); TEX. BUS. & COM. CODE ANN. § 46.003 (2005); WIS. STAT. § 944.25 (2005).


practices that are prohibited by state statutes include false or misleading subject lines, false routing information, and the use of false third-party return addresses or domain names. Most states have banned at least one of these practices. It is expected that these statutes (and the remedies provided thereunder) will become increasingly important tools in the fight against spam. However, to the extent such statutes broadly prohibit any unsolicited bulk email, they might be subject to challenge on free speech grounds. The Virginia Supreme Court recently struck down Virginia’s criminal prohibition on unsolicited bulk email as an unconstitutional burden on anonymous speech.

[E] Bans on Selling Software That Can Be Used to Falsify Routing Information

Finally, some states ban the sale of software designed to falsify routing information or return addresses. These provisions are not preempted because they apply to the sale of software, rather than the use of electronic mail to send commercial messages.

§ 5:5 Identity Theft

Identity theft is a crime in which an imposter obtains key pieces of information such as Social Security and driver’s license numbers and uses them for his or her own personal gain.


(Proskauer, Rel. #4, 7/10) 5–23
§ 5:5.1  Laws Criminalizing Identity Theft

Almost all states have passed laws that make identity theft a specific crime. The statutes generally define the crime as intentionally and fraudulently using the personal identifying information of another person to obtain credit, money, goods, or services without the person’s consent. Most statutes provide that identity theft is a misdemeanor punishable by fine and/or imprisonment, though some states allow felony charges to be brought if certain aggravating factors are present.

California law, for example, makes it a misdemeanor to willfully obtain the personal identifying information of another person and to use that information for any unlawful purpose, which includes obtaining credit, goods, services, or medical information, in the name of the other person without his or her consent. Violations of the statute are punishable by up to one year imprisonment and/or a fine of up to $10,000.

Many statutes also provide that the court may order the offender to make restitution to the victim, which typically includes financial losses caused by the violation, attorneys’ fees and costs incurred by the victim in clearing his or her credit history or defending actions brought by third parties, and any judgments incurred by the victim arising out of the offense.


In addition to criminal penalties, some states have enacted laws that provide identity theft victims the rights to obtain a police report, to seek a court order clearing his or her name, and/or to obtain the cooperation of financial institutions in resolving disputes arising out of identity theft.

Some states require that a law enforcement agency initiate an investigation and prepare a police report, upon a request by an identity theft victim. One state explicitly provides that the police report constitutes prima facie evidence that the identifying information was used without the person’s permission.

Two states provide that a person may petition a court for an expedited judicial determination that he or she was a victim of identity theft. A court that issues a determination of factual innocence may order the names and personal identifying information contained in court records and files to be deleted, sealed or labeled “to show that the data is impersonated and does not reflect the defendant’s identity.” Yet other states provide that, after an offender is convicted, the “sentencing court” may issue an order to correct a public record that contains false information as a result of identity theft, and at least one state allows the victim to use this court order as proof that any accounts that were created or altered were done as a result of identity theft.

California law also imposes a duty on banks, credit unions and certain other entities to cooperate with identity theft victims. If a person discovers that an application has been filed for credit or an account has been opened under his/her name without permission, the identity theft victim may obtain, from the entity with which the application was filed, information related to the application or account.

---


94. 18 PA. CONS. STAT. § 4120 (2005).

95. CAL. PENAL CODE § 530.6(b)-(c) (2005); 720 ILL. COMP. STAT. 5/16G-30 (2005).


and the categories of identifying information that the imposter used to complete the application or to open the account. 98

§ 5:5.3  Rights of Action Against Perpetrators

Several states have enacted statutes that allow victims of identity theft to assert claims against perpetrators and to recover amounts far greater than the actual damages they incurred.

For example, four states allow an identity theft victim to recover $5,000 for each incident or three times the actual damage, whichever is greater, in addition to attorney fees. 99 Connecticut allows a victim to recover $1,000 for each incident or three times the actual damage, whichever is greater, in addition to attorney fees. 100 Georgia allows the victim to recover treble damages plus attorneys’ fees. 101

§ 5:5.4  Protections and Rights of Action Against Debt Collectors

California has enacted legislation that protects victims of identity thefts against claims that arise from transactions procured through such thefts. These protections may be used both defensively and offensively. An identity theft victim who is sued for non-payment of the debt may file a cross-complaint against the claimant to establish that the debt was procured by identity theft. 102 The person also may bring an action against a claimant to establish that he or she is a victim of identity theft with respect to the claim at issue. The statute allows the identity theft victim to obtain declaratory and injunctive relief, actual damages and attorney fees against the claimant. Further, a civil penalty of up to $30,000 may be imposed if the person establishes that he or she gave thirty days’ notice to the claimant about facts relating to the identity theft, the claimant failed to diligently investigate the facts after receiving the notification, and the claimant continued to pursue the claim after being presented with facts that were later held to entitle the victim to a judgment pursuant to this section. 103

California law also requires a debt collector to cease collection activities upon receipt of a police report alleging that the debtor is a victim of identity theft and the debtor’s written statement that he or

99. ALA. CODE § 13A-8-199 (2005); IOWA CODE § 714.16B (2005); MO. REV. STAT. § 570.223 (2005); N.C. GEN. STAT. § 1-539.2C (2005).
100. CONN. GEN. STAT. § 52-571h (2006).
103. Id.
she is a victim of identity theft with respect to the debt being collected. Upon receipt of the information, the debt collector must review and consider all of the information provided by the debtor and other pertinent information in its files or from the creditor. The debt collector may recommence debt collection activities only upon making a good faith determination that the information does not establish that the debtor is not responsible for the specific debt in question. The debt collector must notify the consumer in writing of that determination and its basis before proceeding with any further collection activities.

§ 5:5.5 Notice of Security Breach Legislation

Beginning in 2002, legislators across the country began passing laws requiring consumer notification when there is a security breach involving private information. These laws were in response to consumer fears of identity theft, heightened by highly publicized data security breaches. As of May 5, 2010, forty-six states, the District of Columbia, Puerto Rico, and the U.S. Virgin Islands have passed security breach notification laws affecting private entities. Oklahoma passed a similar law applicable only to state agencies. The laws largely follow California’s first-in-the-nation data security breach notification law; however, there are key differences and compliance requirements between jurisdictions.

Federal legislation, which would preempt the patchwork quilt of state laws and create a uniform national standard, has been seriously considered since 2005; however, a general breach notification statute has not passed as of April 23, 2010.

[A] The California Framework

The Security Breach Information Act, commonly referred to by its bill number S.B. 1386, was the first law passed in the United States that requires notification to customers for security breaches of personal information. The California law, and most state security breach notification schemes, require notification to individuals after a “breach of the security of the system.” A “breach of the security of the system” means unauthorized acquisition of computerized data that

104. Id. § 1788.18 (2006).
105. Id.
107. OKLA. STAT. tit. 74, § 3113.1.
108. CAL. CIV. CODE § 1798.82 et seq.
109. Id. § 1798.82[a].
compromises the security, confidentiality, or integrity of personal information that is maintained by the person or business experiencing the breach.\textsuperscript{110} Good-faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not considered a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.\textsuperscript{111} A non-owner maintaining data on behalf of an owner must notify the owner of any data security breach immediately upon the discovery of the occurrence of the breach.\textsuperscript{112}

Personal information in California is defined as the first name or initial and last name of an individual, with one or more of the following, when either the name or the data elements are not encrypted: Social Security number, driver’s license number, credit card or debit card number, a financial account number with information such as PINs, passwords, or authorization codes that could gain access to the account or medical or health insurance information.\textsuperscript{113} Publicly available information that is lawfully made available from federal, state, or local government records is not considered personal information.\textsuperscript{114}

Subsequent sections of the California Code provide for certain exemptions from the disclosure requirements. One broad exemption is for personal information in encrypted form.\textsuperscript{115} Encryption is not defined. Although some might argue that a simple password may qualify for the exemption, the trend is clearly toward more sophisticated protection, and the common definition of encryption requires transformation of data into unreadable form.\textsuperscript{116} The second exemption allows for delayed notice when there is an ongoing criminal investigation by law enforcement.\textsuperscript{117} Other states have developed exemptions for

\begin{footnotesize}
\begin{enumerate}
\setcounter{enumi}{109}
\item Id. § 1798.82(d).
\item Id.
\item Id. § 1798.82(b).
\item Id. § 1798.82(e). On October 14, 2007, Governor Schwarzenegger approved A.B. 1298 to add medical and health insurance information to the list of personal information elements. “Medical information” means any information regarding an individual’s medical history, mental or physical condition, or medical treatment or diagnosis by a healthcare professional. “Health insurance information” means an individual’s health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual’s application and claims history, including any appeals records. Most other states do not formally recognize medical or health insurance information as “personal information.” But see ARK. CODE ANN. § 4-110-103(5).
\item CAL. CIV. CODE § 1798.82(f).
\item See id. §§ 1798.82[a], [e].
\item See infra section 5:5.5[B][8].
\item CAL. CIV. CODE § 1798.82[c].
\end{enumerate}
\end{footnotesize}
Unauthorized access to information from government agencies or entities that are already regulated under federal privacy laws (for example, FERPA, GLBA, or HIPAA).

California requires notification in the “most expedient time possible and without unreasonable delay,”118 either in writing or electronically, if the electronic notice is consistent with federal e-sign standards, which require consumers to consent to the receipt of electronic notice.119 If a company can show that the cost of notification will exceed $250,000, more than 500,000 people are affected, or the individual’s contact information is unknown, then notice may be effected through “substitute notice” consisting of a direct email to the customer, conspicuous posting on a company website, and notification to major statewide media.120

Beyond the statutory requirements, the State of California Department of Consumer Affairs and the California Office of Privacy Protection121 have developed “Recommended Practices,” which serve as useful guidance for notification procedures in multiple jurisdictions.122 The Recommended Practices also include guidance on data protection, prevention of a security breach, and preparing incident response plans. While not California law, this guide serves as a means to “identify and spread best practices” for those holding personal information.123

These California agencies recommend that notification be made within ten business days, unless law enforcement recommends or requires otherwise. Notice to law enforcement is suggested only if the entity believes illegal activity was involved.124 California recommends, but does not require, that the entity suffering the breach contact consumer reporting agencies if more than 10,000 individuals are affected; this minimizes the number of calls to the consumer reporting agency, allowing it to respond effectively.125

118. Id. § 1798.82[a].
120. CAL. CIV. CODE § 1798.82[g]. The difference between the electronic notice as primary notice and the email notice as an element of substitute notice is that email notice in conjunction with the other elements of substitute notice does not require consent from the consumer; it is simply a good-faith effort by the entity to notify the individual.
121. The California Office of Privacy Protection is now part of the California State and Consumer Services Agency.
123. Id. at 6, 7.
124. Id. at 12.
125. Id. at 13.
In determining whom to notify, the Recommended Practices advise entities to provide notice in breaches involving higher-risk personal information, even when it is not “notice-triggering” information under California law, if such notice would allow individuals to protect themselves from possible harm.\textsuperscript{126} However, entities are also cautioned to develop procedures to avoid “false positives” by sending notice of a security breach to individuals whose personal information was not acquired as part of the breach.\textsuperscript{127}

The Recommended Practices suggest that notice include the following:

1. a general description of the event;
2. the nature of personal information accessed;
3. the entity’s efforts to curb further unauthorized acquisition of personal information;
4. any assistance the entity is offering affected individuals;
5. information on how consumers can protect themselves, including contacts for credit reporting agencies; and
6. contact information for the Federal Trade Commission and the California Office of Privacy Protection.\textsuperscript{128}

Sample notice letters are included in the Recommended Practices.\textsuperscript{129}


While most states generally follow California’s model breach notification framework in many respects, they also include their own subtle distinctions and provisions governing notification procedures.

