LITIGATION RISKS AND COMPLIANCE OBLIGATIONS UNDER THE CALIFORNIA CONSUMER PRIVACY ACT

Excerpted from Chapter 26 (Data Privacy) of
E-Commerce and Internet Law: Legal Treatise with Forms 2d Edition
A 5-volume legal treatise by Ian C. Ballon (Thomson/West Publishing, www.IanBallon.net)

PLANNING FOR AND AVOIDING CCPA CLASS ACTION LITIGATION

INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS (IAPP)

LOS ANGELES

NOVEMBER 21, 2019

Ian C. Ballon
Greenberg Traurig, LLP

Los Angeles:	Silicon Valley:
1840 Century Park East, Ste. 1900	1900 University Avenue, 5th Fl.
Los Angeles, CA 90067	East Palo Alto, CA 914303
Direct Dial: (310) 586-6575	Direct Dial: (650) 289-7881
Direct Fax: (310) 586-0575	Direct Fax: (650) 462-7881

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

This paper has been excerpted from *E-Commerce and Internet Law: Treatise with Forms 2d Edition* (Thomson West 2018 Annual Update), a 5-volume legal treatise by Ian C. Ballon, published by West, https://store.legal.thomsonreuters.com/E-Commerce--Internet-Law-Treatise; (888) 728-7677
www.ianballon.net

GT GreenbergTraurig

Ian C. Ballon

Shareholder

Internet, Intellectual Property & Technology Litigation

Admitted: California, District of Columbia and Maryland
Second, Third, Fourth, Fifth, Seventh, Ninth, Eleventh and Federal Circuits
U.S. Supreme Court
JD, LLM, CIPP/US

Ballon@gtlaw.com
LinkedIn, Twitter, Facebook: IanBallon

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

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

Ian Ballon is a litigator who is Co-Chair of Greenberg Traurig LLP's Global Intellectual Property & Technology Practice and represents Internet, technology, mobile and other companies in intellectual property and internet- and mobile-related litigation, including the defense of data privacy, security breach, and TCPA 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 5-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). He also serves as Executive Director of Stanford University Law School's Center for E-Commerce, which hosts the annual Best Practices Conference where lawyers, scholars and judges are regularly featured and interact. A list of recent cases may be found at http://www.gtlaw.com/Ian-C-Ballon-Experience.

Mr. Ballon was named the Lawyer of the Year for Information Technology Law in the 2019, 2018, 2016 and 2013 editions of Best Lawyers in America. In both 2018 and 2019 he was recognized as one of the Top 1,000 trademark attorneys in the world for his litigation practice by *World Trademark Review*. In addition, in 2019 he was named one of the top 20 Cybersecurity lawyers in California and in 2018 one of the Top Cybersecurity/Artificial Intelligence lawyers in California by the *Los Angeles and San Francisco Daily Journal*. He received the "Trailblazer" Award, Intellectual Property, 2017 from *The National Law Journal* and he has been recognized as a "Groundbreaker" in *The Recorder*'s 2017 Litigation Departments of the Year Awards. In addition, he was the 2010 recipient of the State Bar of California IP Section's Vanguard Award for significant contributions to the development of intellectual property law (http://ipsection.calbar.ca.gov/IntellectualPropertyLaw/IPVanguardAwards.aspx). 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 in California in every year that the list has been published, from 2009 through 2019, and has been listed as a Northern California Super Lawyer every year from 2004 through 2018 and as one of the Top 100 lawyers in California. Mr. Ballon also holds the CIPP/US certification from the International Association of Privacy Professionals (IAPP).

26.13A California Consumer Privacy Act (CCPA)[1]
In General

[Section 26.13A]

[1]This section was co-authored with Greenberg Traurig attorney

The California Consumer Privacy Act (CCPA)[2] was hastily enacted in 2018 to avoid a more inflexible ballot initiative that would have been next to impossible to amend.[3] The CCPA was influenced by the GDPR,[4] which took effect in the European Union and European Economic Area in May 2018, as well as prior California data privacy and consumer laws. The statute was amended in September 2018 and it is expected that it will be amended again at least one more time before it takes effect on January 1, 2020.[5] It is also possible that the enactment of CCPA could prompt Congress to adopt a federal consumer privacy law to preempt state laws so that there is a uniform national standard, as has occurred in the past with other laws such as the CAN-SPAM Act,[6] which was enacted after California enacted a very strict email marketing law. Absent federal preemption, other states may enact similar regulatory schemes—potentially with variations that could make it more complex for companies to comply. A copy of the CCPA as amended in September 2018 is reprinted at the end of this chapter at Appendix 8.

