# CALIFORNIA PRIVACY LAWS

Excerpted from Chapter 26 (Data Privacy) of
*E-Commerce and Internet Law: A Legal Treatise With Forms, Second Edition*,
a 4-volume legal treatise by Ian C. Ballon (Thomson/West Publishing 2015)

SANTA CLARA UNIVERSITY LAW PRESENTS

## "HOT TOPICS IN INTERNET, CLOUD, AND PRIVACY LAW"

SANTA CLARA UNIVERSITY LAW SCHOOL
APRIL 23, 2015


**Ian C. Ballon**
**Greenberg Traurig, LLP**

**Silicon Valley:**
**1900 University Avenue, 5th Fl.**
**East Palo Alto, CA 914303**
**Direct Dial: (650) 289-7881**
**Direct Fax: (650) 462-7881**

**Los Angeles:**
**1840 Century Park East**
**Los Angeles, CA 90067**
**Direct Dial: (310) 586-6575**
**Direct Fax: (310) 586-0575**

Ballon@gtlaw.com
**<www.ianballon.net>**
**Google+, LinkedIn, Twitter, Facebook: IanBallon**



This paper has been excerpted from *E-Commerce and Internet Law: Treatise with Forms 2d Edition* (Thomson West 2015 Annual Update), a 4-volume legal treatise by Ian C. Ballon, published by West LegalWorks Publishing, 395 Hudson Street, New York, NY 10014, (212) 337-8443, www.ianballon.net.

GT GreenbergTraurig


## Ian C. Ballon

Shareholder
Internet, Intellectual Property & Technology Litigation

Admitted: California, District of Columbia and Maryland
JD, LLM, CIPP

Ballon@gtlaw.com
Google+, LinkedIn, Twitter, Facebook: Ian Ballon

Silicon Valley
1900 University Avenue
5th Floor
East Palo Alto, CA 94303
T 650.289.7881
F 650.462.7881

Los Angeles
1840 Century Park East
Los Angeles, CA 90067
T 310.586.6575
F 310.586.0575


Ian Ballon represents Internet, technology, and entertainment companies in copyright, intellectual property and Internet litigation, including the defense of privacy and behavioral advertising class action suits. He is also the author of the leading treatise on Internet law, *E-Commerce and Internet Law: Treatise with Forms 2d edition,* the 4-volume set published by West (www.IanBallon.net). In addition, he is the author of *The Complete CAN-SPAM Act Handbook* (West 2008) and *The Complete State Security Breach Notification Compliance Handbook* (West 2009) and serves as Executive Director of Stanford Law School's Center for E-Commerce.

Mr. Ballon, who practices in both Silicon Valley and LA, has brought or defended novel suits involving computer software, user generated content, rights in the cloud and in social media, links, frames, sponsored links, privacy and security, database protection, screen scraping and content aggregation, digital music, the Digital Millennium Copyright Act, rights of privacy and publicity, the enforceability of Internet Terms of Use and Privacy Policies and preemption under the CDA. A list of recent cases may be found at www.GTLaw.com/People/IanCBallon.

Mr. Ballon was named the Lawyer of the Year for Information Technology Law in the 2013 edition of Best Lawyers in America. In addition, he was the 2010 recipient of the State Bar of California IP Section's Vanguard Award and named new media lawyer of the year in 2012 by the Century City Bar Association. He is listed in Legal 500 U.S., The Best Lawyers in America (in the areas of information technology and intellectual property) and Chambers and Partners USA Guide in the areas of privacy and data security and information technology. He also has been recognized by *The Daily Journal* as one of the Top 75 IP litigators and Top 100 lawyers in California and is consistently listed as a top Northern California and Southern California litigator. Mr. Ballon also holds the CIPP certificate for the International Association of Privacy Professionals (IAPP).

## 26.13[6] Collection of Information from California Residents

### 26.13[6][A] Overview

California has enacted a number of laws governing the

---

[5]*In re Petco Animal Supplies, Inc.*, File No. 032 3221 (consent order entered Nov. 8, 2004); *see supra* § 26.13[5]; *infra* § 27.06.

[6]*See* Federal Trade Commission, "FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising" 21–22 (Feb. 2009), http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf.

[7]*See supra* §§ 26.01, 26.03.

[8]*See* FTC Report, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers (March 26, 2012), available at http://ftc.gov/os/2012/03/120326privacyreport.pdf; *see generally supra* § 26.13[4].

[9]*See infra* § 28.06.

collection of personal information from California residents, which businesses that operate on a nation-wide basis must comply with.[1]

First, California's Online Privacy Protection Act of 2003,[2] which took effect on July 1, 2004, requires operators of commercial websites and online services that collect PII about California residents over the Internet or online to conspicuously post a privacy policy that includes specific information mandated by the statute.[3] As amended effective January 1, 2014, the law also now requires disclosures by websites and online services about how users are tracked online and how the site or service responds to "do not track" settings in web browsers.[4] This law also has been specifically enforced against mobile app providers. The requirements for compliance with Cal-OPPA, as the law is referred to colloquially, are set forth in section 26.13[6][B].

Second, California Civil Code section 1798.81.5, which took effect on Jan. 1, 2005, requires most businesses that own or license personal information about California residents to implement and maintain reasonable security procedures to protect personal information from unauthorized access, destruction, use, modification or disclosure, and to contractually bind third parties who obtain this information to maintain reasonable security procedures. As discussed at greater length in section 27.04, similar provisions have since been adopted in a number of other states. This provision is addressed in section 26.13[6][C].

Third, California Civil Code sections 1798.83 and 1798.84, which took effect on Jan. 1, 2005, require businesses that disclose personal information to third parties for direct marketing purposes to make certain disclosures to consumers and, upon request, provide them with details about the

---

**[Section 26.13[6][A]]**

[1]In addition to statutes, California residents have a unique Constitutional right to privacy that affords a cause of action against even private companies. *See supra* § 26.07.

[2]Cal. Bus. & Prof. Code §§ 22575 *et seq.*

[3]As discussed below in section 26.13[8], Texas also requires that a privacy policy be posted, but only when a business collects Social Security numbers.

[4]*See* Cal. Bus. & Prof. Code §§ 22575(5), 22575(6), 22575(7).

specific information disclosed about them.[5] These laws are analyzed in section 26.13[6][D].

Fourth, the Song-Beverly Credit Card Act[6] restricts the use by merchants of personal information in connection with credit card transactions, including the collection of a person's zip code. This law is addressed in section 26.13[6][E].

Fifth, California Business & Professions Code § 22580, which takes effect on January 1, 2015, will prohibit the operator of a website, online service, online application or mobile app from marketing or advertising specified types of products or services to a minor and will require the operator to remove, or to request and obtain removal of, content or information posted by a minor, unless: (1) it was posted by a third party; (2) state or federal law require the operator to maintain it or (3) the operator anonymizes the content or information. Section 22580 will also require the operator to provide notice to a minor that the minor may remove content or information pursuant to this law. Section 22580, which has been referred to as the "Online Eraser" bill for minors, is set forth in section 26.13[6][F].

### 26.13[6][B] The Obligation to Conspicuously Post a Website or Mobile App Privacy Policy and Disclose Web Tracking Practices (California's Online Privacy Protection Act of 2003)

Operators[1] of commercial websites and online services that collect "personally identifiable information"[2] over the

---

[5]California and many other states also have enacted security breach notification and data destruction statutes that are analyzed in sections 4.07 and 4.09.

[6]Cal. Civ. Code §§ 1747 *et seq.*

**[Section 26.13[6][B]]**

[1]The term *operator* means:

> Any person or entity that owns a website located on the Internet or an online service that collects and maintains personally identifiable information from a consumer residing in California who uses or visits the website or online service if the website or online service is operated for commercial purposes. It does not include any third party that operates, hosts, or manages, but does not own, a website or online service in the owner's behalf or by processing information on behalf of the owner.

Cal. Bus. & Prof. Code § 22577(c).

[2]The term *personally identifiable information* means individually identifiable information about an individual consumer collected online by

Internet about individual consumers[3] residing in California who use or visit the site or service must conspicuously post[4]

---

the operator from that individual and maintained by the operator in an accessible form, including the following:

(1) A first and last name.

(2) A home or other physical address, including street name and name of a city or town.

(3) An email address.

(4) A telephone number.

(5) A Social Security number.

(6) Any other identifier that permits the physical or online contacting of a specific individual.

(7) Information concerning a user that the website or online service collects online from the user and maintains in personally identifiable form in combination with an identifier described in this subdivision.

Cal. Bus. & Prof. Code § 22577(a).

[3]A *consumer* is defined as "any individual who seeks or acquires, by purchase or lease, any goods, services, money, or credit for personal, family, or household purposes." Cal. Bus. & Prof. Code § 22577(d).

[4]The term *conspicuously post* with respect to a privacy policy shall include posting the privacy policy through any of the following:

(1) A Web page on which the actual privacy policy is posted if the Web page is the homepage or first significant page after entering the website.