[B][1] “Material” Breach Necessary to Trigger Notification

One of the most noted, and perhaps most contentious,\textsuperscript{130} developments in security breach notification laws are clauses that require notification only when there is a “material” or “significant” risk

\textsuperscript{126} Id. at 12.
\textsuperscript{127} Id. at 12.
\textsuperscript{128} Id. at 13.
\textsuperscript{129} Id. at app. 2.
\textsuperscript{130} Christopher Conkey, Identity Theft Bills Stall in Congress, WALL ST. J., Nov. 26, 2005.
of harm from the security breach. The specific requirements establishing a breach as “material” vary by jurisdiction. The following illustrate several variations on this common theme:

- **Alaska**: Breach definition is broader than some states’ in that it does not even require that personal information be compromised to require notice—mere access or acquisition is sufficient. However, notification is not required if after an appropriate investigation and written notification to Alaska’s attorney general, the covered person determines that there is not a reasonable likelihood that harm to consumers will result from the breach. The determination must be documented in writing and maintained for five years.

- **Connecticut**: Like Alaska, notice obligation is broad. But notification is not required if after an appropriate investigation and consultation with relevant federal, state and local law enforcement, a company makes a reasonable determination that the breach will “not likely result in harm.”

- **Florida**: Notice is only required when there is a breach “of computerized data that materially compromises the security, confidentiality, or integrity of personal information,” but the law does not specify a procedure for determining whether a breach is “material.”

- **Michigan**: Notification is required “unless the person or agency determines that the security breach has not or is not likely to cause substantial loss or injury to, or result in identity theft with respect to [one] or more residents.”

---

131. The following states have incorporated such triggers: Alaska, Arizona, Arkansas, Colorado, Connecticut, Delaware, Florida, Hawaii, Idaho, Iowa, Kansas, Louisiana, Maine, Maryland, Michigan, Montana [but not for insurance institutions and insurance-support organizations, see MONT. CODE ANN. § 33-19-321], Nebraska, Nevada, New Jersey, North Carolina, Ohio, Oregon, Pennsylvania, Rhode Island, South Carolina, Tennessee, Utah, Virginia, Washington [for technical breaches only], West Virginia, Wisconsin, and Wyoming.

132. ALASKA STAT. § 45.48.010(c).

133. Id.

134. CONN. GEN. STAT. § 36a-701b(b). Iowa’s material breach trigger is similar to those found in the Alaska and Connecticut laws except that a determination not to notify may be reached after either appropriate investigation or consultation with the relevant federal, state or local agencies responsible for law enforcement. IOWA CODE § 715C.2(6). Documentation relating to the decision not to notify must be retained for five years. Id.

135. FLA. STAT. § 817.5681(4).

136. MICH. COMP. LAWS § 445.72.
• **New Jersey:** Notice is not required if the entity “establishes that misuse of the information is not reasonably possible.”\(^{137}\) New Jersey also requires that this determination “shall be documented in writing and retained for five years.”\(^{138}\)

• **Rhode Island:** Requires an “appropriate investigation” or “consultation with relevant, state, or local law enforcement” to determine whether a breach will result “in a significant risk of identity theft.”\(^{139}\)

Certain consumer advocates have voiced concern with the “material harm” standard as a trigger for notification, arguing this standard creates too high a bar for notification. Furthermore, they contend that, without meaningful guidance about the terms “reasonable investigation,” “significant risk,” and similar language in the laws, the terms are open to such wide interpretation that they may become meaningless and provide no protection.\(^{140}\) However, others counter that there will be unnecessary over-notification without such a trigger. This may result in customers becoming desensitized to notification and failing to take the appropriate steps to protect themselves from identity theft when a data security breach takes place that creates an actual risk of harm.\(^{141}\)

\(^{137}\) N.J. STAT. ANN. § 56:8-163[a]. Maine uses a somewhat similar iteration, only requiring notice if after an investigation a company concludes that “misuse of the personal information has occurred or if it is reasonably possible that misuse will occur.” ME. REV. STAT. ANN. tit. 10, § 1348(1)[B]. While the New Jersey and Maine standards are not particularly stringent (since a reasonable possibility of misuse requires notice), it is nonetheless a higher threshold than the California-type unauthorized access standard.

\(^{138}\) N.J. STAT. ANN. § 56:8-163[a]. Maryland imposes a similar three-year retention requirement for information relating to a determination that notice is unnecessary. MD. CODE ANN., COM. LAW § 14-3504[b][4]. Florida requires that a decision not to notify be documented in writing for five years, and punishes failure to do so with an administrative fine of up to $50,000. FLA. STAT. § 817.5681[10].

\(^{139}\) R.I. GEN. LAWS § 11-49.2-3, 4.


Expanded Definition of “Personal Information”

The definition of personal information has been modified in some jurisdictions, requiring notification when a different range of information is the subject of a breach. In California, details such as Social Security or account numbers alone do not trigger notification. Mandatory notice arises only when such details are coupled with an individual’s name, or, in the case of account numbers, access codes. Some state security breach laws may require notice to consumers when account numbers or related account access codes alone are compromised.142

Additional elements of information that trigger notification in certain states are date of birth,143 mother’s maiden name,144 employer identification number145 or individual taxpayer identification number,146 digitized or electronic signature,147 unique biometric data such as a fingerprint, voiceprint, or retina or iris image,148 unique physical representations or digital representations of biometric data,149 an individual’s DNA,150 unique electronic identifiers or routing codes in combination with any required security or access codes that permit access to financial accounts,151 and other numbers or information issued by a governmental or regulatory entity that uniquely identify an individual.152 North Carolina has developed one of the most expansive definitions of personal information, which includes a person’s first name or first initial and last name in combination with the following identifying information:

1. Social Security or employer taxpayer identification numbers;
2. drivers license, state identification card, or passport numbers;
3. checking account numbers;

143. N.D. CENT. CODE § 51-30-02.
144. Id.
145. Id.
146. Md. CODE ANN., COM. LAW § 14-3501(d)[iv].
147. Id.
148. Neb. REV. STAT. § 87-802(5)[e]; Wis. STAT. § 895.507[1][b].
150. Wis. STAT. § 895.507[1][b].
152. S.C. CODE ANN. § 16-13-510(D)[4].
(4) savings account numbers;
(5) credit card numbers;
(6) debit card numbers;
(7) personal identification code;
(8) electronic identification numbers, electronic mail names or addresses, Internet account numbers, or Internet identification names;
(9) digital signatures;
(10) any other numbers or information that can be used to access a person’s financial resources;
(11) biometric data;
(12) fingerprint;
(13) passwords; and
(14) parent’s legal surname prior to marriage.\textsuperscript{153}

Indiana requires notification to individuals if their unencrypted or unredacted Social Security number alone is compromised.\textsuperscript{154} Other states define personal information to include disassociated data so that certain “other” information need not be linked to names or initials. Oregon, for example, defines personal information to include certain data elements set forth in California’s definition or any combination of such data elements when not combined with the consumer’s first name or initial and last name if the information obtained is sufficient to permit a person to commit identity theft against the consumer.\textsuperscript{155}

Ten other states and the District of Columbia at least arguably have disaggregated requirements regarding account numbers and their associated access codes, which is unlike the vast majority of states that require the unauthorized access of a PIN or password plus a relevant account number.\textsuperscript{156} In these states, unauthorized acquisition of either the account number or password (in combination with

\textsuperscript{153} N.C. GEN. STAT. ANN. §§ 14-113.20(b), 75-61(10), 75-65[a]. Significantly, however, personal information does not include electronic identification numbers, electronic mail names or addresses, Internet account numbers, Internet identification names, parent’s legal surname prior to marriage, or a password, unless this information would permit access to a person’s financial account or resources. Id. § 75-65[a].

\textsuperscript{154} IND. CODE § 24-4.9-2-10.

\textsuperscript{155} See, e.g., OR. REV. STAT. § 646A.602(11)[b].

\textsuperscript{156} D.C. CODE § 28-3851(3)(A); HAW. REV. STAT. § 487N-1; KAN. STAT. ANN. § 50-7a01(g); MASS. GEN. LAWS ch. 93H, § 1[a]; ME. REV. STAT. ANN. 

5–34
an individual’s name) will trigger notification. New Jersey has broadened the definition of personal information to include “dissociated data that, if linked, would constitute personal information . . . if the means to link the dissociated data were accessed in connection with access to the dissociated data.” Similarly, Georgia, Maine, and Oregon allow any single data element of the standard definition of personal information to trigger notification, when not in connection with a name, if the information compromised would be sufficient to permit a person to fraudulently assume or attempt to assume the identity of the person whose information was compromised or, in Georgia, to perform or attempt to perform identity theft against that person.

[B][3] Necessity to Notify Customers of a Breach of Non-Computerized Data

Some jurisdictions require entities to notify customers of unauthorized access to non-computerized personal information. Alaska requires notification when personal information in any form is acquired by an unauthorized party. The state’s definition of a “breach of security” includes acquisition by “photocopying, facsimile, or other paper-based method.” North Carolina’s law requires notification when a breach of any record occurs. A record is defined as “[a]ny material on which written, drawn, spoken, visual, or electromagnetic information is recorded or preserved, regardless of physical form or characteristics.” Indiana’s law extends to breaches of computerized data that “have been transferred to another medium, including paper, microfilm, or a similar medium, even if the transferred data are no longer in a computerized format.” Hawaii’s definition of security breach includes the unauthorized access to and acquisition of unencrypted or unredacted records or data containing personal

157. See, e.g., KAN. STAT. ANN. § 50-7a01(g).
158. N.J. STAT. ANN. § 56:8-161.
159. Georgia requires notification only from “information brokers.” Examples of information brokers are credit agencies and background investigation firms. GA. CODE ANN. § 10-1-911(5).
160. GA. CODE ANN. § 10-1-911(5); ME. REV. STAT. ANN. tit. 10, § 1347(6); OR. REV. STAT. § 646A.602(11)[b]; S.C. CODE ANN. § 16-13-510[D][4]; VT. STAT. ANN. tit. 9, § 2430[4][A]; WIS. STAT. § 895.507.
161. ALASKA STAT. § 45.48.010.
162. Id. § 45.48.090[1].
163. N.C. GEN. STAT. ANN. § 75-61(12).
164. IND. CODE ANN. § 24-4.9-2.
information. As such, the statute requires notification when personal information in any form (for example, computerized, paper, or otherwise) is compromised by a breach. Massachusetts’ law also applies to non-computerized data. The statute defines security breach with respect to unauthorized acquisition or use of “unencrypted data or, encrypted electronic data” that is capable of compromising the security of personal information. The inclusion of the word “electronic” with reference to encrypted data suggests that unencrypted data need not be electronic to trigger notification. Wisconsin does not specify which formats containing personal information are subject to the law; thus the statute must be construed to cover personal information maintained in either computerized or non-computerized form. While California law does not require notification if hard copy records are the subject of a breach, the COPP recommends providing notice if such a breach occurs.

[B][4] Notification Procedures

The notice procedures established by California are widely followed with a few modifications in other states. Many jurisdictions have added notification via telephone as an acceptable method of notice. Substitute notice requirements are adjusted in some states, lowering the threshold number of individuals affected or cost demonstrated necessary before use of substitute notice is allowed or requiring only one of the components of substitute notice instead of all three. Indiana allows the most flexibility in notice procedures, allowing notification by mail, telephone, fax, email, or substitute notice consisting of both posting on the company website and in a major media outlet.