Rebekah Guyon.

[2]Cal. Civ. Code §§ 1798.100 to 1798.196.

[3]Real estate millionaire Alastair Mactaggart had spent $2 million to obtain enough signatures for a ballot initiative that would have created a comprehensive consumer privacy law, enforced through litigation. Because laws enacted through ballot initiatives in California require a supermajority to amend—and therefore are effectively almost impossible to revise—legislative and business leaders worked together to enact a somewhat better version of the law by the deadline set by Mactaggart—5 P.M. on June 28, 2018—which was the last date by which the initiative could be withdrawn from the 2018 California ballot. *See, e.g.,* Nicholas Confessore, *The Unlikely Activist Who Took On Silicon Valley—and Won,* N.Y. Times, Aug. 14, 2018. Mactaggart had an incentive to cut a deal because advertising for ballot initiatives is very costly and, even when enacted, many initiatives are subject to legal challenge. The rush to cut a deal with the millionaire backer of the consumer privacy initiative, however, resulted in a statute that was more than 10,000 words long, complex, and contained numerous errors and ambiguities. *See, e.g.,* Eric Goldman, *A First (But Very Incomplete) Crack at Inventorying the California Consumer Privacy Act's Problems,* Technology & Marketing Law Blog, July 24, 2018, available at https://blog.ericgoldman.org/archives/2018/07/a-first-but-very-incomplete-crack-at-inventorying-the-california-consumer-privacy-acts-problems.htm.

[4]*See supra* § 26.04.

[5]*See* Cal. Civ. Code § 1798.198(a) (setting the operative date of the statute as January 1, 2020, subject to the withdrawal of a ballot initiative that in fact was withdrawn).

[6]15 U.S.C.A. §§ 7701 to 7713; *see infra* § 29.03.

The CCPA imposes certain statutory obligations, which will be supplemented by regulations that the California Attorney General will issue in 2019. Subject to enumerated exclusions discussed later in this section (including businesses subject to federal financial services and health care privacy regulations), it broadly addresses the use of personal information about California residents—not merely consumers.[7] Rather than regulating the use, collection and dissemination of information obtained *by companies from consumers*, as past consumer laws did, the CCPA focuses on information *about* state residents, and therefore regulates privacy more broadly than—and addresses perceived loopholes that existed in—prior consumer privacy laws. The statute requires not simply that businesses amend their privacy policies to account for the law, but that specific notices be placed on a business's website, written contracts be entered into with service providers, and ultimately that internal practices and procedures be adjusted to ensure compliance with the statute, for those businesses that are subject to it.

The CCPA is intended to impose compliance obligations on larger business entities and those involved in selling customer information. It applies to a business "that collects[8] consumers' personal information, or on the behalf of which such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information, that does business in the State of California."[9] A business is subject to the CCPA only if it:

(1) has "annual gross revenues in excess of twenty-five million dollars"

(2) buys, receives for commercial purposes, or sells the personal information of 50,000 or more consumers, households, or devices or

---

[7]Cal. Civ. Code § 1798.140(g) (" 'Consumer' means a natural person who is a California resident, as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017, however identified, including by any unique identifier.").

[8]*Collects, collected,* or *collection* means "buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means. This includes receiving information from the consumer, either actively or passively, or by observing the consumer's behavior." Cal. Civ. Code § 1798.140(e).

[9]Cal. Civ. Code § 1798.140(c)(1).