(2) An icon that hyperlinks to a Web page on which the actual privacy policy is posted, if the icon is located on the homepage or the first significant page after entering the website, and if the icon contains the word "privacy." The icon shall also use a color that contrasts with the background color of the Web page or is otherwise distinguishable.

(3) A text link that hyperlinks to a Web page on which the actual privacy policy is posted, if the text link is located on the homepage or first significant page after entering the website, and if the text link does one of the following:

(A) Includes the word "privacy."

(B) Is written in capital letters equal to or greater in size than the surrounding text.

(C) Is written in larger type than the surrounding text, or in contrasting type, font, or color to the surrounding text of the same size, or set off from the surrounding text of the same size by symbols or other marks that call attention to the language.

(4) Any other functional hyperlink that is so displayed that a reasonable person would notice it.

(5) In the case of an online service, any other reasonably accessible means of making the privacy policy available for consumers of the online service.

Cal. Bus. & Prof. Code § 22577(b).

a privacy policy on their websites[5] (or in the case of service providers, by any other reasonably accessible means of making the policy available for consumers of their service).[6] The policy must:

- Identify the categories of personally identifiable information that the operator collects through the website or online service about individual consumers who use or visit its site or service and the categories of third-party persons or entities with whom the operator may share that personally identifiable information;
- Describe the process by which an individual consumer may review and request changes to any personally identifiable information collected, if the operator provides such an option to consumers;[7]
- Describe the process by which the operator will notify consumers who use or visit its site or service of material changes to the policy;
- Identify its effective date;
- Disclose how the operator responds to web browser "do not track" signals or other mechanisms that provide consumers the ability to exercise choice regarding the collection of personally identifiable information about an individual consumer's online activities over time and across third-party websites or online services, if the operator engages in that collection;[8] and
- Disclose whether other parties may collect personally identifiable information about an individual consumer's online activities over time and across different websites when a consumer uses the operator's website or service.[9]

Liability under California's Online Privacy Protection Act

---

[5]Cal. Bus. & Prof. Code § 22575(a).

[6]Cal. Bus. & Prof. Code § 22577(b)(5). Section 22575(a) erroneously identifies the relevant section as 22578(b)(5), which does not exist.

[7]Effective July 1, 2004, site owners were required to do so under certain circumstances. *See infra* § 26.13[6].

[8]Cal. Bus. & Prof. Code § 22575(b)(5). The requirement for disclosing how an operator responds to "do not track" signals may be satisfied "by providing a clear and conspicuous hyperlink in the operator's privacy policy to an online location containing a description, including the effects, of any program or protocol the operator follows that offers the consumer that choice." *Id*. § 22575(b)(7).

[9]Cal. Bus. & Prof. Code § 22575(b).

may be imposed if the operator "knowingly and willfully" or "negligently and materially" fails to comply with these statutory requirements or with the terms of its posted policy.[10] An operator will be deemed to be in violation of this law if it fails to post a policy in compliance with the law within thirty days of being notified of noncompliance.[11]

Starting in 2012, the California Attorney General's office began notifying mobile app providers that were not in compliance of their obligation to comply with "Cal-OPPA." In 2013, the Attorney General's Office released a booklet of guidelines for mobile compliance, entitled *Privacy on the Go,* which is reprinted in the Appendix to this chapter. In May 2014, the Attorney General issued additional guidelines for online a mobile privacy statements in light of the 2013 amendments to Cal-OPPA that address online tracking, entitled *Making Your Privacy Practices Public*. A copy of this document is also included in the Appendix to this chapter.

Businesses that do not collect personally identifiable information online, or which do not collect such information from California residents, need not comply. As a practical matter, however, all other businesses that collect personally identifiable information online should comply with the statute since there is likely no way that a business could reliably exclude California residents.[12]

Although most large consumer-oriented websites already posted privacy policies, there generally was no obligation to do so (outside of the financial services and health care industries or sites or services directed at children) prior to the adoption of this law.

Most established businesses that already have privacy policies posted on their sites likely were already in compliance with most of the provisions of the law. Many sites, however, did not otherwise identify an "effective date." Some

---

[10]Cal. Bus. & Prof. Code § 22576.

[11]Cal. Bus. & Prof. Code § 22575(a).

[12]For a discussion of geofilters and other efforts to restrict access to websites to residents of particular jurisdictions, *see infra* § 36.06. So long as it does not act negligently and materially to violate the law, a website owner or service provider that takes reasonable efforts to not collect personally identifiable information (as defined in the statute) from California residents may avoid liability. Although notice is required prior to liability being imposed, as a practical matter it could be embarrassing and harmful to the reputation of a business cited for non-compliance.

businesses that could not determine the actual date their current policies took effect opted to list an effective date of "July 1, 2004," which was the day the statute took effect.[13]

### 26.13[6][C] The Obligation to Implement and Maintain Reasonable Security Procedures

California Civil Code section 1798.81.5 mandates that a business that owns or licenses[1] personal information[2] about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification or disclosure.[3]

The statute also provide that a business that discloses personal information about a California resident pursuant to a contract with a nonaffiliated third party shall require by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification or disclosure.

Claims under section 1798.81.5 have been asserted against companies following security breaches, where plaintiffs have

---

[13]As a general rule, businesses should keep track of the dates when different versions of their privacy policies were in effect in order to be able to enforce them effectively or defend themselves in litigation or regulatory disputes.

**[Section 26.13[6][C]]**

[1]The phrase *owns or licenses* "is intended to include, but is not limited to, personal information that a business retains as part of the business' internal customer account or for the purpose of using that information in transactions with the person to whom the information relates." California Civil Code § 1798.81.5(a).

[2]*Personal information* for purposes of this statute means an individual's first name or first initial and his or her last name in combination with any one or more of the following data elements, when either the name or the date elements are not encrypted or redacted:

- Social Security number
- Driver's license number or California identification card number
- Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account
- Medical information

[3]Cal. Bus. & Prof. Code § 1798.81.5(b).

argued that the defendant breached its statutory duty to maintain reasonable security.[4]

As discussed in section 27.04[6], other states have since enacted similar statutes.

### 26.13[6][D] The Obligation to Disclose or Provide An Opt Out Right from Personal Information Transfers to Third Parties for Direct Marketing Purposes (the "Shine the Light" Law)

California Civil Code section 1798.83, sometimes referred to as the "Shine the Light" law, "does not make sharing consumer marketing information with third parties unlawful. Rather, it was designed to 'shine the light' on information-sharing practices by requiring businesses to establish procedures by which the consumer can obtain information about such practices."[1] Section 1798.83 provides that if a business with twenty or more full- or part-time employees[2] has an established business relationship[3] with a customer[4] and has within the immediately preceding calendar year

---

[4]*See, e.g.*, *In re Adobe Systems, Inc. Privacy Litig.*, __ F. Supp. 2d __, 2014 WL 4379916 (N.D. Cal. 2014) (holding that plaintiffs had standing to assert claims under Cal. Civil Code § 1798.81.5 and for declaratory relief for allegedly failing to maintain reasonable security and for unfair competition under California law for failing to warn about allegedly inadequate security in a case involving a security breach exposing the user names, passwords, credit and debit card numbers, expiration dates, and email addresses for 38 million customers); *see generally infra* § 27.07 (analyzing claims raised in security breach litigation).

**[Section 26.13[6][D]]**

[1]*Boorstein v. Men's Journal LLC,* No. CV 12-771 DSF (Ex), 2012 WL 2152815, at *1 (C.D. Cal. June 14, 2012).

[2]*See* Cal. Civil Code § 1798.83(c)(1).

[3]The term *established business relationship* is defined to mean

> a relationship formed by a voluntary, two-way communication between a business and a customer, with or without an exchange of consideration, for the purpose of purchasing, renting, or leasing real or personal property, or any interest therein, or obtaining a product or service from the business, if the relationship is ongoing and has not been expressly terminated by the business or the customer, or if the relationship is not ongoing, but is solely established by the purchase, rental, or lease of real or personal property from a business, or the purchase of a product or service, no more than eighteen months have elapsed from the date of the purchase, rental, or lease.

Cal. Civil Code § 1798.83(e)(5).

[4]a *customer* is defined as "an individual who is a resident of California who provides personal information to a business during the creation of, or throughout the duration of, an established business relationship if

disclosed[5] specified categories[6] of personal information (or certain information derived from this information)[7] to third

---

the business relationship is primarily for personal, family, or household purposes." California Civil Code § 1798.83(e)(1).

[5]A *disclosure* "means to disclose, release, transfer, disseminate, or otherwise communicate orally, in writing, or by electronic or any other means to any third party." California Civil Code § 1798.83(e)(3).

[6]The categories of personal information required to be disclosed pursuant to paragraph (1) of subdivision (a) are all of the following:

- Name and address
- Electronic mail address
- Age or date of birth
- Names of children
- Electronic mail or other addresses of children
- Number of children
- The age or gender of children
- Height
- Weight
- Race
- Religion
- Occupation
- Telephone number
- Education
- Political party affiliation
- Medical condition
- Drugs, therapies, or medical products or equipment used
- The kind of product the customer purchased, leased, or rented
- Real property purchased, leased, or rented
- The kind of service provided
- Social Security number
- Bank account number
- Credit card number
- Debit card number
- Bank or investment account, debit card, or credit card balance
- Payment history
- Information pertaining to the customer's creditworthiness, assets, income, or liabilities

California Civil Code § 1798.83(e)(6)(A).