Eleven states and Puerto Rico mandate particular content in a security breach notice. In New York, notification must include contact information for the entity making the notification and a description of the categories of information that were accessed, including a specification of which elements of personal information (a term defined more broadly than the “private information” that triggers notification) were

169. Recommended Practices, supra note 122, at 8.
171. See, e.g., Delaware, Maryland, Pennsylvania, Rhode Island, Texas, West Virginia.
or are reasonably believed to have been acquired. Maryland expands upon the New York law by requiring the business providing notification to list toll-free numbers for the major credit reporting agencies, the Federal Trade Commission, and the Office of the Attorney General as well as a statement that an individual can obtain information from these sources about steps to avoid identity theft. Oregon requires that consumers be advised that they should report any suspected identity theft to law enforcement, including the Federal Trade Commission. In Massachusetts, notice to residents must disclose the consumer’s right to obtain a police report, how a consumer requests a security freeze and the necessary information to be provided when requesting the security freeze, and any fees required to be paid to any of the consumer reporting agencies. Iowa, Michigan, North Carolina, Vermont and Virginia mandate the following in a security breach notice (with slight variations among them):

(1) a description of the incident;
(2) the type of personal information unlawfully obtained;
(3) acts of the business to protect personal information from further unauthorized access;
(4) a telephone number that the person may call for further information and assistance, if one exists; and
(5) direction to the individual to remain vigilant by reviewing account statements and monitoring free credit reports.

173. N.Y. GEN. BUS. LAW § 899-aa[7].
174. MD. CODE ANN., COM. LAW § 14-3504(g). Maryland also requires the notices to include the business’s “address, telephone number, and toll-free telephone number if one is maintained.” Id. § 14-3504(g)[2].
175. OR. REV. STAT. § 646A.604[5][f].
176. MASS. GEN. LAWS ch. 93H, § 3[b]. Notices sent to Massachusetts residents, however, must not include “the nature of the breach or unauthorized acquisition or use or the number of residents of the commonwealth affected by said breach or unauthorized access or use.” Id.
177. MICH. COMP. LAWS § 445.72[6]; N.C. GEN. STAT. § 75-65[d]; VT. STAT. ANN. tit. 9, § 2435[4]; VA. CODE § 18.2-186.6[A]. Oregon also specifies particular content for notices. In addition to the information required by Michigan, North Carolina, and Vermont, Oregon requires the business to disclose the approximate date of the breach, contact information for credit reporting agencies, and advice to report suspected identity theft to law enforcement and the Federal Trade Commission. Oregon does not, however, require the business to describe the steps it is taking to prevent further incidents. OR. REV. STAT. § 646A.604[5]. Iowa’s requirements generally mirror Oregon’s specific content requirements. IOWA CODE § 715C.2[5].
Pennsylvania only prescribes the content of notice made by telephone, requiring such notice to provide a description of the breach, that the individual making the call verifies the consumer’s personal information, and that the phone call provides consumers with a phone number or website for assistance.\textsuperscript{178} West Virginia requires a description of the categories of information reasonably believed to be compromised, a telephone number that affected individuals may use to contact the entity that experienced the breach and learn more about the incident and the toll-free contact telephone numbers of the credit reporting agencies and information on how to place a fraud alert or security freeze.\textsuperscript{179} Wyoming requires notices to include a toll-free number that individuals may use to contact the party experiencing the breach and from which the individual may obtain the toll-free numbers for the major credit reporting agencies.\textsuperscript{180} Puerto Rico requires a notice to include, as far as possible, the needs of any current investigation or court case, the nature of the situation, the number of clients potentially affected, if criminal complaints have been filed, as well as which measures are being taken and an estimate of time and cost required to rectify the situation.\textsuperscript{181} Moreover, if it is specifically known how the confidentiality of the information of an identifiable client was breached, the client has the right to know which information was compromised.\textsuperscript{182}

Timing requirements for notification are vague in most states which, like California, require notice to be made in a “reasonable” time period so long as the notification occurs in the most expedient time possible consistent with the needs of law enforcement or to determine the scope of the breach and restore the system’s integrity. The exceptions are Florida, Ohio, and Wisconsin, which require notice within forty-five days, subject to law enforcement or internal system security needs.\textsuperscript{183}

\section{Duty to Notify Other Entities}

Many jurisdictions with security breach notification laws mandate notification to consumer reporting agencies when a certain number of residents (ranging from 500 to 10,000) are affected by a data security

\begin{itemize}
\item \textsuperscript{178} 73 PA. CONS. STAT. § 2302.
\item \textsuperscript{179} W. VA. CODE § 46A-2A-102(d).
\item \textsuperscript{180} WYO. STAT. ANN. § 40-12-502(e).
\item \textsuperscript{181} P.R. LAWS ANN. tit. 10, § 4053.
\item \textsuperscript{182} Id.
\item \textsuperscript{183} FLA. STAT. § 817.5681[1][a]; OHIO REV. CODE ANN. § 1349.19[B][2]; WIS. STAT. § 895.507[3][a], [5].
\end{itemize}
breach.\textsuperscript{184} Minnesota requires this notice within forty-eight hours.\textsuperscript{185} In Massachusetts, unlike other states, the director of consumer affairs and business regulations is responsible for determining whether and which consumer reporting agencies will be notified of a security breach.\textsuperscript{186}

Some jurisdictions require reporting of a data security breach incident to state law enforcement or governmental agencies. Hawaii requires entities that experience a breach to notify the Office of Consumer Protection if the entity provides notice to more than 1,000 persons at one time.\textsuperscript{187} Louisiana requires timely notification to the Consumer Protection Section of the Office of the Attorney General.\textsuperscript{188} Notification to the Louisiana Attorney General is considered timely if it is received within ten days of distribution to Louisiana citizens.\textsuperscript{189} Maine requires notification to the appropriate state regulators within the Department of Professional and Financial Regulation, or, if the person is not regulated by the department, the Attorney General.\textsuperscript{190} In New Jersey, notification to individuals must be preceded by notice to the Division of State Police, Department of Law and Public Safety.\textsuperscript{191} And in Maryland any business providing individual notices must first notify the Office of the Attorney General.\textsuperscript{192} Massachusetts requires notice to the attorney general and the director of consumer affairs and business regulation in addition to notice to affected state residents.\textsuperscript{193} The New York statute requires notification to the State Attorney General, the Consumer Protection Board, and the State Office of Cyber Security and Critical Infrastructure Coordination as to the timing, content and distribution of the notices and the approximate number of affected persons.\textsuperscript{194} North Carolina is similar to Hawaii in that notice to the Consumer Protection Division of the Attorney General’s office is only required if more than 1,000 people

\textsuperscript{184} These states include: Alaska, Colorado, District of Columbia, Florida, Georgia, Indiana, Kansas, Maine, Maryland, Michigan, Minnesota, Nevada, New Hampshire, New Jersey, New York, North Carolina, Ohio, Oregon, Pennsylvania, South Carolina, Tennessee, Texas, Vermont, Virginia, West Virginia, and Wisconsin.

\textsuperscript{185} MINN. STAT. § 325E.61.

\textsuperscript{186} MASS. GEN. LAWS ch. 93H, § 3[b].

\textsuperscript{187} HAW. REV. STAT. § 487N-2[f].

\textsuperscript{188} LA. ADMIN. CODE tit. 16, § 701.

\textsuperscript{189} Failure to timely notify the Attorney General may be punishable by a fine not to exceed $5,000. “Each day notice is not received by the attorney general shall be deemed a separate violation.” Id.

\textsuperscript{190} ME. REV. STAT. ANN. tit. 10, § 1348(5).

\textsuperscript{191} N.J. STAT. ANN. § 56:8-163[c][1].

\textsuperscript{192} MD. CODE ANN., COM. LAW § 14-3504[h].

\textsuperscript{193} MASS. GEN. LAWS ch. 93H, § 3[b].

\textsuperscript{194} N.Y. GEN. BUS. LAW § 899-aa[8][a].
are affected. Any person engaged in trade or commerce in New Hampshire that is required to notify individuals of a breach must also notify the regulator with “primary regulatory authority over such trade or commerce” or the state attorney general’s office. Puerto Rico requires the responsible parties to inform the Department of Consumer Affairs within ten days, with no extension of time, after the breach is detected, and the Department will then make a public announcement regarding the breach within twenty-four hours. South Carolina, like Hawaii and North Carolina, requires notice to the Consumer Protection Division of the Department of Consumer Affairs if more than 1,000 people are notified at one time. Virginia likewise requires notice to the Office of the Attorney General when more than 1,000 people are notified.

**[B][6] Duty of Non-Owners Maintaining Data**

Most states, like California, place the ultimate responsibility for notifying consumers of a breach on the data owner. Non-owners collecting data are generally required only to notify the owner or licensee of the information of a breach following discovery of the same. Several states, however, take a slightly different approach. Security breach notification statutes in Florida and Wyoming, for example, provide that the party who maintains the data on behalf of another (the non-data owner) and the entity on whose behalf the data is maintained (the owner) may agree amongst themselves who will provide any required notices. Nonetheless, if agreement cannot be reached, the entity who has a direct business relationship with the Florida or Wyoming resident must provide notice. In most cases this will be the data owner. Breach notification statutes in Alaska, Arizona, Colorado, Idaho, Massachusetts, Nebraska, and Utah also depart slightly from the California model. In those states, in addition to the obligation to notify the data owner of an information security breach, a non-data owner is required to “cooperate” with the data owner or licensee. “Cooperation” generally requires sharing with the data owner or licensee relevant details about the breach incident.

---

195. N.C. GEN. STAT. § 75-65(f).
197. P.R. LAWS ANN. tit. 10, § 4052.
199. VA. CODE ANN. § 18.2-186.6(E).
200. See, e.g., CAL. CIV. CODE § 1798.82(b).
201. FLA. STAT. § 817.5681(2)(a); WYO. STAT. ANN. § 40-12-502(g).
202. FLA. STAT. § 817.5681(2)(a).
203. ALASKA STAT. § 45.48.070; ARIZ. REV. STAT. ANN. § 44-7501(B); COLO. REV. STAT. § 6-1-716(2)(b); IDAHO CODE ANN. § 28-51-105(2); MASS. GEN. LAWS ch. 93H, § 3(a); NEB. REV. STAT. § 87-803(2); UTAH CODE ANN. § 13-44-202(3).
and about any remedial measures being taken, but does not require the disclosure of confidential business information or providing notice to affected individuals.\textsuperscript{204} Alaska expressly relieves non-data owners from any responsibility for consumer notifications.\textsuperscript{205}

\textbf{[B][7] Exemption from Notification for Entities in Compliance with GLBA}

An exemption from notification used by approximately twenty-five states and the District of Columbia allows entities that are otherwise required by another state or federal law to notify individuals of a security breach to follow those procedures.\textsuperscript{206} Typically the exemptions are for entities regulated by the Gramm-Leach-Bliley Act (GLBA),\textsuperscript{207} and the related Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notification [Interagency Guidance],\textsuperscript{208} or the Health Insurance Portability and Accountability Act (HIPAA). Entities that are subject to these federal laws and comply with their notification requirements are sometimes deemed in compliance with the various state security breach notification statutes. Indiana provides the most detailed listing of federal laws that apply to this exception, including the USA PATRIOT Act; Executive Order 13224; the Driver’s Privacy Protection Act; the Fair Credit Reporting Act; GLBA; and HIPAA.\textsuperscript{209}

\textbf{[B][8] Exemption from Notification for Encrypted Information}

Virtually all jurisdictions have mirrored California’s exemption from notification for data that is encrypted or otherwise rendered secure. However, Alaska, Indiana, Massachusetts, Michigan,

\begin{itemize}
\item \textsuperscript{204} See, e.g., ARIZ. REV. STAT. ANN. § 44-7501[B]; MASS. GEN. LAWS ch. 93H, § 3[a].
\item \textsuperscript{205} ALASKA STAT. § 45.48.070(b) (“If an information recipient notifies an information distributor of a breach . . . , the information distributor shall comply with AS 45.48.010-45.48.030 as if the breach occurred to the information system maintained by the information distributor.”).
\item \textsuperscript{206} Arkansas, Delaware, District of Columbia, Florida, Iowa, Louisiana, Maryland, Michigan, Montana, Minnesota, New Jersey, Nevada, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, Tennessee, Texas, Utah, Virginia, West Virginia, Wisconsin, and Wyoming.
\item \textsuperscript{207} 15 U.S.C. § 6801 et seq.
\item \textsuperscript{208} This interpretive guidance published by the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, and the Office of Thrift Supervision is available at www.federalreserve.gov/boarddocs/press/bcreg/2005/20050323/attachment.pdf.
\item \textsuperscript{209} IND. CODE ANN. § 24-4.9-2.
\end{itemize}
New York, North Carolina, Oklahoma, Pennsylvania, Virginia, and West Virginia require notification for a breach of encrypted information when there is access to an encryption key or code. Encryption is not defined in the California legislation and may mean a simple password, although the trend is certainly toward more sophisticated mechanisms for securing data. Several states have attempted to define encryption. Hawaii, Iowa, Kansas, Maryland, Massachusetts, Michigan, New Hampshire, North Carolina, Ohio, Oregon, Pennsylvania, Virginia, and West Virginia define encryption as “the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.” Maine uses a broader definition, “[d]isguising of data using generally accepted practices.” Arizona and Nebraska define encryption as conversion using an algorithmic process that renders data unreadable or unusable without the use of a confidential process or key. Nevada has the most detailed definition:

“Encryption” means the use of any protective or disruptive measure, including, without limitation, cryptography, encingiphering, encoding or a computer contaminant, to: (1) Prevent, impede, delay or disrupt access to any data, information, image, program, signal or sound; (2) Cause or make any data, information, image, program, signal or sound unintelligible or unusable; or [3] Prevent, impede, delay or disrupt the normal operation or use of any component, device, equipment, system or network.