(3) "[d]erives 50 percent or more of its annual revenues from selling consumers' personal information."[10]

The collection or sale of personal information that takes place "wholly outside of California" is not subject to the CCPA.[11]

By contract, businesses subject to the CCPA must impose use and deletion obligations with respect to personal information on *service providers*. A service provider is "a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that processes information on behalf of a business and to which the business discloses a consumer's personal information for a business purpose[12]

---

[10]Cal. Civ. Code § 1798.140(c) (defining a *business*). The law also applies to an entity "that controls or is controlled by a business . . . and that shares common branding with the business." *Id.* § 1798.140(c)(2). *Control* or *controlled* means "ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business; control in any manner over the election of a majority of the directors, or of individuals exercising similar functions; or the power to exercise a controlling influence over the management of a company. *Id. Common branding* means "a shared name, servicemark, or trademark." *Id*.

[11]Cal. Civ. Code § 1798.145(a)(6).

[12]*Business purpose* means "the use of personal information for the business's or a service provider's operational purposes, or other notified purposes, provided that the use of personal information shall be reasonably necessary and proportionate to achieve the operational purpose for which the personal information was collected or processed or for another operational purpose that is compatible with the context in which the personal information was collected." Cal. Civ. Code § 1798.140(d). The statute provides seven examples of *business purposes,* which presumably is a non-exclusive list of examples. Those examples are:

(1) Auditing related to a current interaction with the consumer and concurrent transactions, including, but not limited to, counting ad impressions to unique visitors, verifying positioning and quality of ad impressions, and auditing compliance with this specification and other standards.

(2) Detecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, and prosecuting those responsible for that activity.

(3) Debugging to identify and repair errors that impair existing intended functionality.

(4) Short-term, transient use, provided the personal information that [sic] is not disclosed to another third party and is not used to build a profile about a consumer or otherwise alter an individ-

pursuant to a written contract, provided that the contract prohibits the entity receiving the information from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract for the business, or as otherwise permitted by [the CCPA], including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract with the business."[13] Thus, a *service provider* under the CCPA is broadly defined as an entity or person that processes information for a business, but only includes persons or entities operating for profit (or financial benefit), and requires that a written contract be in place restricting the service provider's ability to retain, use or disclose personal information except as permitted by the contract or the CCPA. A service provider also must certify in its written contract with a business its compliance with the CCPA.[14] A business that discloses personal information to a service provider will not be liable under the CCPA if the service provider uses the personal information in violation of the

---

ual consumer's experience outside the current interaction, including, but not limited to, the contextual customization of ads shown as part of the same interaction.

(5) Performing services on behalf of the business or service provider, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing advertising or marketing services, providing analytic services, or providing similar services on behalf of the business or service provider.

(6) Undertaking internal research for technological development and demonstration.

(7) Undertaking activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by the business, and to improve, upgrade, or enhance the service or device that is owned, manufactured, manufactured for, or controlled by the business.

Id. Subsection 4 contains obvious typographical errors and likely was intended to refer to short-term, transient use, provided that personal information is not disclosed to a third party.

[13]Cal. Civ. Code § 1798.140(v).

[14]Cal. Civ. Code § 1798.140(w)(2)(a)(ii). The requirement that a service provider certify its compliance with the CCPA is not included in the statute's definition for *service provider*, but is separately set forth as a requirement to avoid being classified as a "third party," which would subject the business to potential liability under the CCPA. *Compare* Cal. Civ. Code § 1798.140(v) *with* Cal. Civ. Code § 1798.140(w).

CCPA, "provided that, at the time of disclosing the personal information, the business does not have actual knowledge, or reason to believe, that the service provider intends to commit such a violation."[15] A service provider will likewise not be liable under the CCPA for the obligations of a business for which it provides services.[16] Service providers are subject to enforcement actions brought by the California Attorney General[17] and presumably breach of contract actions brought by a contracting business.

Unlike a *third party*,[18] a business is not required to dis-

---

[15]Cal. Civ. Code § 1798.145(h).

[16]Cal. Civ. Code § 1798.145(h).

[17]Cal. Civ. Code § 1798.155(b).

[18]A *third party* means a person who is not any of the following:

(1) The business that collects personal information from consumers under this title.

(2)

(A) A person to whom the business discloses a consumer's personal information for a business purpose pursuant to a written contract, provided that the contract:

(i) Prohibits the person receiving the personal information from:

(I) Selling the personal information.

(II) Retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract.

(III) Retaining, using, or disclosing the information outside of the direct business relationship between the person and the business.