[7]If a list, description, or grouping of customer names or addresses is derived using any of the categories listed in the preceding footnote, and is disclosed to a third party for direct marketing purposes in a manner that permits the third party to identify, determine, or extrapolate any other personal information from which the list was derived, and that personal information when it was disclosed identified, described, or was associated with an individual, the categories set forth in this subdivision that correspond to the personal information used to derive the list, description, or

parties,[8] and if the business knows or reasonably should know that the third parties used the personal information for their own direct marketing purposes,[9] the business shall, upon request[10] once per calendar year,[11] provide the customer

---

grouping shall be considered personal information for purposes of the statute. *See* California Civil Code § 1798.83(e)(6)(B).

[8]*Third party* or *third parties* mean one or more of the following:

- A business that is a separate legal entity from the business that has an established business relationship with a customer;
- A business that has access to a database that is shared among businesses, if the business is authorized to use the database for direct marketing purposes, unless the use of the database is exempt from being considered a disclosure for direct marketing purposes pursuant to section 1798.83(d);
- A business not affiliated by a common ownership or common corporate control with the business required to comply with section 1798.83(a).

California Civil Code § 1798(e)(8).

[9]*Direct marketing purposes* means "the use of personal information to solicit or induce a purchase, rental, lease, or exchange of products, goods, property, or services directly to individuals by means of the mail, telephone, or electronic mail for their personal, family, or household purposes." California Civil Code § 1798.83(e)(2). The sale, rental, exchange, or lease of personal information for consideration to businesses is a direct marketing purpose of the business that sells, rents, exchanges or obtains consideration for the personal information. California Civil Code § 1798.83(e)(2). *Direct marketing purposes* does not include the use of personal information

- by bona fide tax exempt charitable or religious organizations to solicit charitable contributions,
- to raise funds from and communicate with individuals regarding politics and government,
- by a third party when the third party receives personal information solely as a consequence of having obtained for consideration permanent ownership of accounts that might contain personal information, or
- by a third party when the third party receives personal information solely as a consequence of a single transaction where, as a part of the transaction, personal information had to be disclosed in order to effectuate the transaction.

California Civil Code § 1798.83(e)(2).

[10]Requests must be in writing or email. A business subject to the law must designate the addresses to which requests should be sent. If a business chooses to do so, it may also allow customers to make requests by toll-free telephone or facsimile numbers. *See* California Civil Code § 1798.83(b)(1). Businesses subject to the law must (a) notify all agents and managers who directly supervise employees who regularly have contact with customers of the designated addresses or means to obtain those addresses or numbers and instruct those employees that customers

free of charge (in writing or by email) within thirty (30)[12] days:

- a list of the categories disclosed for third party direct marketing purposes during the immediately preceding calendar year; and
- the names and addresses of all of the third parties that received such information and, if the nature of the third parties' business cannot reasonably be determined from their names, examples of the products or services marketed, if known to the business, sufficient to give the customer a reasonable indication of the nature of the third parties' business.[13]

The obligations under this statute may be avoided if a business otherwise required to comply with the statute (1)

---

who inquire about the company's privacy practices or compliance with this law shall be given this information; (b) add to its homepage a link either to a page titled "Your Privacy Rights" (written in a larger type than the surrounding text, or in contrasting type, font, or color, or set off by other marks or symbols that call attention to the language) or add the words "Your Privacy Rights" to a link to the business's privacy policy (in which case other words may appear on the link so long as "Your Privacy Rights" appears in the same size or style), where on the first page a customer's rights pursuant to this section and the designated addresses or numbers are listed; or (c) make the designated addresses or numbers, or means to obtain them, readily available upon request at every place of business in California where the business or its agents regularly have contact with customers. *See* California Civil Code § 1798.83(b)(1).

*Employees who regularly have contact with customers* means:

> Employees whose contact with customers is not incidental to their primary employment duties, and whose duties do not predominantly involve ensuring the safety or health of the businesses customers. It includes, but is not limited to, employees whose primary employment duties are as cashier, clerk, customer service, sales, or promotion. It does not, by way of example, include employees whose primary employment duties consist of food or beverage preparation or service, maintenance and repair of the business' facilities or equipment, direct involvement in the operation of a motor vehicle, aircraft, watercraft, amusement ride, heavy machinery or similar equipment, security, or participation in a theatrical, literary, musical, artistic, or athletic performance or contest.

California Civil Code § 1798.83(e)(4).

[11] *See* California Civil Code § 1798.83(c)(1).

[12] If a request is directed to the business at other than one of its designated addresses or numbers, it must comply within "a reasonable period in light of the circumstances related to how the request was received," but not longer than 150 days from the date received.

[13] A business that is required to comply with this statute is not obligated to provide the information associated with specific individuals and may provide the required information in standardized format. California Civil Code § 1798.83(b)(3).

adopts and discloses to the public in its privacy statement a policy of not disclosing personal information of customers to third parties for the third parties' direct marketing purposes unless the customer first affirmatively agrees to that disclosure, or of not disclosing such information if the customer has "exercised an option that prevents that information from being disclosed to third parties for those purposes," (2) maintains and discloses this policy, (3) notifies the customer of his or her right to prevent disclosure of personal information, and (4) provides the customer with a cost free means to exercise this right.[14]

In other words, a business subject to the statute must do one of the following: (1) refrain from third party transfers;[15] (2) adopt and disclose a policy of requiring opt-in consent for third party transfers;[16] (3) adopt and disclose a policy of allowing consumers to opt-out of third party disclosures;[17] or (4) allow consumers to obtain an annual written disclosure, upon request, of third party transfers.[18] Unless a business is not covered by the statute or elects not to make any third party disclosures subject to it (*i.e.,* option 1), the company must provide adequate disclosures to California residents of its opt-in policy, opt-out policy or the means for consumers to request annual disclosures[19] by "at its election, do at least one of the following:" (A) provide training to agents and managers who supervise employees who regularly have contact with customers, (B) make adequate Internet disclosures, or (C) make the information readily available upon request at every place of business in California where agents regularly have contact with customers.[20] For businesses that operate exclusively online, this likely means providing website disclosures pursuant to section 1798.83(b)(1)(B), although an Internet business potentially could comply through agent and manager training pursuant to section

---

[14]California Civil Code § 1798.83(c)(2).

[15]A business that has not disclosed specific categories of personal information to third parties are not required to comply with the law's requirements. *See* Cal. Civil Code § 1798.83(a).

[16]California Civil Code § 1798.83(c)(2).

[17]California Civil Code § 1798.83(c)(2).

[18]California Civil Code § 1798.83(b)(1)(C).

[19]The requirements for notice, as set forth in section 1798.83(b), are detailed earlier in this subsection.

[20]California Civil Code § 1798.83(b)(1).

1798.83(b)(1)(A) if employees regularly have contact with customers (or through a combination of online notice with a toll free number and training).

The law includes a non-exclusive list of disclosures (in subdivision (d)) that are not deemed to be disclosures of personal information by a business for a third parties' direct marketing purposes for purposes of the statute:

- Disclosures between a business and a third party pursuant to contracts or arrangements pertaining to any of the following:
  - ○ The processing, storage, management, or organization of personal information, or the performance of services on behalf of the business during which personal information is disclosed, if the third party that processes, stores, manages, or organizes the personal information does not use the information for a third party's direct marketing purposes and does not disclose the information to additional third parties for their direct marketing purposes;
  - ○ Marketing products or services to customers with whom the business has an established business relationship where, as a part of the marketing, the business does not disclose personal information to third parties for the third parties' direct marketing purposes;
  - ○ Maintaining or servicing accounts, including credit accounts and disclosures pertaining to the denial of applications for credit or the status of applications for credit and processing bills or insurance claims for payment;
  - ○ Public record information relating to the right, title, or interest in real property or information relating to property characteristics, as defined in section 408.3 of the Revenue and Taxation Code, obtained from a governmental agency or entity or from a multiple listing service, as defined in section 1087, and not provided directly by the customer to a business in the course of an established business relationship;
  - ○ Jointly offering a product or service pursuant to a written agreement with the third party that receives the personal information, provided that all of the following requirements are met:
    - — The product or service offered is a product or

service of, and is provided by, at least one of the businesses that is a party to the written agreement.

— The product or service is jointly offered, endorsed, or sponsored by, and clearly and conspicuously identifies for the customer, the businesses that disclose and receive the disclosed personal information.

— The written agreement provides that the third party that receives the personal information is required to maintain the confidentiality of the information and is prohibited from disclosing or using the information other than to carry out the joint offering or servicing of a product or service that is the subject of the written agreement.