210. ALASKA STAT. § 45.48.090(7); IND. CODE ANN. § 24-4.9-3-1(a)(2); MASS. GEN. LAWS ch. 93H, § 1[a]; MICH. COMP. LAWS § 445.72(1)[b]; N.Y. GEN. BUS. LAW § 899-aa[b]; N.C. GEN. STAT. § 75-61[14]; 24 OKLA. STAT. § 163[A] (effective Nov. 1, 2008); 73 PA. CONS. STAT. § 2303[b]; VA. CODE ANN. § 18.2-186.6[c]; W. VA. CODE § 46A-2A-102[b]. Indiana provides a separate exemption for a “portable electronic device” if the device is password protected. IND. CODE ANN. § 24-4.9-2.

211. HAW. REV. STAT. § 487N-1; IOWA CODE § 715C.1[5]; KAN. STAT. ANN. § 50-7a01[b]; MASS. GEN. LAWS ch. 93H, § 1[a]; MICH. COMP. LAWS § 445.63[g]; MD. CODE ANN., COM. LAW § 14-3501[c]; N.H. REV. STAT. ANN. § 359-C:19[II]; N.C. GEN. STAT. ANN. § 75-61[8]; OHIO REV. CODE ANN. § 1349.19[A][4]; OR. REV. STAT. § 646A.602(6); 73 PA. CONS. STAT. ANN. § 2302; VA. CODE ANN. § 18.2-186.6[a]; W VA. CODE § 46a-2a-105[3]. Massachusetts also allows the department of consumer affairs and business regulation to adopt regulations to revise the definition of “encrypted” to reflect technological advances. MASS. GEN. LAWS ch. 93H, § 1[b].

212. ME. REV. STAT. ANN. tit. 10, § 1347[2].

213. ARIZ. REV. STAT. ANN. § 44-7501[L][3]; NEB. REV. STAT. § 87-802(3); see also CONN. GEN. STAT. § 36-701b[a] (defining breach to include unauthorized access to information that has not been secured by encryption or by any other method that renders the information unreadable or unusable).

214. NEV. REV. STAT. § 205.4742.
Nevada will require encryption for all electronic transmission of personal information (other than a facsimile) outside of secure networks, effective October 1, 2008.215

[B][9] Penalties for Violation

Ten states and the District of Columbia follow California’s lead by providing individuals with a private right of action against businesses for noncompliance.216 Other jurisdictions allow for enforcement by the state’s Attorney General or consumer protection agency, who may seek either civil or injunctive relief.217 Arkansas and Maryland provide for criminal penalties in some cases.218

Schedules of fines for failure to abide by the law are specified in several states, the District of Columbia, and Puerto Rico, as described below.219

- **Alaska**: An information collector that violates the statute may, subject to some limitations, be liable to the state for a civil penalty of up to $500 for each state resident who was not notified under Alaska Statutes sections 45.48.010 to 45.48.090, except that the total civil penalty may not exceed $50,000.220

- **Arizona**: An entity that willfully and knowingly fails to notify may be liable for a fine up to $10,000 per breach.221

- **District of Columbia**: The Attorney General may recover a civil penalty not to exceed $100 per failure to provide a required notice. The Attorney General also may petition the D.C. Superior Court for an injunction or restitution for property lost by D.C. residents as a result of the breach.222

215. NEV. REV. STAT. § 597.970.
216. District of Columbia, Louisiana, Maryland, New Hampshire, New Jersey, North Carolina, South Carolina, Tennessee, Texas, and Washington. In Virginia, an affected individual may recover direct economic damages from a violation of the statute. VA. CODE ANN. § 18.2-186.6[I].
220. ALASKA STAT. § 45.48.080[b].
221. ARIZ. REV. STAT. ANN. § 44-7501[H].
222. D.C. CODE § 28-3853[b].

(Proskauer, Rel. #4, 7/10) 5–43
• **Florida:** If an entity does not notify within the forty-five-day time period specified, the entity faces fines of: (1) $1,000 per day, up to thirty days; (2) $50,000 each thirty days thereafter, up to 180 days; (3) if there is no notification within 180 days, a fine of up to $500,000. The fines are per breach, not per individual. The Florida Department of Legal Affairs may institute proceedings to collect fines.223

• **Idaho:** An entity that intentionally fails to notify may be liable for a fine of up to $25,000 per breach.224

• **Indiana:** Allows for a civil money penalty of not more than $150,000.225

• **Iowa:** Attorney general may request and the court may impose a civil penalty not to exceed $40,000 per incident.226

• **Maine:** A fine of not more than $500 per violation, up to a maximum of $2,500 for each day the entity is in violation of the requirements.227

• **Maryland:** A merchant who violates the law may be fined up to $1,000 for each violation and up to $5,000 for each subsequent repeat violation.228

• **Michigan:** A person that knowingly fails to provide any required notice may be ordered to pay a fine of not more than $250 for each violation, capped at $750,000.229

• **New York:** For knowing or reckless violations, violators are subject to fines of the greater of $5,000 or $10 per failed notification, capped at $150,000.230

• **Oklahoma:** For failure to comply with the notification law, the Attorney General or appropriate District Attorney may recover a civil penalty not to exceed $150,000 per breach of the system.231

• **Oregon:** Any person who violates, or who procures, aids or abets in a violation of the Act may be required to pay up to $1,000 per

---

223. FLA. STAT. § 817.5681(10), (11).
224. IDAHO CODE ANN. § 28-51-104 et seq.
225. IND. CODE § 24-4.9-4-2.
226. IOWA CODE §§ 715C.2(8), 714.16.
227. ME. REV. STAT. ANN. tit. 10, § 1349(2).
228. MD. CODE ANN., COM. LAW § 14-3508 [citing MD. CODE ANN., COM. LAW § 13-401 et seq.].
229. MICH. COMP. LAWS § 445.72(13)-{14}.
230. N.Y. GEN. BUS. LAW § 899-aa(6).
231. OKLA. STAT. tit. 24, § 165[B].
violation to the state treasury up to $500,000 total for any occurrence.\textsuperscript{232}

- **Puerto Rico**: The secretary may impose fines from $500 up to a maximum of $5,000 for each violation of the law or its accompanying regulation.\textsuperscript{233}

- **Rhode Island**: Violation may result in civil penalties of not more than $100 per occurrence and not more than $25,000 per defendant.\textsuperscript{234}

- **South Carolina**: Knowing and willful violations are subject to an administrative fine of up to $1,000 per resident whose information was made accessible through the security breach.\textsuperscript{235}

- **Texas**: Civil penalties between $2,000 to $50,000 per violation may be imposed.\textsuperscript{236}

- **Utah**: In aggregate, the fine to a Utah entity for failure to comply with the law can be no more than $100,000. The fine per consumer can be up to $2,500.\textsuperscript{237}

- **Virginia**: Allows for a civil money penalty of not more than $150,000 per breach or series of breaches of a similar nature discovered in a single investigation.\textsuperscript{238}

- **West Virginia**: Allows for a civil money penalty of not more than $150,000 per breach or series of breaches of a similar nature discovered in a single investigation.\textsuperscript{239} No civil penalties unless a court finds repeated and willful violations.

Some states, like Montana, do not specify an amount, but allow for civil fines for willful violations of the statute.\textsuperscript{240} Vermont allows the state attorney general, state’s attorney, or courts to dissolve business licenses within the state and revoke the certificate of authority to foreign corporations if an entity violates its security breach notification statute.\textsuperscript{241}

\begin{itemize}
\item \textsuperscript{232} OR. REV. STAT. § 646A.624(4).
\item \textsuperscript{233} P.R. LAWS ANN. tit. 10, § 4055.
\item \textsuperscript{234} R.I. GEN. LAWS § 11-49.2-6.
\item \textsuperscript{235} S.C. CODE ANN. § 39-1-90[H].
\item \textsuperscript{236} TEX. BUS. & COM. CODE ANN. § 48.201[a].
\item \textsuperscript{237} UTAH CODE ANN. § 13-44-301[3].
\item \textsuperscript{238} VA. CODE ANN. § 18.2-186.6[I].
\item \textsuperscript{239} W. VA. CODE § 46-2A-104[b].
\item \textsuperscript{240} MONT. CODE ANN. § 30-14-1704.
\item \textsuperscript{241} VT. STAT. ANN. tit. 9, §§ 2435[g][1], 2458[a].
\end{itemize}
### [B][10] Minnesota Law Requires Reimbursement of Card-Issuing Financial Institutions for Costs Associated with a Data Breach

In response to the massive data breach at TJX Companies, Inc., which required card issuers to reissue millions of debit and credit cards, lawmakers in Minnesota and Washington have passed laws that require merchants or data brokers to reimburse card reissuance costs associated with data breaches. To date, only Minnesota and Washington have passed such laws.

On May 21, 2007, the Minnesota governor signed H.F. 1758,\(^{242}\) which took effect on August 1, 2007. The law applies to any “person or entity conducting business in Minnesota” that accepts credit cards, debit cards, stored value cards or similar cards “issued by a financial institution.” Such companies are prohibited from retaining the following card data after authorization of a transaction: “the full contents of a track of magnetic stripe data” (which encompasses the “card verification value” or CVV—a unique authentication code embedded on the magnetic stripe); the three-to-four-digit security code on the back of the card by the signature block (also known as CVV2); and any PIN verification code number. If a debit card with PIN is used, a company is prohibited from retaining the data more than forty-eight hours after authorization of the transaction.

The liability provision of H.F. 1758 applies to data breaches occurring after August 1, 2008. It requires companies to reimburse card-issuing financial institution for the “costs of reasonable actions” to both protect its cardholders’ information and to continue to provide services to its cardholders after a breach. The reimbursement would cover costs related to providing cardholders with notification of the breach, cancellation and reissuance of cards, closing or reopening of accounts and stop payments, and cardholder refunds for unauthorized transactions charged to their accounts. A financial institution may also bring an action to recover for the costs of damages it pays to cardholders resulting from a breach.

Under the new Washington law, businesses and card processors that fail to encrypt customer data or comply with industry processing standards, and subsequently suffer a breach, will be affected by the law.\(^{243}\) The law allows financial institutions to seek reparations via the courts for damages as a result of a data breach.

---

\(^{242}\) H.F. 1758, *codified at Minn. Stat. § 325E.61* [2007].

\(^{243}\) Wash. H.B. 1149 (effective July 1, 2010).