(ii) Includes a certification made by the person receiving the personal information that the person understands the restrictions in subparagraph (A) and will comply with them.

(B) A person covered by this paragraph that violates any of the restrictions set forth in this title shall be liable for the violations. A business that discloses personal information to a person covered by this paragraph in compliance with this paragraph shall not be liable under this title if the person receiving the personal information uses it in violation of the restrictions set forth in this title, provided that, at the time of disclosing the personal information, the business does not have actual knowledge, or reason to believe, that the person intends to commit such a violation.

Cal. Civ. Code § 1798.140(w).

close to consumers the categories of service providers to which it provides access to personal information.[19] A third party is restricted from selling personal information about a consumer sold to it by a business "unless the consumer has received explicit notice and is provided an opportunity to exercise the right to opt-out pursuant to Section 1798.120."[20]

As amended in September 2018, the Act affords California residents the rights to:

- Notice of the personal information collected and the purpose for collecting each category of information, at or before the point at which the information is collected;
- Request that a business that collects a consumer's personal information disclose the categories of personal information collected about a consumer and provide copies of the specific personal information collected;
- Request that a business that sells or discloses a consumer's personal information disclose the categories of personal information sold or disclosed about a consumer;
- Opt-out of the collection of personal information (and, for minors not otherwise subject to the Child Online Privacy Protection Act (COPPA),[21] affirmatively requires opt-in consent[22]);
- Request that a business that collects a consumer's personal information delete any personal information about the consumer that the business has collected.

The CCPA also prohibits a business from selling personal information purchased from another business without explicitly notifying the consumers whose information would be sold and providing an opportunity to opt out.[23]

Personal information includes, but is not limited to, a non-exclusive list of specific data elements,[24] "if it identifies, relates to, describes, is capable of being associated with, or could be reasonably linked, directly or indirectly, with a par-

---

[19]*Compare* Cal. Civ. Code § 1798.115(a)(2) *with* Cal. Civ. Code § 1798.140(t).

[20]Cal. Civ. Code § 1798.115(d).

[21]15 U.S.C.A. §§ 6501 to 6506; 16 C.F.R. §§ 312.1 to 312.13; *supra* § 26.13[2].

[22]Cal. Civ. Code § 1798.120(c).

[23]Cal. Civ. Code § 1798.115(d).

[24]Cal. Civ. Code § 1798.140(o)(1).

ticular consumer or household. . . .” The data elements identified in the statute, which may be supplemented by regulation,[25] are:

(A) Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver’s license number, passport number, or other similar identifiers.

(B) Any categories of personal information described in subdivision (e) of Section 1798.80.[26]

(C) Characteristics of protected classifications under California or federal law.

(D) Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.

(E) Biometric information.

(F) Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer’s interaction with an Internet website, application, or advertisement.

(G) Geolocation data.

(H) Audio, electronic, visual, thermal, olfactory, or similar information.

(I) Professional or employment-related information.

(J) Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C.A. § 1232g, 34 C.F.R. Part 99).

(K) Inferences drawn from any of the information identi-

---

[25]Cal. Civ. Code § 1798.185(a)(1).

[26]Cal. Civ. Code § 1798.80 defines *personal information* as

> any information that identifies, relates to, describes, or is capable of being associated with, a particular individual, including, but not limited to, his or her name, signature, social security number, physical characteristics or description, address, telephone number, passport number, driver’s license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information. “Personal information” does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

Id.

> fied in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.[27]

Personal information, however, excludes *publicly available information*.[28] But this exclusion is less than what meets the

---

[27]Cal. Civ. Code § 1798.140(o)(1).

[28]*Publicly available* means "information that is lawfully made available from federal, state, or local government records, if any conditions associated with such information." Cal. Civ. Code § 1798.140(o)(2). Words such as "are complied with" appear to have been omitted from the end of this sentence, which plainly appears to be a clause limiting the scope of what may constitute publicly available information. This is made clear two sentences later in the same definitional section, which provides that "information is not 'publicly available' if that data is used for a purpose that is not compatible with the purpose for which the data is maintained and made available in the government records or for which it is publicly maintained." *Id.*

The definition of what constitutes material *publicly available* also excludes "consumer information that is deidentified or aggregate consumer information." *Id.* This may seem at face value as a perplexing exclusion because government data frequently includes deidentified or aggregate consumer information. One might assume that this exclusion was not intended to apply to data released by a government agency that has been deidentified, as opposed to information deidentified by a business. However, given the language of the statute and the obligations imposed on a business that use deidentified or aggregate consumer information, it appears that the definition broadly encompasses even deidentified or aggregate consumer data provided by a government agency.