○ Disclosures to or from a consumer reporting agency of a customer's payment history or other information pertaining to transactions or experiences between the business and a customer if that information is to be reported in, or used to generate, a consumer report as defined in subdivision (d) of section 1681a of Title 15 of the United States Code, and use of that information is limited by the federal Fair Credit Reporting Act;

○ Disclosure of personal information by a business to a third party financial institution solely for the purpose of the business obtaining payment for a transaction in which the customer paid the business for goods or services with a check, credit card, charge card, or debit card, if the customer seeks the information required by subdivision (a) of the business obtaining payment, whether or not the business obtaining payment knows or reasonably should know that the third party financial institution has used the personal information for its direct marketing purposes;

○ Disclosures of personal information between a licensed agent and its principal, if the personal information disclosed is necessary to complete, effectuate, administer, or enforce transactions between the principal and the agent, whether or not the licensed agent or principal also uses the personal information for direct marketing purposes, if

that personal information is used by each of them solely to market products and services directly to customers with whom both have established business relationships as a result of the principal and agent relationship; and

- ○ Disclosures of personal information between a financial institution and a business that has a private label credit card, affinity card, retail installment contract, or co branded card program with the financial institution, if the personal information disclosed is necessary for the financial institution to maintain or service accounts on behalf of the business with which it has a private label credit card, affinity card, retail installment contract, or branded card program, or to complete, effectuate, administer, or enforce customer transactions or transactions between the institution and the business, whether or not the institution or the business also uses the personal information for direct marketing purposes, if that personal information is used solely to market products and services directly to customers with whom both the business and the financial institution have established business relationships as a result of the private label credit card, affinity card, retail installment contract, or co branded card program.[21]

In addition to the exemptions created by subdivision (d), the statute, by its terms, does not apply to a financial institution that is subject to the California Financial Information Privacy Act,[22] subject to certain limitations.[23]

The statute also contains special, less demanding rules for disclosures of personal information for direct marketing purposes between affiliated third parties that share the same brand name.[24]

The requirements of this statute may not be waived. Any purported effort to waive rights created by section 1798.83

---

[21]Cal. Civil Code § 1798.83(d).

[22]*See* Cal. Fin. Code §§ 4050 *et seq*.

[23]Cal. Civil Code § 1798.83(h).

[24]*See* Cal. Civil Code § 1798.83(f).

will be treated as void and unenforceable.[25]

Customers injured by violations of section 1798.82 may initiate a civil action to obtain injunctive relief and/or damages of up to $500 per violation (or $3,000 per violation for violations that were willful, intentional or reckless).[26] Unless a violation is willful, intentional or reckless, a complete defense is provided if, within ninety days of the business learning that it had failed to provide requested information, failed to provide complete or accurate information, or failed to provide the information in a timely fashion, the business fully provides complete and accurate information.[27] In addition to damages, the statute provides that injunctive relief may be obtained against any business that violates, proposes to violate or has violated the statute.[28]

In the event of litigation, a prevailing plaintiff (but not a prevailing defendant) shall be entitled to recover reasonable attorneys' fees and costs.[29]

Beginning in 2012, a number of lawsuits were filed against companies alleged to have inadequate disclosure statements (even though in fact some of the target companies simply did not transfer personal information to third parties). Many of these cases were dismissed because the plaintiffs could not allege any statutory injury resulting from the alleged failure to provide adequate notice where the plaintiff never re-

---

[25]Cal. Civil Code § 1798.84(a). Indeed, in an unreported decision, a federal court declined to enforce a venue selection provision in a Terms of Use agreement that provided for resolution of disputes in New York under New York law in a suit brought under section 1798.83 because the court reasoned that to do so would have effectuated an impermissible waiver under section 1798.84. *See Miller v. Hearst Communications, Inc.,* No. CV 12-0733-GHK (PLAx), 2012 WL 3205241, at *3 (C.D. Cal. Aug. 3, 2012).

[26]*See* Cal. Civil Code § 1798.84.

[27]Cal. Civil Code § 1798.84(d); *see generally In re Sony Gaming Networks and Customer Data Security Breach Litigation*, 903 F. Supp. 2d 942, 973 (S.D. Cal. 2012) (dismissing putative class action claims brought by California residents because section 1798.84(d) provided a complete defense where plaintiffs alleged "that Sony either knew or should have known that its security measures were inadequate, and failed to inform Plaintiffs of the breach in a timely fashion, [and] none of Plaintiffs current allegations assert willful, intentional, or reckless conduct on behalf of Sony.").

[28]*See* Cal. Civil Code § 1798.84(e).

[29]Cal. Civil Code § 1798.84(f).

quested a disclosure.[30]

### 26.13[6][E] Collection of PII and Zip Code Information in Connection with Credit Card Transactions

Some states prohibit the collection of personal information in connection with credit card transactions, including even the mere request for a person's zip code.[1] For example, California's Song-Beverly Credit Card Act[2] makes it unlawful for any "person, firm, partnership, association, or corpora-

---

[30]*See, e.g.*, *Murray v. Time Inc.*, No. C 12-00431 JSW, 2012 WL 3634387 (N.D. Cal. Aug. 24, 2012) (dismissing, with leave to amend, plaintiff's claims under Cal. Civil Code § 1798.83 and Cal. Bus. & Professions Code § 17200 for lack of statutory standing due to lack injury and dismissing plaintiff's claim for injunctive relief for lack of Article III standing); *Boorstein v. Men's Journal LLC,* No. CV 12-771 DSF (Ex), 2012 WL 3791701 (C.D. Cal. Aug. 17, 2012) (dismissing with prejudice plaintiff's claims under Cal. Civil Code § 1798.83 and Cal. Bus. & Professions Code § 17200 for lack of statutory standing due to lack of injury); *King v. Condé Nast Publications,* No. CV-12-0719-GHK (Ex), 2012 WL 3186578 (C.D. Cal. Aug. 3, 2012) (dismissing, with leave to amend, plaintiff's claims under Cal. Civil Code § 1798.83 and Cal. Bus. & Professions Code § 17200 for lack of statutory standing due to lack of injury); *Miller v. Hearst Communications, Inc.,* No. CV 12-0733-GHK (PLAx), 2012 WL 3205241 (C.D. Cal. Aug. 3, 2012) (dismissing, with leave to amend, plaintiff's claims under Cal. Civil Code § 1798.83 and Cal. Bus. & Professions Code § 17200 for lack of statutory standing due to lack of injury); *Boorstein v. Men's Journal LLC,* No. CV 12-771 DSF (Ex), 2012 WL 2152815 (C.D. Cal. June 14, 2012) (dismissing, with leave to amend, plaintiff's claims under Cal. Civil Code § 1798.83 and Cal. Bus. & Professions Code § 17200 for lack of statutory standing due to lack of injury). These cases rejected arguments that the plaintiffs had experienced economic or informational injury.

**[Section 26.13[6][E]]**

[1]*See, e.g.*, *Pineda v. Williams-Sonoma Stores, Inc.*, 51 Cal. 4th 524, 120 Cal. Rptr. 3d 531 (2011) (California law); *Tyler v. Michaels Stores, Inc.*, 464 Mass. 492, 984 N.E.2d 737 (2013) (holding zip codes to constitute personal identification information under Massachusetts law, Mass. Gen. L. Ann. ch. 93H, § 105(a), and that a plaintiff need not allege identity theft to sue for a violation of the statute, which applies to both electronic and paper credit card forms). *But see Hancock v. Urban Outfitters, Inc.*, ___ F. Supp. 2d ___, 2014 WL 98871 (D.D.C. 2014) (holding that a zip code, by itself, is not an "address" within the meaning of the District of Columbia's Consumer Identification Information Act or District of Columbia Consumer Protection Procedures Act, D.C.Code §§ 28–3904(e), 28–3904 (f), and 28–3904 (t), and therefore dismissing plaintiff's claim against a retailer that requested the plaintiff's zip code in connection with a consumer credit card transaction).

[2]Cal. Civ. Code §§ 1747 *et seq.*

tion that accepts credit cards for the transaction of business . . .” to:

- Request, or require as a condition to accepting the credit card as payment in full or in part for goods or services, the cardholder to write any personal identification information upon the credit card transaction form or otherwise;
- Request, or require as a condition to accepting the credit card as payment in full or in part for goods or services, the cardholder to provide personal identification information, which the person, firm, partnership, association, or corporation accepting the credit card writes, causes to be written, or otherwise records upon the credit card transaction form or otherwise; or
- Utilize, in any credit card transaction, a credit card form that contains preprinted spaces specifically designated for filling in any personal identification information of the cardholder.[3]

Subject to specific exceptions, the statute, which is codified as Civil Code § 1747.08, covers information that is both required and merely requested, putting companies potentially at risk for merely *requesting* personal identification information. Unless an exception applies, the Act thus may be violated any time (1) personal identification information is (a) requested or required and (b) recorded (or written by the cardholder on the credit card transaction form or otherwise) as a condition to accepting a credit card, or (2) if a form is used with preprinted spaces specifically designed for filling in personal identification information.

*Personal identification information* (or “PII”) is defined as “information concerning the cardholder, other than information set forth on the credit card,” and includes, but is “not limited to, the cardholder’s address and telephone number.”[4]

In *Pineda v. Williams-Sonoma Stores, Inc.*,[5] the California Supreme Court held that even a customer’s zip code, without

---

[3]Cal. Civ. Code § 1747.08(a)(1).