\(^{244}\) [Reserved.]
[B][11] State Credit Freeze Laws

State legislatures passed credit freeze laws in response to consumers’ fear of identity theft. Credit freeze laws allow consumers to restrict third-party access to their credit reports. Forty-four states and the District of Columbia have enacted such laws.245 States typically allow the victims of identity theft to place a credit freeze free of charge.

After an eligible consumer enacts a credit freeze, credit reporting agencies cannot release the frozen credit report to most third-party requestors without the consumer’s express authorization.246 Some entities will continue to have access to frozen credit reports, including those having a business relationship with the consumer before the enactment of the freeze, government agencies, and those working under the direction of a court order.247 The Fair Credit Reporting Act (FCRA) preempts portions of these state laws and specifies


246. See, e.g., CAL. CIV. CODE § 1785.11.2[a] (2007).

247. See, e.g., id. § 1785.11.2[l][1]-[9] (2007).
accepted methods for pre-screening reports, including frozen reports, by certain entities wishing to extend credit.248

A consumer with a credit freeze in place has a few options to release his or her credit report. For temporary removal, the consumer can remove the credit freeze for a specific time period or to a certain entity.249 Typically, states do not allow credit reporting agencies to charge fees to the victims of identity theft or senior citizens for the temporary removal of a credit freeze.250 Entities that have requested a frozen credit report can prompt the consumer to remove the freeze or the individual may choose to remove the freeze.

Another mechanism, similar to a security freeze in its effect, is also available to consumers for credit report protection. Some states allow the victims of identity theft to place a “security alert” on their credit report.251 The security alert informs requesting parties that the information on the credit report may not be accurate because the person was recently the victim of identity theft.252

§ 5:5.6   Data Security and Destruction Requirements

In an attempt to develop a comprehensive legal framework to combat identity theft, some states mandate implementation of procedures and creation of written policies to safeguard personal information.

Nevada requires all businesses in the state to encrypt an electronic transmission (other than via facsimile) of any personal information of a customer to a person outside of the secure system of the business unless the business encrypts such data.252.1 “Personal information” has a materially similar definition as in the California framework.252.2

As of January 1, 2010, Nevada State Bill 227 repealed Nevada Revised Statutes 597.970, but kept the basic framework of the old encryption statute and extended its reach to include portable devices like computers, cellular phones, and portable hard drives.

248. 15 U.S.C. § 1681. FCRA allows consumers to opt-out of this prescreening. The FTC implements and monitors this opt-out program.
250. Id. Other consumers will have to pay a fee for these services ranging from $5.00 to $20.00.
251. See, e.g., CAL. CIV. CODE § 1785.11.1.
252. Other states, including Louisiana and Texas, also allow for alerts. Federal law also provides for alerts.
252.2. NEV. REV. STAT. § 603A.040 (2007).
Massachusetts law\textsuperscript{252.3} and implementing regulations\textsuperscript{252.4} require all persons that own or license personal information of Massachusetts residents to, as of March 1, 2010,

develop, implement and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical and physical safeguards that are appropriate to \(a\) the size, scope and type of business of the person obligated to safeguard the personal information . . . \(b\) the amount of resources available to such person; \(c\) the amount of stored data; and \(d\) the need for security and confidentiality of both consumer and employee information.\textsuperscript{252.3}

Among other things, the regulations require that such policies include training of employees, identifying media and records that contain personal information, monitoring, and verifying and requiring that third-party service providers comply with the Massachusetts regulations.

The Massachusetts regulations also require specific technical safeguards including, to the extent technically feasible, secure user authentication protocols; secure access control measures; and encryption of personal information stored on laptops or other portable devices, as well as encryption of all records and files containing personal information “that will travel across public networks” or will be transmitted wirelessly.

Oregon law requires persons that own, maintain or otherwise possess consumer personal information used in the course of the person’s business, vocation, occupation or volunteer activities to develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the personal information. Such safeguards must include administrative, technical and physical safeguards enumerated in the statute, as well as a disposal program.\textsuperscript{252.6} A person that complies with a state or federal law requiring greater protection, including the Gramm-Leach-Bliley Act and HIPAA, need not comply with Oregon’s requirements. Persons with personal information must ensure, in written contracts, that service providers maintain [and are capable of maintaining] appropriate safeguards.

Several other states have similar laws, in most cases less detailed than Oregon’s law.

Finally, some states also have specific destruction requirements for records containing personal information no longer needed to be

\begin{itemize}
  \item \textsuperscript{252.3} Mass. Gen. Laws. ch. 93H, § 2(a) (2008).
  \item \textsuperscript{252.4} 201 Mass. Code Regs. 17.00-17.04 (2009).
  \item \textsuperscript{252.5} 201 Mass. Code Regs. 17.03[1].
  \item \textsuperscript{252.6} Or. Rev. Stat. § 646A.622 (2007).
\end{itemize}
retained. For example, California requires that such records be shreded, erased or otherwise modified such that the personal information is “unreadable or undecipherable through any means.”

§ 5:6 Financial Privacy

An increasing number of state have enacted laws to prevent the unauthorized sharing of personally identifiable nonpublic information among financial institutions, and to prevent identity theft through phishing schemes and digging through the garbage for credit card receipts. Some aspects of these state laws—in particular, affiliate sharing provisions and credit card receipt truncation—are preempted by the federal Fair Credit Reporting Act (FCRA).

§ 5:6.1 California Financial Information Privacy Act

California’s Financial Information Privacy Act (CalFIPA), which took effect on July 1, 2004, prohibits financial institutions from sharing or selling personally identifiable nonpublic information without obtaining a consumer’s consent. It was the intent of the California Legislature in enacting CalFIPA to “afford persons greater privacy protections than those provided in Public Law 106-102, the federal Gramm-Leach-Bliley Act,” due to the increased “likelihood that the personal financial information of California residents would be widely shared among, between, and within companies.”

Under CalFIPA, consumers must, with some exceptions:

(a) provide their consent, or opt-in, before a financial institution may share “nonpublic personal information” with a non-affiliated third party;

252.7. CAL. CIV. CODE § 1798.81.
254. Id. § 4051(b).
255. Id. § 4051.5[a][2].
256. “Nonpublic personal information” is defined as “personally identifiable financial information [1] provided by a consumer to a financial institution, [2] resulting from any transaction with the consumer or any service performed for the consumer, or [3] otherwise obtained by the financial institution. Nonpublic personal information does not include publicly available information that the financial institution has a reasonable basis to believe is lawfully made available to the general public from [1] federal, state, or local government records, [2] widely distributed media, or [3] disclosures to the general public that are required to be made by federal, state, or local law.” Id. § 4052[a]. “Personally identifiable financial information,” in turn, is defined as “information [1] that a consumer provides to a financial institution to obtain a product or service from the
(b) be provided with written notice of their right to opt-out of sharing of “nonpublic personal information” with a financial institution's affiliates.\textsuperscript{257}

An institution may share its customers’ personal information with an affiliate without providing an opt-out right where the affiliate is wholly owned, or among the insurance and management entities of a single insurance holding company system consisting of one or more reciprocal insurance exchanges that has a single corporation or its wholly owned subsidiaries providing management services to the reciprocal insurance exchanges, provided that the disclosing and receiving companies are in the same line of business (insurance, banking, or securities), subject to the same functional regulator, and share a common brand.\textsuperscript{258}

\textbf{§ 5:6.2 Other States}

A number of other states have enacted legislation restricting the disclosure of personal information by financial institutions.\textsuperscript{259}

North Dakota prohibits disclosure of customer information by financial institutions unless a customer opts-in, or pursuant to valid legal process, with limited exceptions.\textsuperscript{260} In some respects similar to California, Alaska prohibits a financial institution from disclosing the records and information relating to their depositors and customers except where disclosure is authorized in writing by the depositor or customer, required by statute, regulation, or court order, made to the holder of a negotiable instrument drawn on the financial institution as to whether the drawer has sufficient funds in the financial institution to cover the instrument, made to a consumer reporting agency regulated under the FCRA, or made in connection with the maintenance or servicing of the depositor’s or customer’s account with the financial institution or with another entity as part of a private label credit card or other extension of credit on behalf of the entity. The statute does not prevent a financial institution from disclosing

\begin{itemize}
\item financial institution, [2] about a consumer resulting from any transaction involving a product or service between the financial institution and a consumer, or [3] that the financial institution otherwise obtains about a consumer in connection with providing a product or service to that consumer. Any personally identifiable information is financial if it was obtained by a financial institution in connection with providing a financial product or service to a consumer.” \textit{Id.} § 4052(b). Section 4052(b) provides several examples of personally identifiable financial information.
\end{itemize}

\textsuperscript{257.} CAL. FIN. CODE §§ 4050–60 [2005].
\textsuperscript{258.} \textit{Id.} § 4053.
\textsuperscript{259.} This section does not address financial privacy provisions found in state insurance statutes.
\textsuperscript{260.} N.D. CENT. CODE §§ 6-08.1-01 to -08 [2005].
information if the disclosure is necessary to provide the services of the financial institution to a depositor or customer or to market financially related products or services of the institution and its marketing partners, and the person receiving the information has a written agreement with the financial institution to be bound by the statute’s requirements.\footnote{261} Similarly, under Connecticut and New Jersey law, a customer’s records may not be disclosed by a financial institution without legal process or other specifically listed circumstances.\footnote{262} Massachusetts prohibits the disclosure of information regarding any account or electronic fund transfer to any person except: the customer pursuant to his or her written authorization; a party to the transaction; a person authorized by law to have access in the course of such personal official duties; auditors; a consumer reporting agency; the institution’s attorney or collection agent; employees of the institution for the purpose of pursuing or disposing of a dispute or claim involving an account; or pursuant to legal process.\footnote{263} In Maryland, an institution may not disclose any financial records unless the customer has authorized the disclosure or in other limited circumstances, including certain requests of the Department of Human Resources, or Comptroller.\footnote{264} Many other states have similar provisions.\footnote{265}

\section*{§ 5:6.3 Preemption}

In June, 2005, the U.S. Court of Appeals for the Ninth Circuit held that the affiliate-sharing preemption clause of the FCRA\footnote{266} preempts CalFIPA, at least insofar as it attempts to regulate the communication between affiliates of “information” as that term is defined by FCRA;\footnote{267} the court also noted that it construed the affiliate-sharing preemption

\begin{thebibliography}{9}
\footnotesize
\item 261. ALASKA STAT. § 06.01.028 (2005).
\item 263. MASS. GEN. LAWS ch. 167B, § 16 (2005).
\item 264. MD. CODE ANN., FIN. INST. § 1-302 (2006).
\item 267. “[I]nformation . . . bearing on a consumer’s credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the
clause to preempt “all state ‘requirement[s]’ and ‘prohibition[s]’ on the communication of ‘information’ between affiliated parties,” applying the restricted definition of “information in section 1681a[d][1].”

On October 4, 2005, the U.S. District Court for the Eastern District of California held on remand that CalFIPA’s affiliate sharing provision does not survive preemption and, even if some limited applications could be saved, they cannot be severed from the remainder of the statute. The Ninth Circuit Court of Appeals agreed that the FCRA preempts the statute to the extent it pertains to “consumer report” information. However, the court allowed the other affiliate data-sharing provisions to stand. The Supreme Court denied American Bankers Association’s petition for a writ of certiorari.

§ 5:6.4 Credit Card Transactions

[A] Restrictions on Merchants

California’s Song-Beverly Credit Card Act of 1971 prohibits any person accepting a credit card in payment for most goods or services from requesting, or requiring as a condition to accepting the credit card as payment, the cardholder to provide personal identification information, which the retailer writes, causes to be written, or records upon the credit card transaction form or otherwise. ZIP codes are not personal identification information. The California Court of Appeal held that a consumer stated a cause of action under the statute where she alleged that the cashier requested and recorded her personal identification information (specifically, her telephone number) when

consumer’s eligibility for (A) credit or insurance to be used primarily for personal, family, or household purposes; (B) employment purposes; or (C) any other purpose authorized under section 1681b of this title.”

Id. § 1681a[d][1] [2006].