The CCPA treats consumer information that has been deidentified or presented in aggregate form as a separate category of information and imposes special obligations on businesses that use it. A business that uses deidentified or aggregate consumer information must have:

(1) implemented technical safeguards that prohibit reidentification of the consumer to whom the information may pertain.

(2) implemented business processes that specifically prohibit reidentification of the information.

(3) implemented business processes to prevent inadvertent release of deidentified information.

(4) made no attempt to reidentify the information.

Cal. Civ. Code § 1798.140(h). Otherwise, the information will be treated as *personal information* (because it will not qualify as *deidentified* or *aggregate consumer data* under the statute, and therefore will not be excluded from the definition of *personal information* as information that is *publicly available*). Hence, it appears that the legislature intended to exclude *deidentified* and *aggregate consumer data* from the definition of material that is *publicly available* to ensure that it was handled with the same

eye. Information is "not 'publicly available' if that data is used for a purpose that is not compatible with the purpose for which the data is maintained and made available in the government records or for which it is publicly maintained."[29] Accordingly, unless a business intends to use public information for the same purpose as the government entity that maintains it, public information collected, sold, or disclosed may be subject to the CCPA's disclosure and deletion requirements.

Publicly available also does not mean biometric information collected by a business about a consumer without the consumer's knowledge[30] (and thus constitutes *personal information*).

The CCPA does not restrict a business's collection, use, retention, sale, or disclosure of "deidentified" or "aggregate consumer information."[31] However, as noted earlier in connection with the definition of what constitutes information made *publicly available,* deidentified and aggregate consumer information could become *personal information* if a business fails to undertake the four protective measures included in section 1798.140(h).

Conversely, the CCPA generally does not require reidentification or de-anonymization of deidentified or aggregate consumer data so that the information would be subject to the requirements imposed on *personal information* under the law. The CCPA may not be construed to require "a business to reidentify or otherwise link information that is not maintained in a manner that would be considered personal

---

level of care by a business as information that has been de-anonymized by a private business.

[29]Cal. Civ. Code § 1798.140(o)(2).

[30]Cal. Civ. Code § 1798.140(o)(2).

[31]Cal. Civ. Code § 1798.145(a)(5). *Deidentified* is defined as "information that cannot reasonably identify, relate to, describe, or be capable of being associated with, or be linked, directly or indirectly, to a particular consumer," provided that a business has implemented the four technical safeguards and business processes discussed earlier, to prevent reidentification of the information. *Id.* § 1798.140(h). *Aggregate consumer information* is defined as information that "relates to a group or category of consumers, from which individual consumer identities have been removed" and which is "not linked or reasonably linkable to any consumer or household, including via a device." *Id.* § 1798.140(a). A collection of individual consumer records that have been deidentified, however, is not "[a]ggregate consumer information" under the CCPA. *Id.* § 1798.140(a).

information."[32]

Overall, the definition of *personal information* is quite broad. For example, the inclusion of "[i]nferences drawn from the information identified in this subdivision to create a profile about a consumer" means any time a company draws an inference about a user, the inferences themselves become personal information, subject to the statute. Likewise, the fact that public information can become *personal information* if used for a different purpose or if a business fails to treat deidentified or aggregate consumer data from a government agency as required by section 1798.140(h), reflects an expansive notion of what constitutes PII compared to other U.S. state and federal laws.

The CCPA directs the California Attorney General to issue regulations to provide greater clarity on a number of aspects of the law on or before January 1, 2020, and empowers the AG to enforce it six months after the publication of final regulations or by July 1, 2020, whichever is sooner.[33]

The statute also creates a private right of action and provides for statutory damages for a security breach involving personal information that results from a business's failure to implement and maintain reasonable security procedures, subject to a 30 day right to cure.[34]

Existing California privacy laws in effect prior to the time the CCPA takes effect are analyzed in section 26.13[6].