[4]Cal. Civ. Code § 1747.08(b).

[5]*Pineda v. Williams-Sonoma Stores, Inc.*, 51 Cal. 4th 524, 120 Cal. Rptr. 3d 531 (2011).

more, is deemed *personal identification information*[6] under the statute. Based on the court's holding—and its conclusion that the definition of PII must be construed broadly[7]—the Act thus prohibits a company from requesting and recording a customer's address and telephone number (which are listed in the statute), zip code (based on the holding in *Pineda*), and potentially other data points such as some email addresses or other identifying information that do not appear on the credit card, unless a statutory exception applies.[8] In a later case, the California Supreme Court explained that section 1747.08 was enacted primarily to protect consumer privacy and prevent fraud.[9]

Section 1747.08 creates narrow exemptions for cash advance transactions, where the credit card is used as a deposit to secure payment, if the merchant is contractually obligated to provide PII to complete a credit card transaction or for a special purpose incidental but related to the transaction. Specifically, the Act does not impose liability:

- If the credit card is being used as a deposit to secure payment in the event of default, loss, damage, or other similar;
- For cash advance transactions;

---

[6]PII variously is referred to as personally identifying information and personally identifiable information, but there is no single definition of what constitutes PII. *See supra* § 26.01. The statutory term used in the Song-Beverly Credit Card Act, personal identification information, is not commonly used except in the context of that statute. For convenience, personal identification information is abbreviated in this section as PII. The California Supreme Court's interpretation of what constitutes personal identification information under the Song-Beverly Act, however, should be viewed in the specific context of that statute, and not ascribed any broader significance.

[7]The court, among other things, concluded that use of the term *concerning* evidenced an intent to broadly construe the definition of PII. *Pineda v. Williams-Sonoma Stores, Inc.*, 51 Cal. 4th 524, 531, 120 Cal. Rptr. 3d 531, 535 (2011). It likewise brushed aside the lower, intermediate appellate court's contrary conclusion, based on the doctrine of ejusdem generis, that the statute's explicit reference to address and telephone number precluded a finding that a zip code—which is merely part of an address—was of the same category as an address or telephone number and therefore covered by the Act. 51 Cal. 4th at 532, 120 Cal. Rptr. 2d at 537.

[8]*See* Ian C. Ballon & Robert Herrington, Are Your Data Collection Practices Putting Your Company At Risk?, ABA Information Security & Privacy News (Autumn 2011).

[9]*Apple v. Superior Court*, 56 Cal. 4th 128, 139–41, 151 Cal. Rptr. 3d 841 (2013) (analyzing legislative history).

- If the person, firm, partnership, association, or corporation accepting the credit card is contractually obligated to provide personal identification information in order to complete the credit card transaction or is obligated to collect and record the personal identification information by federal law or regulation; or
- If personal identification information is required for a special purpose incidental but related to the individual credit card transaction, including, but not limited to, information relating to shipping, delivery, servicing, or installation of the purchased merchandise, or for special orders.[10]

The statute also does not apply where PII is not recorded (or where a driver's license or ID number is recorded in connection with a transaction where a cardholder does not make the credit card available upon request to allow verification of the number).[11] It likewise does not apply to debit card transactions or the use of credit cards for cash advances.[12]

In *Apple, Inc. v. Superior Court*,[13] a divided California Supreme Court further held that section 1747.08 did not apply to online purchases of products that are downloaded

---

[10]Cal. Civ. Code § 1747.08(c). An intermediate appellate court held that requiring ZIP codes in pay-at-the-pump transactions at gas stations was permitted by section 1747.08 where (1) there was a high risk of fraud, (2) ZIP codes were collected solely to prevent fraud, and (3) the information was purged shortly after credit card transactions were reconciled, because the information was "required for a special purpose incidental but related to the individual credit card transaction" for the purpose of preventing fraudulent transactions. *See Flores III v. Chevron U.S.A. Inc.*, 217 Cal. App. 4th 337, 339, 158 Cal. Rptr. 3d 242, 243 (Cal. Ct. App. 2013).

[11]Cal. Civ. Code § 1747.08(d). Subpart (d) specifically provides that:

> This section does not prohibit any person, firm, partnership, association, or corporation from requiring the cardholder, as a condition to accepting the credit card as payment in full or in part for goods or services, to provide reasonable forms of positive identification, which may include a driver's license or a California state identification card, or where one of these is not available, another form of photo identification, provided that none of the information contained thereon is written or recorded on the credit card transaction form or otherwise. If the cardholder pays for the transaction with a credit card number and does not make the credit card available upon request to verify the number, the cardholder's driver's license number or identification card number may be recorded on the credit card transaction form or otherwise.

*Id.*

[12]*See* Cal. Civ. Code § 1747.03(a)(1).

[13]*Apple, Inc. v. Superior Court*, 56 Cal. 4th 128, 151 Cal. Rptr. 3d 841 (2013).

electronically.[14] A federal district court subsequently ruled more broadly that the provision does not apply to any online sales,[15] which goes beyond what the California Supreme Court was prepared to hold in *Apple, Inc. v. Superior Court*.[16]

Where applicable, section 1747.08 potentially may present compliance issues for companies that seek to collect personal information from users who are also credit card customers and record that information for marketing purposes (or who include blank spaces for PII in forms intended for consumers to fill out). Indeed, it was enacted in 1990 as an Amendment to the Song-Beverly Act of 1971 to address concern that retailers were acquiring additional personal information—beyond what was required to process credit card transactions—to build mailing and telephone lists that could be used for in-house marketing or to sell to direct mail companies or telemarketers.[17]

A person paying by credit card (or the Attorney General,

---

[14]*See Apple, Inc. v. Superior Court*, 56 Cal. 4th 128, 150, 151 Cal. Rptr. 3d 841 (2013) (holding that the statute did not apply to online purchases of downloadable files from Apple's iTunes store); *see also Saulic v. Symantec Corp.*, 596 F. Supp. 2d 1323, 1325–26 (C.D. Cal. 2009) (holding, in a case pre-dating *Apple, Inc. v. Superior Court*, that the statute was inapplicable to online purchases of downloadable anti-virus software); *Mehrens v. Redbox Automated Retail LLC*, No. 2:11-cv-02936-JHN-Ex., 2012 WL 77220, at *3-4 (C.D. Cal. Jan. 6, 2012) (holding that purchases from an automated movie rental machine, which are akin to online purchases, were not covered by section 1747.08).

[15]*See Ambers v. Buy.com, Inc.,* No. SACV 13-0196 AG (JPRx), 2013 WL 1944430, at *5–6 (C.D. Cal. Apr. 30, 2013) (holding that the Act does not apply to online transactions, even when the transaction involves merchandise that will be shipped or delivered to customers, such as the DVD purchases at issue in that case).

[16]The court in *Apple* limited its ruling to downloadable transactions. The majority wrote:

> We have no occasion here to decide whether section 1747.08 applies to online transactions that do not involve electronically downloadable products or to any other transactions that do not involve in-person, face-to-face interaction between the customer and retailer. . . . [E]ven if the statute does apply to MOTO [mail order and telephone order] transactions, we do not think such transactions, which often involve 'shipping [or] delivery . . . of the purchased merchandise,' are readily likened to online purchases of electronically downloadable products with respect to possible means of preventing or detecting fraud.

*Apple, Inc. v. Superior Court*, 56 Cal. 4th 128, 151, 151 Cal. Rptr. 3d 841 (2013).

[17]*Pineda v. Williams-Sonoma Stores, Inc.*, 51 Cal. 4th 524, 534–35, 120 Cal. Rptr. 3d 531, 539 (2011) (discussing legislative history).

District Attorney or City Attorney) may sue for violations of the statute and recover as a "civil penalty" up to $250 for an initial violation and up to $1,000 for each subsequent one.[18] The range of a penalty award, in the words of one intermediate appellate court, is "between a penny (or even the proverbial peppercorn we all encountered in law school) to the maximum amounts authorized by the statute."[19] The Attorney General, and the District Attorney or City Attorney within his or her respective jurisdiction, also are authorized to obtain injunctive relief.[20]

No penalty may be awarded, however, if a defendant shows by a preponderance of the evidence that a violation "was not intentional and resulted from a *bona fide* error made notwithstanding the defendant's maintenance of procedures reasonably adopted to avoid that error."[21] In addition, any suit seeking an award of statutory penalties must be brought within the one year of a violation.[22]

The potential availability of a statutory penalty *per violation* over a twelve month period encourages plaintiff's counsel to file putative class actions suits based on alleged violations of section 1747.08. Although the statute nominally only applies where a request for information is a *condition* of accepting a credit card transaction, Song-Beverly Act claims are easy to assert in litigation, even where a defendant ultimately may be able to prevail on the merits. Where a company is contractually obligated to record PII to comply with credit card transaction or has a special purpose for doing so—such as shipping, delivery, servicing, or installation of the purchased merchandise, or for special orders—recording PII will be permissible, although companies may find themselves embroiled in litigation over whether the information in fact was required.