269. Am. Bankers Ass’n v. Lockyer, 2005 WL 2452798, at *4 (E.D. Cal. Oct. 5, 2005). To date, we are unaware of other published cases that have addressed whether and to what extent the financial privacy laws of other states prohibiting the disclosure of personal information without consent are preempted by FCRA’s affiliate sharing preemption clause.

270. Am. Bankers Ass’n v. Lockyer, 541 F.3d 1214 (9th Cir. 2008).
272. CAL. CIV. CODE §§ 1747–1748.7 [2006].
273. “Personal identification information” is defined as “information concerning the cardholder, other than information set forth on the credit card, and including, but not limited to, the cardholder’s address and telephone number.” Id. § 1747.08[b] [2006].
274. Id. § 1747.08.
she made purchases with a credit card.276 In reaching its holding, the court noted that the statute:

is a consumer protection statute, and the retailer’s request for personal identification information must be viewed from the customer’s standpoint. In other words, the retailer’s unannounced subjective intent is irrelevant. What does matter is whether a consumer would perceive the store’s “request” for information as a “condition” of the use of a credit card.277

The California Court of Appeal stated that nothing in the statute “prevents a retailer from soliciting a consumer’s address and telephone number for a store’s mailing list, if that information is provided voluntarily,” but that a request for personal identification information is prohibited if it immediately precedes the credit card transaction, “even if the consumer’s response was voluntary and made only for marketing purposes.”278

A number of states and the District of Columbia have enacted legislation similar to California’s Credit Card Act.279 In most instances, the states prohibit a merchant from writing down or requesting to be written down the address and/or telephone number of a customer as a condition of accepting a credit card except if the information is necessary for shipping, delivery, installation, or special orders. A merchant in Ohio may not record the telephone or Social Security number of a credit card holder in credit card sales, except for “legitimate business purposes,” including collection, provided that the

277. Id. at 451.
278. Id. at 451, 453. The court suggested a number of options for retailers to consider for purposes of soliciting the voluntary provision of this information: “A merchant can easily delay the request until the customer tenders payment or makes his or her preferred method of payment known. If the payment is made with cash, and the customer is so inclined, personal identification information can be recorded at that time. Alternatively, retailers could delete a customer’s personal identification information as soon as the customer reveals an intention to pay by credit card. In other words, the statutory mandate can hardly be described as draconian. None of these alternatives represents any great imposition on retailers.” Id. at 451–52.
customer consents and the information is not disclosed to any third party for any other purpose and is not used to market goods or services unrelated to the goods or services purchased in the transaction.\textsuperscript{280} Nevada businesses may not record a customer’s telephone number on a sales slip as a condition of accepting credit card payment.\textsuperscript{281} Oregon merchants may require personal information as a condition of purchase, but may not write such information on the credit or debit transaction slip.\textsuperscript{282}

[B] Prohibition on Disclosure of Marketing Information

California’s Credit Card Full Disclosure Act of 1986\textsuperscript{283} requires credit card issuers to provide cardholders with a written notice of their right to prohibit the disclosure of marketing information that discloses the cardholder’s identity. This written notice must advise the cardholder of his or her ability to respond either by completing a preprinted form or a toll-free number that cardholders may call to exercise this right.\textsuperscript{284}

Virginia has enacted legislation prohibiting merchants (as distinguished from credit card issuers) from selling customer information gathered in connection with a transaction without notice to the customer.\textsuperscript{285}

§ 5:7 Privacy of Insurance-Related Information

The federal Gramm-Leach-Bliley Act of 1999 (GLBA),\textsuperscript{286} requires (1) disclosure of a financial institution’s privacy policy to consumers, and (2) that the institution provide consumers an opportunity to opt out of certain disclosures of nonpublic personal information (NPI) to nonaffiliated third parties.\textsuperscript{287} Further, financial institutions are required to adopt “administrative, technical, and physical safeguards” in accordance with federal regulations to protect consumers’ nonpublic personal information.\textsuperscript{288} The GLBA applies only to “financial institutions.” However, the GLBA defines a “financial institution” extremely broadly as “any institution the business of which is engaging in financial activities as described in section 1843(k) of Title 12,” which

\textsuperscript{280} OHIO REV. CODE ANN. § 1349.17 [2005].
\textsuperscript{281} NEV. REV. STAT. § 597.940 [2009].
\textsuperscript{282} OR. REV. STAT. § 646A.214 [2007].
\textsuperscript{283} CAL. CIV. CODE § 1748.12 [2005].
\textsuperscript{284} Id. § 1748.12(b).
\textsuperscript{285} VA. CODE ANN. § 59.1-442 [2006].
\textsuperscript{287} 15 U.S.C. § 6801[a].
\textsuperscript{288} See id. § 6801[b].
is section 4(k) of the Bank Holding Company Act of 1956. Acting as an
insurance agent or broker specifically is covered under that statute.\footnote{289}

Although the GLBA is a federal law, state insurance authorities are
responsible for the enforcement of the financial institution safeguards
and disclosure/opt-out procedures required by section 6801[b] as they
are applied to “any person engaged in providing insurance.”\footnote{290}

\section*{§ 5:7.1 The National Association of Insurance
Commissioners (NAIC) Model Acts}

Most states’ GLBA-implementing statutes derive in whole or in
part from Model Acts promulgated by the NAIC,\footnote{291} a forum composed
of the insurance commissioners of all fifty states, the District of
Columbia and U.S. territories. The NAIC has issued several model
acts devoted to consumer privacy. Key differences among the acts
involve the definition of personal information covered by the acts and
the type of consent required for an insurer to share a consumer’s
personal information. Most states follow the 1982 Model Act, the
1992 Model Act or the 2003 Model Act.\footnote{292} According to the National
Association of Insurance and Financial Advisors, as of 2001, sixteen
states\footnote{293} including California, follow the 1982/1992 Model Act. The
rest essentially follow the 2003 Model Act, with the exception of
Wyoming, which has created a model loosely based on the 1992 Model
Act.

After passage of the GLBA in 1999, the sixteen states that follow
the 1982/1992 Model Act modified their insurance codes and pro-
mulgated appropriate regulations in order to comply. Pursuant to the
GLBA, the insurance codes and regulations of all fifty states include
the following three basic elements:

1. Annual notice to “customers” describing the manner in which
nonpublic personal information is collected, maintained, and
disseminated;

2. Notification of the opportunity to opt-out from the sharing of
nonpublic personal information about a “consumer” with
non-affiliated third parties for marketing purposes prior to the sharing of such information;\textsuperscript{294} and

3. Safeguards for storage of nonpublic personal information.\textsuperscript{295}

The specific contours of these elements vary somewhat from state to state.

\section*{§ 5:7.2 Definitions of “Personal Information” and Similar Terms}

The 1982 Model Act defines “personal information” as

any individually identifiable information gathered in connection with an insurance transaction from which judgments can be made about an individual’s character, habits, avocations, finances, occupation, general reputation, credit, health, or any other personal characteristics.\textsuperscript{296}

Personal information does not include “medical record information,” which, generally speaking, is information concerning one’s physical or mental condition, medical history or treatment history any of which is derived from a medical professional, medical institution, parent, spouse or guardian. Personal information also is not “privileged information,” which is information relating to claims or that is collected by insurers in anticipation of litigation or at the request of governmental authorities.\textsuperscript{297}

The 2003 Model Act contains the term “nonpublic personal information” which essentially has the same definition. The Model Acts enumerate several additional categories of protected information not discussed in detail here.\textsuperscript{298}

\section*{§ 5:7.3 The GLBA Joint Marketing Exception and 2003 Model Act States}

The key difference between states that follow the pre-GLBA model acts and the 2003 Model Act is the type of consent required prior to disclosure of nonpublic personal information for marketing purposes. In Arizona, California, Connecticut, Georgia, Illinois, Kansas, Maine,
Massachusetts, Minnesota, Montana, Nevada, New Jersey, North Carolina, Ohio, Oregon, and Virginia, covered insurance entities must obtain affirmative ("opt-in") consent from consumers prior to disclosure of any information to nonaffiliated third parties for any purpose other than the actual performance of insurance functions.\textsuperscript{299}

By contrast, pursuant to the GLBA's joint marketing exception, covered insurance entities in states that follow the 2003 Model Act may freely disclose nonpublic personal information to nonaffiliated third parties, even for marketing purposes, when such disclosure is pursuant to a "joint agreement." A "joint agreement" is "a written contract pursuant to which a licensee and one or more financial institutions jointly offer, endorse or sponsor a financial product or service."\textsuperscript{300} Furthermore, a covered insurance entity may disclose nonpublic personal information to any nonaffiliated third parties so long as the consumer is given initial and annual notice of the opportunity to opt out of disclosure and a reasonable means of doing so.\textsuperscript{301}

Another key difference between the pre- and post-GLBA model acts is that under the 1982/1992 Model Acts, customers must be given the opportunity to view and correct personal information.\textsuperscript{302}

\section*{§ 5:8 Laws Governing Disclosure and Use of Social Security Numbers}

An individual’s Social Security number (SSN) is a particularly sensitive piece of information and the number-one identifier used by criminals to commit identity theft. As a result, the all-too-familiar business practice of using SSNs as personal identifiers for routine communications and correspondence has come under fire. Policymakers at nearly every level of government and private industry are pursuing limits on the use and dissemination of SSNs in an effort to counteract the growing threat of identity theft. As is discussed in more detail below, a mesh of federal and state laws currently requires businesses and government agencies to protect the confidentiality of SSNs.

Certain federal laws with broader application to consumers’ "personal information" limit public and private sector entities’ use and disclosure of SSNs.\textsuperscript{303} For example, the Fair Credit Reporting Act

\begin{itemize}
\item \textsuperscript{299} 1982 MODEL ACT § 13; CAL. INS. CODE § 791.13.
\item \textsuperscript{300} 2003 MODEL ACT § 15(C).
\item \textsuperscript{301} 2003 MODEL ACT §§ 5–12, 15.
\item \textsuperscript{302} 1982 MODEL ACT §§ 8–9.
\item \textsuperscript{303} Over the past several years, various pieces of legislation aimed specifically at restricting the use and disclosure of SSNs in the public and/or private sectors have been considered and introduced in both houses of Congress, but no overarching SSN protection law has been enacted to date.
\end{itemize}
(FCRA) limits access to credit data (including SSNs) to those who have a permissible purpose under the law.\textsuperscript{304} Likewise, the Fair and Accurate Credit Transactions Act, which amended FCRA, allows consumers who request a copy of their credit report to ask that the first five digits of their SSN not be included in the file. Still other laws, like the Gramm-Leach-Bliley Act (GLBA),\textsuperscript{305} the Drivers Privacy Protection Act\textsuperscript{306} and the Health Insurance Portability and Accountability Act (HIPAA),\textsuperscript{307} protect the confidentiality of personally identifiable information (including SSNs) in particular industries or situations.

In addition to federal laws that restrict the use and dissemination of SSNs, more than half of all states regulate their use and disclosure by public and private entities in some significant way.\textsuperscript{308} Consistent with California’s role as a privacy leader, California adopted the first nondisclosure law pertaining to specifically SSNs, and other states quickly climbed on board, adopting similar laws with some (usually minor) variations.