Notice to consumers of the personal information collected and the purpose for its collection, at or before the point at which the information is collected

The CCPA requires that a business that collects personal information from consumers notify consumers, at or before the point at which information will be collected, what categories of personal information will be collected and the purposes for which each category of personal information will be used.[35] As a corollary to this rule, the CCPA provides that a business may not "collect additional categories of personal information or use personal information collected for additional purposes" without providing this notice to a

---

[32]Cal. Civ. Code § 1798.145(i).

[33]*See.*Cal. Civ. Code § 1798.185.

[34]Cal. Civ. Code § 1798.150(a).

[35]Cal. Civ. Code § 1798.100(b).

consumer.[36]

Disclosure requirements pursuant to consumer requests

The CCPA provides California residents with a right to request disclosures of the "categories" of their personal information that a business has collected, sold, and used.[37] The "categories" referred to in these disclosure requirements "follow the definition of personal information" in the statute, which are the same categories (A) through (K) noted earlier, and may be supplemented by the California Attorney General.[38]

A business may only provide the required disclosures "upon receipt of a verifiable consumer request."[39] It likewise is not required to provide personal information requested to a consumer more than twice in a 12-month period.[40]

A business is required to disclose the information requested within "45 days of receiving a verifiable consumer request from the consumer."[41] The 45 day time period may be extended once by an additional 45 days.[42] Additionally, a business may take up to "90 additional days where necessary, taking into account the complexity and number of the requests" to respond.[43] A business is required to notify the consumer of the extension within 45 days of receiving the request and, for extensions beyond the additional 45 days,

---

[36]Cal. Civ. Code § 1798.100(b).

[37]Cal. Civ. Code §§ 1798.100, 1798.110, 1798.115.

[38]Cal. Civ. Code §§ 1798.130(c), 1798.140(o), 1798.185(a)(2).

[39]Cal. Civ. Code § 1798.100(c), Cal. Civ. Code § 1798.130(a)(2). A *verifiable consumer request* is a request "by a consumer," on his or her own behalf or on behalf of a minor child or other person authorized to act on the consumer's behalf, "that the business can reasonably verify" pursuant to regulations that the Attorney General is required to implement no later than July 1, 2020. Cal. Civ. Code § 1798.140(y). A business is not required to produce personal information if it cannot verify the identity of the requesting party. *Id.* § 1798.140(y). However, it is unclear what steps a business will be required to take to verify a consumer request after the CCPA's effective date if the Attorney General has not implemented the regulations provided in this section by then.

[40]Cal. Civ. Code § 1798.100(d).

[41]Cal. Civ. Code § 1798.130(a)(2).

[42]Cal. Civ. Code § 1798.130(a)(2).

[43]Cal. Civ. Code § 1798.145(g)(1).

the business must provide the reason for the delay.[44]

A business must deliver the information "free of charge to the consumer," unless the requests are "manifestly unfounded or excessive . . . because of their repetitive character," in which case a business may charge a "reasonable fee" for the disclosure.[45] The disclosure "shall cover the 12-month period preceding the business's receipt of the verifiable consumer request".[46] The information should be sent via a consumer's "account with the business," if one exists, and if not, it may be delivered by mail or electronically, at the consumer's option.[47] The information must be "in a portable and, to the extent technically feasible, in a readily useable format that allows the consumer to transmit this information to another entity without hindrance.[48]

If a business does not "take action on the request of the consumer, the business shall inform the consumer, without delay and at the latest within the time period permitted" for its response "of the reasons for not taking action and any rights the consumer may have to appeal the decision to the business."[49]

A business must provide consumers "two or more designated methods for submitting" disclosure requests, which must include, "at a minimum, a toll-free telephone number, and if the business maintains an Internet Web site, a Web site address."[50] A business must also ensure that its customer service representatives are "informed" of the CCPA's requirements regarding disclosure of personal information collected, sold, and disclosed, and financial incentives offered for personal information, and how to "direct consumers to exercise" their disclosure rights under the CCPA.[51]

Right to the disclosure of the categories and specific pieces of personal information collected

The CCPA provides that a "consumer shall have the right

---

[44]Cal. Civ. Code §§ 1798.130(a)(2), 1798.145(g)(1).