Indeed, as noted later in this chapter in section 26.15, more than 150 putative class action suits alleging violations of this statute were filed just in the first half of 2011 in the

---

[18]Cal. Civ. Code § 1747.08(e).

[19]*TJX Companies, Inc. v. Superior Court*, 163 Cal. App. 4th 80, 86, 77 Cal. Rptr. 3d 114, 117 (4th Dist. 2008).

[20]Cal. Civ. Code § 1747.08(f).

[21]Cal. Civ. Code § 1747.08(e).

[22]*See TJX Companies, Inc. v. Superior Court*, 163 Cal. App. 4th 80, 84, 77 Cal. Rptr. 3d 114, 116 (4th Dist. 2008).

immediate aftermath of the *Pineda* decision.[23] While litigation of claims under section 1747.08 has dropped dramatically since that time, it remains a real risk for companies doing business with California residents.

The safest way to comply with section 1747.08 is either to not process credit card transactions or not record PII—although these options are not realistic for most e-commerce businesses.

Alternatively, a business potentially may collect PII separate and apart from processing a credit card since the statute on its face addresses requests or mandatory disclosures sought *as a condition* of accepting a credit card payment or the use of blank spaces in a pre-printed form intended for PII in any credit card transaction.[24] It may also be permissible to request PII *after,* although not before, a credit card transaction is completed.[25] A federal district court further upheld the practice of seeking personal information in connection with a loyalty rewards program, even before a trans-

---

[23]*See infra* § 26.15.

[24]*See* Cal. Civ. Code § 1747.08(a)(1).

[25]*Florez v. Linens 'N Things, Inc.*, 108 Cal. App. 4th 447, 451, 133 Cal. Rptr. 2d 465 (4th Dist. 2003) (*dicta*); *Davis v. Devanlay Retail Group, Inc.,* No. 2:11-CV-01719-KJM-CKD, 2012 WL 6589204, at *4 (E.D. Cal. Dec. 17, 2012) (holding that a policy of asking for a customer's personal information after the customer has a receipt in hand conveys that the transaction has concluded and does not violate the Song-Beverly Credit Card Act); Ian C. Ballon & Robert Herrington, Are Your Data Collection Practices Putting Your Company At Risk?, ABA Information Security & Privacy News (Autumn 2011). In rejecting the defendant's argument that collection prior to a transaction was permissible, the court in *Florez* explained that "a customer might perceive that request as a condition of credit card payment." 108 Cal. App. 4th at 453. Thus, pre-transaction collection, in this court's view, is "prohibited if it immediately preceded the credit card transaction, even if the consumer's response was voluntary and made only for marketing purposes." *Id.* As further explained by the court in *dicta*, however, nothing prevents a retailer from soliciting a consumer's address and telephone number for a store's mailing list, if that information is provided voluntarily. Retailers are not without options in this regard. 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. *Id.* at 451–52.

action is concluded.[26] In all cases, collection of PII should be consistent with a company's posted Privacy Policy.[27]

To limit or avoid liability, a company that seeks to record PII from credit card customers should set forth its policies with respect to collection of PII in connection with credit card transactions in its Privacy Policy or Terms of Use.[28] Given the number of lawsuits filed since *Pineda*, some businesses may consider even more prominent opt-in consent to a policy document identifying what PII, if any, is requested or required in connection with processing a credit card transaction and then recorded (and why), and what information should not be provided or will not be recorded. Among other things, a prominent notice could deter potential class action lawyers from filing suit if they otherwise would have misunderstood why certain information was collected or wrongly assumed that all information provided had been recorded. A clear statement of policy also may be helpful in establishing eligibility for the safe harbor by showing potentially that any improper collection of PII resulted from an error, rather than a deliberate practice.

Although perhaps tempting, a company should not seek a waiver of the requirements of section 1747.08 in its Terms of Use or Privacy Policy. The provisions of the statute may not be waived and any attempt to do so will be deemed void.[29]

Companies also should seek to benefit from the safe harbor available for errors where a defendant may show "maintenance of procedures reasonably adopted to avoid that error."[30] In addition to adopting a clear statement of its policies, as suggested above, businesses that process credit card payments from California residents should provide employees

---

[26]*See Grass v. Best Buy Co.*, 279 F.R.D. 561 (C.D. Cal. 2012). In *Grass*, the court concluded that no reasonable consumer could perceive a request for personal information to be a condition of completing a credit card transaction where a cashier first asks a customer if she wants to enroll in a rewards program, and the customer affirmatively responds, or if the customer affirmatively states that she is part of the rewards program and wishes to receive credit for the transaction but does not have her membership card with her.

[27]*See infra* § 26.14 (elements of a Privacy Statement).

[28]*See* Ian C. Ballon & Robert Herrington, Are Your Data Collection Practices Putting Your Company At Risk?, ABA Information Security & Privacy News (Autumn 2011).

[29]Cal. Civ. Code § 1747.04.

[30]Cal. Civ. Code § 1747.08(e).

with education and training about their practices and procedures to ensure that employees carefully implement them.

### 26.13[6][F] California Bus. & Prof. Code § 22580—California's "Online Eraser" Law for Minors

California Business & Professions Code § 22580, which takes effect on January 1, 2015, will prohibit the operator of a website, online service, online application or mobile app from marketing or advertising specified types of products or services to a minor and will require the operator to remove, or to request and obtain removal of, content or information posted by a minor, unless: (1) it was posted by a third party; (2) state or federal law require the operator to maintain it or (3) the operator anonymizes the content or information. Section 22580 will also require the operator to provide notice to a minor that the minor may remove content or information pursuant to this law.

The advertising restrictions purport to limit advertising to minors about alcoholic beverages, firearms, ammunition, handgun safety certificates, aerosol paint capable of defacing property, etching cream that is capable of defacing property, and any tobacco or smoking-related products.

Sections 22580 and 22581, which have been referred to as the "Online Eraser" bill for minors, provide as follows:

**Cal. Bus. & Prof. Code 22580.**

(a) An operator of an Internet Web site, online service, online application, or mobile application directed to minors shall not market or advertise a product or service described in subdivision (i) on its Internet Web site, online service, online application, or mobile application directed to minors.

(b) An operator of an Internet Web site, online service, online application, or mobile application:

(1) Shall not market or advertise a product or service described in subdivision (i) to a minor who the operator has actual knowledge is using its Internet Web site, online service, online application, or mobile application and is a minor, if the marketing or advertising is specifically directed to that minor based upon information specific to that minor, including, but not limited to, the minor's

profile, activity, address, or location sufficient to establish contact with a minor, and excluding Internet Protocol (IP) address and product identification numbers for the operation of a service.

(2) Shall be deemed to be in compliance with paragraph (1) if the operator takes reasonable actions in good faith designed to avoid marketing or advertising under circumstances prohibited under paragraph (1).

(c) An operator of an Internet Web site, online service, online application, or mobile application directed to minors or who has actual knowledge that a minor is using its Internet Web site, online service, online application, or mobile application, shall not knowingly use, disclose, compile, or allow a third party to use, disclose, or compile, the personal information of a minor with actual knowledge that the use, disclosure, or compilation is for the purpose of marketing or advertising products or services to that minor for a product described in subdivision (i).

(d) "Minor" means a natural person under 18 years of age who resides in the state.

(e) "Internet Web site, online service, online application, or mobile application directed to minors" mean an Internet Web site, online service, online application, or mobile application, or a portion thereof, that is created for the purpose of reaching an audience that is predominately comprised of minors, and is not intended for a more general audience comprised of adults. Provided, however, that an Internet Web site, online service, online application, or mobile application, or a portion thereof, shall not be deemed to be directed at minors solely because it refers or links to an Internet Web site, online service, online application, or mobile application directed to minors by using information location tools, including a directory, index, reference, pointer, or hypertext link.

(f) "Operator" means any person or entity that owns an Internet Web site, online service, online application, or mobile application. It does not include any third party that operates, hosts, or manages, but does not own, an Internet Web site, online service, online application, or mobile application on the owner's behalf or processes information on the owner's behalf.

(g) This section shall not be construed to require an operator of an Internet Web site, online service, online application, or mobile application to collect or retain age information about users.

(h) (1) With respect to marketing or advertising provided by an advertising service, the operator of an Internet Web site, online service, online application, or mobile application directed to minors shall be deemed to be in compliance with subdivision (a) if the operator notifies the advertising service, in the manner required by the advertising service, that the site, service, or application is directed to minors.

(2) If an advertising service is notified, in the manner required by the advertising service, that an Internet Web site, online service, online application, or mobile application is directed to minors pursuant to paragraph (1), the advertising service shall not market or advertise a product or service on the operator's Internet Web site, online service, online application, or mobile application that is described in subdivision (i).

(i) The marketing and advertising restrictions described in subdivisions (a) and (b) shall apply to the following products and services as they are defined under state law:

(1) Alcoholic beverages, as referenced in Sections 23003 to 23009, inclusive, and Section 25658.

(2) Firearms or handguns, as referenced in Sections 16520, 16640, and 27505 of the Penal Code.

(3) Ammunition or reloaded ammunition, as referenced in Sections 16150 and 30300 of the Penal Code.