\textbf{§ 5:8.1 The California Framework}

In 2001 California enacted S.B. 168 to restrict private sector use of SSNs. Senate Bill 168, codified at California Civil Code section 1798.85, generally prohibits:

\begin{quote}
(1) posting or publicly displaying SSNs (defined as intentionally communicating or making the SSNs available to the general public);
\end{quote}

\begin{footnotes}
\begin{itemize}
\item \textsuperscript{304} 15 U.S.C. § 1681b.
\item \textsuperscript{305} 15 U.S.C. § 6801 et seq.
\item \textsuperscript{306} 18 U.S.C. §§ 2721–25.
\item \textsuperscript{307} Pub. L. No. 104-191, 100 Stat. 1936 [1996].
\end{itemize}
\end{footnotes}
(2) printing SSNs on cards required to access the company’s products or services (California also prohibits embedding or encoding an SSN on such a card);\(^{309}\)

(3) requiring consumers to transmit an SSN over the Internet unless the connection is secure or the number is encrypted;

(4) requiring consumers to log onto a website using an SSN without a password; or

(5) printing SSNs on anything mailed to a customer unless required by law or the document is a form or application.\(^{310}\)

California provides exemptions from these requirements for any use, collection or release of SSNs required by state law, uses of SSNs for internal verification or administrative purposes, or documents that are required to be open to the public under state law. Approximately thirty-three states have adopted largely similar laws.\(^{311}\)

Based on the California framework, Michigan has created a more comprehensive framework for protecting SSNs. Michigan limits not only the use of the entire SSN, but also of more than four sequential digits of an SSN in the ways proscribed in California. There is a further prohibition on using all or more than four sequential digits of an SSN as a primary account number. New Jersey, Nebraska, Arizona, and South Carolina laws also protect portions of SSNs, and New York law protects numbers “derived from” SSNs.\(^{312}\)

Other state laws regarding the use of SSNs include a prohibition against requiring a consumer’s SSN to complete certain transactions, or an obligation for institutions that collect SSNs to develop a privacy policy to protect them, both discussed below.

---


311. Id. § 303.

[A] Jurisdictional Modification to the California Framework

[A]1  Prohibiting SSNs in Customer Mailings

The California framework’s requirement that SSNs not be included in customer mailings unless required by state or federal law is subject to considerable variation. Social Security numbers may, for example, be included on documents sent as part of an account application, amendment, or termination.313 But even if they may be included on customer mailings, they cannot be printed on a postcard or visible through an envelope.314

Arizona specifically exempts an entity from reviewing documents sent from a third party to determine whether SSNs are included.315 Therefore, documents from third parties may be attached to a mailing without liability as long as the mailing entity does not have actual knowledge that an SSN is included.316 Maryland includes faxes and emails as mailings, but allows SSNs to be included in emails if they are sent over a secure connection or are encrypted.317 Hawaii allows an entire SSN to be printed on employer-to-employee communications or where the communication is specifically requested by the individual.318

[A]2  Expanded Exemptions from the California Framework

The broadest exemption from this framework is available in Arizona, Colorado, Illinois, Maryland, Pennsylvania, and Vermont, which provide a grandfather clause for entities that were using SSNs in one of the prohibited manners prior to enactment of the statute. In order to continue using the SSNs, the use of the SSN must be continuous, the consumer must be provided with an annual written disclosure of the right to stop the use of their SSN in this manner, and if the individual submits a written request to cease the use of their SSN the entity must stop using the SSN within thirty days. There may be no fee or denial of services for implementing a request to stop using the SSN.319 Tennessee’s SSN protection law also includes a fairly broad exemption for any disclosure that is made for a legitimate business or government purpose and pursuant to the terms of a valid contract or other legal obligation.320 Entities engaged in the provision

313. CAL. CIV. CODE § 1798.85(a)(5).
314. Id.
315. ARIZ. REV. STAT. § 44-1373.
316. Id.
317. MD. CODE ANN., COM. LAW § 14-3402[A](6).
318. HAW. REV. STAT. § 487J-2[a](5).
319. ARIZ. REV. STAT. § 44-1373[B].
320. TENN. CODE ANN. § 47-18-2110[b].
of specified healthcare services also are exempt from Tennessee’s SSN protection law.\textsuperscript{321}

Arizona specifies that it is permissible to mail documents where the individual printed his or her own SSN on the document.\textsuperscript{322} Arkansas, Maryland, and New Jersey shield electronic communications services that are the conduit for an entity that violates the SSN regulation.\textsuperscript{323} Moreover, Maryland’s SSN protection law specifically states that it does not impose on interactive computer services or telecommunications providers any duty to monitor for the transmission of SSNs on their service.\textsuperscript{324} Maine allows exemptions from compliance with the SSN use regulations for entities that are requesting SSNs for a consumer report, supervised lenders, supervised financial organizations, insurance companies, background checks, if the SSN is used for healthcare purposes, or if the information is necessary to verify identity and prevent fraud.\textsuperscript{325} North Carolina and Hawaii do not apply the provisions regulating the use of SSNs if the number is redacted.\textsuperscript{326} Hawaii, like Maine, also provides numerous exemptions from compliance with the SSN use regulations for various entities and purposes, including the collection, use, or release of a SSN in the course of administering a claim, benefit, or procedure relating to an individual’s employment and use in connection with opening an account or the provision of or payment for a product or service authorized by an individual.\textsuperscript{327} Oregon exempts certain records or copies of records from the state’s SSN protection requirements, including records received on or before the law’s effective date, records received after the law’s effective date if the submitter could have legally protected the SSN from public disclosure, and various court records.\textsuperscript{328}

\section*{§ 5:8.2 Other State Law Regulation of the Use of Social Security Numbers}

\subsection*{[A] Requiring a Consumer’s SSN to Complete a Transaction}

Maine, Michigan, New Mexico, and Rhode Island have a broad prohibition against denying goods or services to a consumer due to

\begin{itemize}
  \item TENN. CODE ANN. § 47-18-2110(c).
  \item ARIZ. REV. STAT. § 44-1373.01(4).
  \item ARIZ. REV. STAT. § 4-86-107(c); MD. CODE ANN., COM. LAW § 14-3401; N.J. STAT. ANN. § 56:8-164.
  \item MD. CODE ANN., COM. LAW § 14-3401(c).
  \item ME. REV. STAT. ANN. tit. 10, § 1272-B(1).
  \item HAW. REV. STAT. § 487J-2[b][10]; N.C. GEN. STAT. § 75-62[b].
  \item HAW. REV. STAT. § 487J-2[b][1]-[11].
  \item OR. REV. STAT. § 646A.600 (2007).
\end{itemize}
their refusal to provide a SSN. Each has detailed exemptions from this prohibition. Michigan, for example, allows the requirement of an SSN if the requirement is authorized by applicable state or federal law, for a credit report pursuant to a FCRA permissible purpose, for a landlord to conduct a background check in connection with the lease of real property, when the transaction includes an application for extension of credit, or if the SSN is requested to complete an electronic or telephone transaction initiated by the consumer and is used solely to verify identity. Rhode Island allows licensed financial institutions to require applicants to disclose SSNs if it is required for billing purposes or for applying for a credit card. Rhode Island punishes violations with a criminal misdemeanor penalty and a $500 fine.

A Colorado entity may not require an SSN when a consumer is paying by check, unless the check is used to pay a student loan. Ohio similarly prohibits recording an SSN in connection with a check, draft or credit card payment unless the SSN is needed for a legitimate business purpose. Legitimate business purposes include collections or when the party consents to the recording of the SSN, as long as the SSN is not then disclosed to a third party for purposes other than collection. New York and Michigan also prohibit a seller from recording a purchaser’s Social Security number on a check or other negotiable instrument as a condition of accepting the instrument. Rhode Island punishes the recording of an SSN on a check with a $100 fine.

[B] Privacy Policy for Handling SSNs

Michigan requires entities that maintain SSNs to develop and publish in an electronically available employee manual a privacy policy that ensures confidentiality, prohibits unlawful disclosure, limits who has access to documents containing SSNs, describes how to properly dispose of SSNs, and establishes penalties for a breach of the privacy

330. For example, Maine exempts supervised lenders, their affiliates, and subsidiaries, supervised financial organizations, or entities that provide goods or services in conjunction with the organization; and insurers. In addition, the requirement does not apply when the SSN is used to obtain a consumer report, to obtain a background check, to obtain and bill for healthcare, and when used to prevent fraud. ME. REV. STAT. ANN. tit. 10, § 1272-B[2].
331. MICH. COMP. LAWS § 445.83.
332. R.I. GEN. LAWS § 6-13-17.
333. Id.
334. COLO. REV. STAT. § 4-3-506.
335. OHIO REV. CODE ANN. § 1349.17.
336. N.Y. GEN. BUS. LAW § 518-a; MICH COMP. LAWS § 600.2964.
policy. However, this requirement is not applicable to entities that possess SSNs in the ordinary course of business in compliance with the Fair Credit Reporting Act (FCRA) and the Gramm-Leach-Bliley Act. Other states, including New Mexico and New York, similarly require the development of a privacy policy or internal regulations for ensuring SSN confidentiality.\footnote{338} 

In Texas, a privacy policy is only required if disclosure of a consumer’s SSN is mandatory in order to obtain goods or services. The Texas law counsels that one provision of the policy “may” consist of reciting the policy to the individual at the time of SSN disclosure (and then providing written copy electronically or by mail) or by mailing the policy.\footnote{339}

Connecticut requires any person that collects SSNs in the course of business to create a privacy protection policy to be publicly displayed (including on a website). The policy must: protect confidentiality of SSNs, prohibit unlawful disclosure of SSNs, and limit access to SSNs.\footnote{340}

**[C] Employers**

In California, certain information must be provided to an employee on a pay stub or by another format at the time wages are distributed. Beginning in 2008, only the last four digits of the SSN may be shown on this statement.\footnote{341} Missouri employers may not require use of an SSN as an employee ID number or for any type of employment-related activity.\footnote{342} As part of the Oklahoma state employment code, the state prohibits an employing entity from displaying SSNs on Health Membership cards in any of the manners proscribed by California, including: publicly displayed, printed on a card, mailed, used to login to a website, or required to be transmitted unencrypted or without using a secure connection.\footnote{343} New York employers may not, unless otherwise required by law: publicly post or display an employee’s SSN; visibly print an SSN on any ID badge or card, including time card; place an SSN in files with unrestricted access; or communicate an employee’s personal identifying information to the general public.\footnote{344}

**[D] Other Modifications**

New Jersey prohibits the display of an SSN on any document intended to be recorded by the county recorder.\footnote{345} An SSN may not

\begin{footnotes}
\item[338] N.M. STAT. § 57-12B-3(d); N.Y. GEN. BUS. LAW § 399-dd|4|.
\item[339] TEX. BUS. & COM. CODE § 501.051|.053.
\item[340] CONN. GEN. STAT. § 42-471.
\item[341] CAL. LAB. CODE § 226.
\item[342] MO. REV. STAT. § 407.1355 sub. 1{|d|}.
\item[343] OKLA. STAT. tit. 40, § 173.1.
\item[344] N.Y. LAB. LAW § 203-d (2009).
\item[345] N.J. STAT. ANN. § 47:1-16.
\end{footnotes}
be a PIN code to activate any remote financial service unit in New Mexico.\footnote{N.M. STAT. § 58-16-13(b).} In North Carolina, it is unlawful to sell, lease, loan or otherwise intentionally disclose SSNs to third parties without written consent from the individual, when the entity making the disclosure knows, or with reasonable diligence would know, that the third party lacks a legitimate purpose for obtaining the information.\footnote{N.C. GEN. STAT. § 75-62(a)(6).}

§ 5:9 Unsolicited Telephone Marketing

§ 5:9.1 Telemarketing: State Do-Not-Call Laws


The FCC opined that a single national registry is more efficient and effective than having myriad national and/or state databases.\footnote{Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, CC Docket No. 02-278, Report and Order, FCC 03-153, July 3, 2003, ¶ 77 [hereinafter 1991 TCPA Order] (codified at 47 C.F.R. pts. 64, 68).} Accordingly, the system is designed so that the states can download the names on their registries into the federal registry. In a July 3, 2003 Report and Order, the FCC adopted an eighteen-month transition period for states to download their state lists into the national database.\footnote{Id.}

Though the FCC expressed a preference for a single national database, it noted that states are not precluded from continuing to maintain and use separate databases.\footnote{Id.} The states, however, may not use a list that does not include the part of the national database that relates to that state.\footnote{1991 TCPA Order, FCC 03-153 at 76–77; 47 U.S.C. § 227(e)(2).} One of the unresolved issues is whether the states that compile separate registries will, in fact, integrate their
registries into the federal database. Thus far, only a handful of states have enacted specific legislation that accomplishes this integration.\textsuperscript{355}

In addition to the issues surrounding the states’ uses of separate registries, another unresolved issue is whether the substantive provisions in the state laws are preempted by the federal regulations. The FCC has determined that the federal regulations constitute a “floor” and supersede all less restrictive do-not-call statutes.\textsuperscript{356} Thus, state laws are preempted to the extent that they are less restrictive than the federal law.\textsuperscript{357}

The federal law exempts calls made by charities, survey researchers, political campaigns, companies with which the consumer has a business relationship, and companies to which the consumer has given written consent to remain on their calling list. State laws that contain additional exemptions from liability are preempted, at least under the FCC’s interpretation. For example, California law exempts calls made by specified small businesses who call consumers with respect to goods or services offered by the small business.\textsuperscript{358} In addition to the small business exemption found in California and a few states, other states have adopted exemptions for calls made by insurance agents, newspapers, funeral directors, and others.\textsuperscript{359} These provisions appear to be preempted.