[45]Cal. Civ. Code § 1798.100(d); Cal. Civ. Code § 1798.145(g)(3).

[46]Cal. Civ. Code § 1798.130(a)(2).

[47]Cal. Civ. Code §§ 1798.100(d), 1798.130(a)(2).

[48]Cal. Civ. Code §§ 1798.100(d), 1798.130(a)(2).

[49]Cal. Civ. Code § 1798.145(g)(2).

[50]Cal. Civ. Code § 1798.130(a)(1)

[51]Cal. Civ. Code § 1798.130(a)(6).

to request that a business that collects a consumer's personal information disclose to that consumer the categories and specific pieces of personal information the business has collected."[52] Pursuant to section 1798.110, a consumer has the right to request that the business disclose:

(1) "the categories of personal information it has collected about that consumer"

(2) "the categories of sources from which the personal information is collected"

(3) "the business or commercial purpose for collecting or selling personal information"

(4) "the categories of third parties with whom the business shares personal information"; and

(5) "the specific pieces of personal information it has collected about that consumer."[53]

As a limiting factor, however, a business is not required to "[r]eidentify or otherwise link any data that, in the ordinary course of business, is not maintained in a manner that would be considered personal information" to comply with these disclosure requirements.[54] Thus, the fact that information may be de-anonymized or re-personalized does not mean that it is in fact subject to the statute's disclosure requirements.

Likewise, section 1798.100 does not require a business "to retain any personal information collected for a single, one-time transaction, . . ." if the information "is not sold or retained by the business or [used] to reidentify or otherwise link information that is not maintained in a manner that would be considered personal information."[55] Although drafted inartfully, this section appears intended to obviate the need for a business to retain (and hence potentially produce) personal information collected for a single, one-time transaction, provided the information is not (1) sold to third parties, (2) retained by the business, or (3) used to reidentify (or repersonalize) aggregate data or otherwise link information that would not be considered *personal information*.[56]

---

[52]Cal. Civ. Code § 1798.100(a).

[53]Cal. Civ. Code §§ 1798.110(a)(1)—(5).

[54]Cal. Civ. Code § 1798.110(d)(1).

[55]Cal. Civ. Code § 1798.100(e).

[56]Similarly, section 1798.110, which further specifies a business's

Right to the disclosure of the categories of personal information sold or disclosed

The CCPA provides that a consumer "shall have the right to request that a business that sells the consumer's personal information, or that discloses it for a business purpose" make certain disclosures to the consumer.[57] *Sell* is not limited in the statute to the exchange of personal information for money, but covers any transfer "by the business to another business or a third party for monetary or other valuable consideration."[58] The CCPA further provides that courts

---

duty to disclose personal information collected, more broadly states that a business is not required to retain personal information "collected for a single one-time transaction if, in the ordinary course of business, that information about the consumer is not retained." Cal. Civ. Code § 1798.110(d)(1).

[57]Cal. Civ. Code § 1798.115(a). What constitutes a *business purpose* is discussed earlier in this section and defined in Cal. Civ. Code § 1798.140(d).

[58]Cal. Civ. Code § 1798.140(t). The statute provides that a business does *not* sell personal information when:

(A) A consumer uses or directs the business to intentionally disclose personal information or uses the business to intentionally interact with a third party, provided the third party does not also sell the personal information, unless that disclosure would be consistent with the provisions of this title. An intentional interaction occurs when the consumer intends to interact with the third party, via one or more deliberate interactions. Hovering over, muting, pausing, or closing a given piece of content does not constitute a consumer's intent to interact with a third party.

(B) The business uses or shares an identifier for a consumer who has opted out of the sale of the consumer's personal information for the purposes of alerting third parties that the consumer has opted out of the sale of the consumer's personal information.

(C) The business uses or shares with a service provider personal information of a consumer that is necessary to perform a business purpose if both of the following conditions are met:

  (i) The business has provided notice that information being used or shared in its terms and conditions consistent with Section 1798.135.

  (ii) The service provider does not further collect, sell, or use the personal information of the consumer except as necessary to perform the business purpose.