(4) Handgun safety certificates, as referenced in Sections 31625 and 31655 of the Penal Code.

(5) Aerosol container of paint that is capable of defacing property, as referenced in Section 594.1 of the Penal Code.

(6) Etching cream that is capable of defacing property, as referenced in Section 594.1 of the Penal Code.

(7) Any tobacco, cigarette, or cigarette papers, or blunt wraps, or any other preparation of tobacco, or any other instrument or paraphernalia that is designed for the smoking or ingestion of tobacco,

products prepared from tobacco, or any controlled substance, as referenced in Division 8.5 (commencing with Section 22950) and Sections 308, 308.1, 308.2, and 308.3 of the Penal Code.

(8) BB device, as referenced in Sections 16250 and 19910 of the Penal Code.

(9) Dangerous fireworks, as referenced in Sections 12505 and 12689 of the Health and Safety Code.

(10) Tanning in an ultraviolet tanning device, as referenced in Sections 22702 and 22706.

(11) Dietary supplement products containing ephedrine group alkaloids, as referenced in Section 110423.2 of the Health and Safety Code.

(12) Tickets or shares in a lottery game, as referenced in Sections 8880.12 and 8880.52 of the Government Code.

(13) Salvia divinorum or Salvinorin A, or any substance or material containing Salvia divinorum or Salvinorin A, as referenced in Section 379 of the Penal Code.

(14) Body branding, as referenced in Sections 119301 and 119302 of the Health and Safety Code.

(15) Permanent tattoo, as referenced in Sections 119301 and 119302 of the Health and Safety Code and Section 653 of the Penal Code.

(16) Drug paraphernalia, as referenced in Section 11364.5 of the Health and Safety Code.

(17) Electronic cigarette, as referenced in Section 119405 of the Health and Safety Code.

(18) Obscene matter, as referenced in Section 311 of the Penal Code.

(19) A less lethal weapon, as referenced in Sections 16780 and 19405 of the Penal Code.

(j) The marketing and advertising restrictions described in subdivisions (a), (b), and (c) shall not apply to the incidental placement of products or services embedded in content if the content is not distributed by or at the direction of the operator primarily for the purposes of marketing and advertising of the products or services described in subdivision (i).

(k) "Marketing or advertising" means, in exchange for monetary compensation, to make a communication to one or more individuals, or to arrange for the dissemination to the public of a communication, about a

product or service the primary purpose of which is to encourage recipients of the communication to purchase or use the product or service.

**Cal. Bus. & Prof. Code § 22581**

(a) An operator of an Internet Web site, online service, online application, or mobile application directed to minors or an operator of an Internet Web site, online service, online application, or mobile application that has actual knowledge that a minor is using its Internet Web site, online service, online application, or mobile application shall do all of the following:

(1) Permit a minor who is a registered user of the operator's Internet Web site, online service, online application, or mobile application to remove or, if the operator prefers, to request and obtain removal of, content or information posted on the operator's Internet Web site, online service, online application, or mobile application by the user.

(2) Provide notice to a minor who is a registered user of the operator's Internet Web site, online service, online application, or mobile application that the minor may remove or, if the operator prefers, request and obtain removal of, content or information posted on the operator's Internet Web site, online service, online application, or mobile application by the registered user.

(3) Provide clear instructions to a minor who is a registered user of the operator's Internet Web site, online service, online application, or mobile application on how the user may remove or, if the operator prefers, request and obtain the removal of content or information posted on the operator's Internet Web site, online service, online application, or mobile application.

(4) Provide notice to a minor who is a registered user of the operator's Internet Web site, online service, online application, or mobile application that the removal described under paragraph (1) does not ensure complete or comprehensive removal of the content or information posted on the operator's Internet Web site, online service, online application, or mobile application by the registered user.

(b) An operator or a third party is not required to erase or otherwise eliminate, or to enable erasure or elimina-

tion of, content or information in any of the following circumstances:

(1) Any other provision of federal or state law requires the operator or third party to maintain the content or information.

(2) The content or information was stored on or posted to the operator's Internet Web site, online service, online application, or mobile application by a third party other than the minor, who is a registered user, including any content or information posted by the registered user that was stored, republished, or reposted by the third party.

(3) The operator anonymizes the content or information posted by the minor who is a registered user, so that the minor who is a registered user cannot be individually identified.

(4) The minor does not follow the instructions provided to the minor pursuant to paragraph (3) of subdivision (a) on how the registered user may request and obtain the removal of content or information posted on the operator's Internet Web site, online service, online application, or mobile application by the registered user.

(5) The minor has received compensation or other consideration for providing the content.

(c) This section shall not be construed to limit the authority of a law enforcement agency to obtain any content or information from an operator as authorized by law or pursuant to an order of a court of competent jurisdiction.

(d) An operator shall be deemed compliant with this section if:

(1) It renders the content or information posted by the minor user no longer visible to other users of the service and the public even if the content or information remains on the operator's servers in some form.

(2) Despite making the original posting by the minor user invisible, it remains visible because a third party has copied the posting or reposted the content or information posted by the minor.

(e) This section shall not be construed to require an operator of an Internet Web site, online service, online application, or mobile application to collect age information about users.

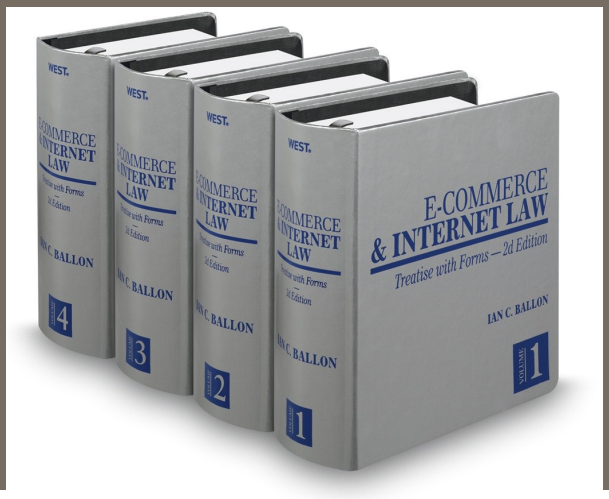
(f) "Posted" means content or information that can be accessed by a user in addition to the minor who posted the content or information, whether the user is a registered user or not, of the Internet Web site, online service, online application, or mobile application where the content or information is posted.

---

# E-COMMERCE & INTERNET LAW: TREATISE WITH FORMS,2D 2015

*Ian C. Ballon*

**The most comprehensive authority available on digital media, the cloud, mobile, social media Internet and e-commerce law**




THOMSON REUTERS™

# TAKE YOUR INTERNET AND MOBILE PRACTICE TO THE NEXT LEVEL

E-Commerce & Internet Law is a comprehensive, authoritative work covering business-to-business and business-to-customer issues, regulatory issues, and emerging trends. It includes practice tips and forms, nearly 10,000 detailed footnotes, and references to more than hundreds of unpublished court decisions, many of which are not available elsewhere. Its unique organization facilitates finding quick answers to your questions.

The updated new edition offers an unparalleled reference and practical resource. Organized into four sectioned volumes, the 59 chapters cover:

- Sources of Internet Law and Practice
- Intellectual Property
- Licenses and Contracts
- Privacy, Security and Advertising
- The Conduct and Regulation of E-Commerce
- Internet Speech, Defamation, Online Torts and the Good Samaritan Exemption
- Obscenity, Pornography, Adult Entertainment and the Protection of Children
- Theft of Digital Information and Related Internet Crimes
- Liability of Internet and Mobile Sites and Services (Including Social Networks and Blogs)
- Civil Jurisdiction and Litigation

Questions to Answer as Internet law moves to mobile devices, social media and the cloud:

- Does content syndication to mobile providers take a service provider outside the DMCA?
- How does text marketing differ from email marketing?
- Privacy issues when dealing with users who are subject to COPPA or teenagers not subject to COPPA but subject to heightened concern
- Facebook and Twitter contacts as the basis for personal jurisdiction
- How to obtain substitute service over a foreign defendant in an Internet dispute

## Key Features of E-Commerce & Internet Law

- The only treatise to comprehensively and exhaustively cover the liability of Internet and mobile service providers, cloud storage providers, bloggers, and owners and operators of social networks and other Web 2.0 applications
- Substantial caselaw coverage on Terms of Use and Internet contracts to help you draft better agreements, with sample forms and provisions
- Latest caselaw and analysis on sponsored links, key word sales, and liability for search engine optimization practices
- Includes coverage on enforcing judgments against domain names and the extent to which even unrelated claims against foreign defendants could be satisfied in U.S. courts
- Rethinking consumer criticism, gripe site, blog, and fan site law in light of new Lanham Act and CDA caselaw (including a checklist for evaluating potential claims and their viability)
- Comprehensive analysis of state law security breach notification statutes, together with practical tips on how to prepare for and respond to security breaches
- Extensive data on the prices paid for domain names and how to value them
- How to draft Privacy Policies, Terms of Use, and other documents and conduct website and privacy audits
- Practical tips, checklists, forms, and helpful information that goes well beyond what is usually included in a legal treatise
- Glossary terms drawn from the latest caselaw (helpful for briefs and contract definitions)
- Practical strategies for effectively documenting Internet transactions, drafting forms, and devising winning litigation strategies
- Exhaustive DMCA guidelines, CDA analysis, and strategies for managing user content
- Most thorough and clear cut analysis of Internet jurisdiction available anywhere
- Clear, concise, comprehensive and practical analysis