By contrast, state laws are not preempted to the extent they (i) incorporate more restrictive laws and (ii) such laws govern intrastate telemarketing. Thus, states may pass laws that contain fewer exemptions than the federal rules with respect to telemarketing that is conducted solely within that state. For example, Idaho’s exemption for calls made by charitable organizations is narrower than the federal law. The Idaho exemption applies only to calls made by minors seeking to sell goods or services for a charitable purpose or


\textsuperscript{356.} 1991 TCPA Order, at 81.

\textsuperscript{357.} 1991 TCPA Order, at 79, 81.

\textsuperscript{358.} \textsc{Cal. Bus. \& Prof. Code} § 17592[e][5] [2006].

\textsuperscript{359.} See, e.g., \textsc{Alaska Stat.} § 45.63.080 [2005] [providing exemptions for telemarketing calls made by real estate brokers, contractors, funeral directors, insurance agents, newspapers]; \textsc{Idaho Code Ann.} § 48-1005 [2005] [providing exemptions for telemarketing calls made by newspaper publishers, persons whose sales from telemarketing from the prior year were less than 60% from the result of telephone solicitations, and others]; \textsc{Miss. Code Ann.} § 77-3-711 [2006] [providing exemptions for telemarketing calls made by newspaper publishers, funeral directors, and others] (repealed effective July 1, 2010); \textsc{N.C. Gen. Stat.} § 75-103 [2005] [providing exemptions for telemarketing calls made by newspaper publishers, small businesses, and others].
organization. This provision appears to survive the federal regime, at least with respect to intrastate calls.

It is not entirely clear whether the states may enact more restrictive laws with respect to interstate telemarketing. The FCC stated that it believes “that any state regulation of interstate telemarketing calls that differs from our rules almost certainly would conflict with and frustrate the federal scheme and almost certainly would be pre-empted.” Though the FCC indicated its strong preference for federal uniformity, it left the door open to considering whether states may enact more restrictive laws governing interstate calls. It went on to state that it would “consider any alleged conflicts between state and federal requirements and the need for preemption on a case-by-case basis. Accordingly, any party that believes a state law is inconsistent with section 227 or our rules may seek a declaratory ruling from the Commission.”

§ 5:9.2 Laws Restricting Cell Phone Marketing

Cell phones currently are capable of receiving two forms of unsolicited commercial advertising: text messages and telephone calls. Unsolicited text messages fall under the purview of the federal CAN-SPAM Act to the extent that the messages are sent from Internet addresses. Such “Internet-to-phone” text messages are subject to CAN-SPAM and FCC regulations enacted thereunder, because they are initially directed by the sender to an address that contains an Internet domain reference.

CAN-SPAM and the FCC regulations do not apply, however, to text messages that are sent from “phone-to-phone” because such messages do not involve Internet domains. Phone-to-phone text messages are still subject to the prohibition under the Telephone Consumer Protection Act (TCPA) against using “automatic dialing systems” to dial cell phone numbers. Thus, the only type of text messages that are not regulated by federal law are phone-to-phone messages in which an automatic dialing system is not used to dial the number. It is doubtful

361. 1991 TCPA Order, at 84.
362. Id.
364. Id.
365. CAN-SPAM Order, ¶ 17.
366. Id. See also Joffe v. Acacia Mortgage Corp., 121 P.3d 831 (Ariz. Ct. App. 2005) [holding that company’s use of an automatic dialing system to send Internet-to-phone text messages violated the TCPA].

(Proskauer, Rel. #4, 7/10) 5–67
that telemarketers would make significant use of this “loophole” because it is probably cost-prohibitive to send bulk messages without using an automatic dialing system.

In any event, state laws might serve to plug this regulatory gap. Three states currently prohibit sending text messages to cell phones of subscribers within those states if the principal purpose is to advertise a good or service. These statutes are probably not preempted by federal law to the extent they are applied to phone-to-phone text messages that do not rely on automatic dialing systems.

In addition to the regulations governing unsolicited text messages, the FCC has promulgated regulations that govern unsolicited commercial telephone calls made to cell phones. FCC regulations prohibit using automated dialers and artificial or prerecorded voices when dialing cell phone numbers. Automated dialers are standard in the telemarketing industry, so the ability of telemarketers to make calls to consumers on their cell phones without their consent is significantly decreased. In addition, consumers can place their cell phone numbers on the National Do Not Call Registry, discussed above.

A few states have supplemented the protections afforded to cell phone users under federal law by prohibiting carriers from providing the names and cell phone numbers of their subscribers for inclusion in a telephone directory without the express consent of the subscriber.

§ 5:10 Electronic Eavesdropping

§ 5:10.1 State Statutory Schemes

Forty-nine states, and the District of Columbia, have enacted legislation making illegal one or more forms of electronic surveillance. Thirty-eight states, including New York, and the District of
Columbia, make surveillance legal with a single party’s consent. Eleven states, including California and Illinois, require that all parties consent for the surveillance to be legal.

Vermont is the only state with no law on the books addressing the interception of communications; however, the state’s highest court has held that electronic monitoring of communications in a person’s home constitutes an unlawful invasion of privacy.

—


372. Alabama, Alaska, Arizona, Arkansas, Colorado, Delaware, District of Columbia, Georgia, Hawaii, Idaho, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, Michigan, Minnesota, Mississippi, Missouri, Nebraska, New Jersey, New Mexico, New York, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Rhode Island, South Carolina, South Dakota, Tennessee, Texas, Utah, Virginia, West Virginia, Wisconsin, and Wyoming. Despite the apparently plain language of the Michigan statute requiring two-party consent, a Michigan court has interpreted the statute as not requiring two-party consent for recording by a participant in the conversations. Sullivan v. Gray, 324 N.W.2d 58 (Mich. 1982). Under Sullivan, a participant does not need the other party’s consent to record, but a third party must have both parties’ consent. However, in a 1999 decision, the Michigan Supreme Court noted that “a participant may not unilaterally nullify other participants’ expectations of privacy by secretly broadcasting the conversation.” Dickerson v. Raphael, 601 N.W.2d 108 (Mich. 1999). Thus, it appears that the Michigan courts have interpreted the statute to mean a participant can record but not broadcast the conversation without the other party’s consent.


In July 2006, the California Supreme Court expressly ruled that out-of-state companies are subject to California’s law requiring two-party consent for the recording of telephone conversations made to or received from California.375 A company may implement or maintain a practice of recording calls made to or from California clients or customers, provided that the clients or customers are informed at the outset of the call of the company’s policy of recording such calls.

§ 5:11 Radio Frequency Identification

Radio Frequency Identification (RFID) allows interested parties to identify, track, and store information on a tag that is embedded in products, cases, palettes, cards, or other objects. RFID technology has become widespread, ranging from building access control to shipment tracking. The technology has caused great concern among privacy advocates,376 and fifteen states have passed legislation addressing use of RFID technology: Arkansas, California, Delaware, Michigan, Nevada, New Hampshire, North Dakota, Oklahoma, Rhode Island, Texas, Vermont, Virginia, Washington, Wisconsin, and Wyoming. Legislation considered by Congress in 2004 died in committee.377

California prohibits the mandatory or coercive subcutaneous implanting of an RFID into any person,378 as do Oklahoma,379 North Dakota,380 and Wisconsin.381 Delaware prohibits installing a location tracking device on another’s vehicle without the owner’s or lessor’s consent.382 New Hampshire has established a commission on the use of radio frequency technology. The committee submitted its report on November 24, 2008.383 New Hampshire also prohibits the use of surveillance devices, including RFID devices, to identify ownership of a vehicle or the identity of a vehicle’s occupants.384

378. CAL. CIV. CODE § 52.7 (2008).
381. WIS. STAT. § 146.25 (2008).
Michigan and Washington require encryption or other security measures if RFID technology is used in driver’s licenses or state identification cards, and Washington prohibits, with certain exceptions, the scanning of an RFID tag by anyone except the business or agency that issued the tag. Wyoming expressly permits the use of RFID tags by telepharmacies.

Nevada prohibits capturing, storing, or reading information from a person’s RFID document for the purpose of knowingly or intentionally committing fraud, identity theft, or any other unlawful act, without that person’s prior knowledge and consent. Nevada defines an RFID document as a document containing data that are issued to an individual for the primary purpose of establishing identity. Rhode Island prohibits using RFID for tracking the movement or identity of any student on school grounds, at school functions, or while being transported to or from school grounds or school functions.

Some states have focused on RFID in driver’s licenses and personal identification cards. Arkansas prohibits the inclusion of an electronic chip or any type of RFID tag or chip in any driver’s license or identification cards. Michigan allows its secretary of state to issue an enhanced driver’s license or personal ID that contains RFID, limited to a randomly assigned number that is encrypted, if agreed to by the Department of Homeland Security. Michigan further requires the secretary of state to ensure that the RFID technology is secure from unauthorized access and includes reasonable security measures to protect against unauthorized disclosure of personal information. Vermont does not allow compiling or maintaining a database of electronically readable information from an enhanced identification card or driver’s license. Personal RFID chip numbers in Vermont will be given federal protection under the Drivers Privacy Protection Act. Virginia prohibits its Department of Motor Vehicles from following any potential federal law requiring the department to use computer chips or RFID tags in driver’s licenses or identification cards.

387. WASH. REV. CODE §§ 42.56.230, 42.56.330 (2009).
390. Id.
394. Id.
396. Id. § 8 (2008).
397. VA. CODE ANN. § 46.2-323.01 (2009).

(Proskauer, Rel. #4, 7/10)
In addition to state regulation, a number of industry leaders have agreed on principles of self-regulation. EPCglobal, an industry organization that develops standards for the electronic product code (EPC) in RFID technology, has set forth Guidelines on EPC for Consumer Products. These guidelines provide that consumers “be given clear notice of the presence of EPC on products or their packaging and will be informed of the use of EPC technology.” Further, the guidelines require that consumers “be informed of the choices that are available to discard or remove or in the future disable EPC tags from the products they acquire. It is anticipated that for most products, the EPC tags would be part of disposable packaging or would be otherwise discardable.”

Wal-Mart, one of the first retailers to try to implement EPC, has placed a list of frequently asked questions regarding EPC on its website. It explains that EPC tags will be clearly labeled on all packaging containing EPC and that customers can throw away the EPC tag if they do not want to keep it.

Procter & Gamble likewise has issued a position statement on EPC tags “supporting the application of the following privacy principles for item-level EPC:

1. Clear and accurate notice should be provided wherever EPC is being used, and consumers should be informed as to whether products they are buying contain EPC tags.

2. Consumers should have a choice as to whether EPC tags in the products they buy are permanently disabled or discarded, without incurring cost or penalty.

3. Consumers should have a choice as to whether personally identifiable information about themselves is electronically linked to the EPC number on products they buy.”

---

399. Id.
400. Id.
402. Id.