SUMMARY OF CONTENTS


## Volume 1

Part I. Sources of Internet Law and Practice: A Framework for Developing New Law

*Chapter* 1. Context for Developing the Law of the Internet
2. A Framework for Developing New Law
3. Using the Internet in Your Legal Practice: Online Resources and Strategies

Part II. Intellectual Property

4. Copyright Protection in Cyberspace
5. Database Protection and Screen Scraping
6. Trademark, Service Mark, Trade Name and Trade Dress Protection in Cyberspace
7. Rights in Internet Domain Names
8. Internet Patents

## Volume 2

*Chapter* 10. Misappropriation of Trade Secrets in Cyberspace
11. Employer Rights in the Creation and Protection of Internet-Related Intellectual Property
12. Privacy and Publicity Rights of Celebrities and Others in Cyberspace
13. Idea Protection and Misappropriation

Part III. Licenses and Contracts

14. Documenting Internet Transactions: Introduction to Drafting License Agreements and Contracts
15. Drafting Agreements in Light of Model and Uniform Contract Laws: UCITA, the UETA, Federal Legislation and the EU Distance Sales Directive
16. Internet Licenses: Content, Access and Development
17. Licensing Pre-Existing Content for Use Online: Music, Literary Works, Video, Software and User Generated Content
18. Drafting Internet Content and Development Licenses
19. Website Development and Hosting Agreements
20. Website Cross-Promotion and Cooperation: Co-Branding, Widget and Linking Agreements
21. Obtaining Assent in Cyberspace: Contract Formation for Click-Through and Other Unilateral Contracts
22. Structuring and Drafting Website Terms and Conditions
23. ISP Service Agreements
24. Software as a Service: On-Demand, Rental and Application Service Provider Agreements

Part IV. Privacy, Security and Internet Advertising

25. Introduction to Consumer Protection in Cyber space
26. Data Privacy

## Volume 3

*Chapter* 27. Internet, Network and Data Security
28. Advertising in Cyberspace
29. Spamming, Email Marketing and the Law of Unsolicited Commercial Email
30. Online Gambling

Part V. The Conduct and Regulation of Internet Commerce

31. Online Financial Transactions and Payment Mechanisms
32. Online Securities Law
33. Taxation of Electronic Commerce
34. Antitrust Restrictions on the Conduct of Electronic Commerce
35. State and Local Regulation of the Internet
36. Best Practices for U.S. Companies in Evaluating Global E-Commerce Regulations and Operating Internationally

Part VI. Internet Speech, Defamation, Online Torts and the Good Samaritan Exemption

37. Defamation, Torts and the Good Samaritan Exemption
38. Tort and Related Liability for Hacking, Cracking, Computer Viruses, Disabling Devices and Other Network Disruptions
39. E-Commerce and the Rights of Free Speech, Press and Expression In Cyberspace

## Volume 4

Part VII. Obscenity, Pornography, Adult Entertainment and the Protection of Children

*Chapter* 40. Child Pornography and Obscenity
41. Laws Regulating Non-Obscene Adult Content Directed at Children
42. U.S. Jurisdiction, Venue and Procedure in Obscenity and Other Internet Crime Cases

Part VIII. Theft of Digital Information and Related Internet Crimes

43. Detecting and Retrieving Stolen Corporate Data
44. Criminal and Related Civil Remedies for Soft ware and Digital Information Theft
45. Crimes Directed at Computer Networks and Users: Viruses and Malicious Code, Service Disabling Attacks and Threats Transmitted by Email
46. Identity Theft
47. Civil Remedies for Unlawful Seizures

Part IX. Liability of Internet Sites and Service (Including Social Networks and Blogs)

48. Assessing and Limiting Liability Through Policies, Procedures and Website Audits
49. Website Owner and Service Provider Liability for User Generated Content and User Misconduct
50. Strategies for Managing Third-Party Liability Risks
51. Web 2.0 Applications: Social Networks, Blogs, Wiki and UGC Sites

Part X. Civil Jurisdiction and Litigation

52. General Overview of Cyberspace Jurisdiction
53. Personal Jurisdiction in Cyberspace
54. Venue and the Doctrine of Forum Non Conveniens
55. Choice of Law in Cyberspace
56. Internet ADR
57. Internet Litigation
58. Email and other Electronic Communications in Litigation and in Corporate and Employer Policies
59. Use of Email in Attorney-Client


*"Should be on the desk of every lawyer who deals with cutting edge legal issues involving computers or the Internet."*
Jay Monahan
Deputy General Counsel, Zynga, Inc.

## NEW IN THE 2015 EDITION

**********
ABOUT THE AUTHOR
**********

### IAN C. BALLON

Mr. Ballon, who is admitted to practice in California, the District of Columbia and Maryland and in the U.S. District Court for the District of Colorado, represents companies in copyright, trademark, trade secret, right of publicity, privacy and security and other Internet-related cases and in defense of data privacy, security, TCPA, advertising and Internet and mobile class action suits.

Mr. Ballon was the recipient of the 2010 Vanguard Award from the State Bar of California's Intellectual Property Law Section. He also has been recognized by The Daily Journal as one of the Top 75 Intellectual Property litigators and Top 100 lawyers in California.

Mr. Ballon is listed in Legal 500 U.S., The Best Lawyers in America (in the areas of information technology and intellectual property) and Chambers and Partners USA Guide in the areas of privacy and data security and information technology. He also was recognized by the Los Angeles and San Francisco Daily Journal in 2009 for obtaining the third largest plaintiff's verdict in California in 2008 in MySpace, Inc. v. Wallace, which was one of several cases in which he served as lead counsel that created important precedents on the applicability of the CAN-SPAM Act, California's anti-phishing statute and other laws to social networks.

Mr. Ballon received his B.A. magna cum laude from Tufts University, his J.D. with honors from George Washington University Law School and an LLM in international and comparative law from Georgetown University Law Center. He also holds the C.I.P.P. certification from the International Association of Privacy Professionals.

In addition to E-Commerce and Internet Law: Treatise with Forms 2d edition, Mr. Ballon is the author of The Complete CAN-SPAM Act Handbook (West 2008) and The Complete State Security Breach Notification Compliance Handbook (West 2009), published by Thomson West (www.IanBallon.net).

He may be contacted at ballon@gtlaw.com and followed on Google+, Twitter and LinkedIn (@IanBallon).

**Contributing authors:** Ed Chansky, Emilio Varanini , Tucker McCrady, Parry Aftab and Josh Raskin

- Exhaustive coverage of the latest law and trends in data privacy, data security, TCPA and CAN-SPAM Act litigation (including class action litigation) – the most comprehensive available anywhere!
- The U.S. Supreme Court's decision in *Aereo* and its impact on public performance and direct liability case law (and the continuing validity of *Cartoon Network* in light of *Aereo*)
- New standards for false advertising law based on the U.S. Supreme Court's 2014 opinions
- Patent law in light of *Alice* and other new U.S. Supreme Court opinions (updated by Joshua Raskin)
- Exhaustive circuit-by-circuit, claim-by-claim and fact pattern analysis of the CDA, 47 U.S.C. § 203(c) – the most comprehensive available anywhere!
- Understanding the TCPA, how it differs from the CAN-SPAM Act and whether and to what extent FCC rules and guidelines impact laws and litigation governing text marketing.
- The interplay between the DMCA, the CDA and other safe harbors, defenses and exemptions available to cloud service providers, operators of social networks, mobile providers, app developers and app store hosts, service providers and employer-owned computer networks.
- The parameters of federal preemption of right of publicity and other IP claims under the Telecommunications Act.
- The latest analysis on the interplay between Internet, cloud and mobile business and antitrust law (updated by Emilio Varanini)
- New sections addressing the common law copyright issues for sound recordings in digital media and California's law prohibiting sites and services from restricting user criticism
- Updated analysis of state security breach laws in the 48 states that have them and in D.C., Puerto Rico and Guam – analyzed holistically the way a practitioner would, rather than merely by chart or graph.
- Music licensing (updated by Tucker McCrady)
- Latest law and practice on how to draft, enforce and litigate Terms of Use agreements and privacy policies for websites and mobile devices
- Complete analysis of security breach case law, statutes and trends
- Mobile, Internet and social media contests and promotions (updated by Ed Chansky)
- Latest law on sponsored links, database protection, screen scraping and search engine optimization
- Complete, updated catalogue of state statutes governing state security breach notification laws, email marketing and online dating
- Latest case law on subpoenaing data from internet, mobile and social network sites and what is permissible under ECPA and state statutory and common law privacy laws
- Hundreds of new and recent cases and FTC data privacy, security and COPPA enforcement actions and settlements
- The most comprehensive authority available on the law of digital media, the cloud, mobile and social media law as well as e-Commerce and internet law.