(D) The business transfers to a third party the personal information of a consumer as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the business, provided that information is used or shared consistently with Sections 1798.110 and 1798.115. If a third party materially alters how it uses or shares the personal information of a consumer in a manner that

examining compliance with its provisions should take a liberal approach to determining whether a transaction is a sale subject to its regulation. The CCPA mandates that, where a series of "steps or transactions" are taken "with the intention of avoiding the reach of this title, including the disclosure of information by a business to a third party in order to avoid the definition of sell, a court shall disregard the intermediate steps or transactions for purposes of effectuating the purposes of this title."[59]

A consumer has the right to request disclosure of:

(1) the "categories of personal information that the business collected about the consumer";
(2) the "categories of personal information that the business sold about the consumer and the categories of third parties to whom the personal information was sold," broken down by "category or categories of personal information for each third party to whom the personal information was sold"; and
(3) the "categories of personal information that the business disclosed about the consumer for a business purpose."[60]

A business that both sells and discloses personal information is required to separately list the categories of personal information sold and disclosed in response to a consumer request.[61]

Right to the deletion of personal information

The CCPA provides that a "consumer shall have the right to request that a business delete any personal information

---

> is materially inconsistent with the promises made at the time of collection, it shall provide prior notice of the new or changed practice to the consumer. The notice shall be sufficiently prominent and robust to ensure that existing consumers can easily exercise their choices consistently with Section 1798.120. This subparagraph does not authorize a business to make material, retroactive privacy policy changes or make other changes in their privacy policy in a manner that would violate the Unfair and Deceptive Practices Act (Chapter 5 (commencing with Section 17200) of Part 2 of Division 7 of the Business and Professions Code).

Id. § 1798.140(t)(2).

[59]Cal. Civ. Code § 1798.190.

[60]Cal. Civ. Code §§ 1798.115(a)(1)—(3).

[61]Cal. Civ. Code § 1798.130(a)(4).

about the consumer which the business has collected from the consumer."[62] When a business receives a "verifiable consumer request from a consumer to delete the consumer's personal information" the business must "delete the consumer's personal information" not only from its own records, but the business must also direct any "service providers to delete the consumer's personal information from their records" as well.[63]

The CCPA carves out specific exceptions to the deletion requirement. Although not expansive, as written the exceptions allow a business to retain personal information when it is necessary for an ongoing business relationship with the consumer because the information is necessary to complete a transaction or provide a good or service that the consumer requested.[64] Additionally, a business may retain the information for internal use, as long as the use is "reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business" or "compatible with the context in which the consumer provided the information."[65] A business may also retain consumer information for the purpose of detecting "security incidents," protecting against or prosecuting malicious and fraudulent activity,[66] debugging,[67] and to comply with the California Electronic Communications Privacy Act, Cal. Penal Code § 1546 or another "legal obligation."[68] Other statutory exclusions are less clear; a business may retain and use consumers' personal information after a deletion request to "[e]xercise free speech," or

---

[62]Cal. Civ. Code § 1798.105(a).

[63]Cal. Civ. Code § 1798.105(c). A *service provider* is a for-profit entity that "process information on behalf of a business and to which the business discloses a consumer's personal information for a business purpose pursuant to a written contract." *Id.* § 1798.140(v). The definition of "service provider" additionally requires a business subject to CCPA to specify in a written contract that the provider is prohibited from using the personal information for any purpose other than that outlined in the contract. *Id.* § 1798.140(v). Businesses thus must put in place written contracts with service providers. A service provider is also required to certify to its compliance with the CCPA in its written contract with a business. *Id.* § 1798.140(w)(2)(A)(ii).

[64]Cal. Civ. Code § 1798.105(d)(1).

[65]Cal. Civ. Code §§ 1798.105(d)(7), (9).

[66]Cal. Civ. Code § 1798.105(d)(2).

[67]Cal. Civ. Code § 1798.105(d)(3).

[68]Cal. Civ. Code §§ 1798.105(d)(5), (8).

ensure another's right to exercise his or her free speech, or for the purpose of engaging in "public or peer-reviewed scientific, historical, or statistical research in the public interest."[69] Presumably, this is intended to allow an interactive computer service provider discretion to decline takedown requests directed at consumer review sites or other online discussion fora, and to protect free speech and the integrity of academic research. The exact contours of this exception, including the undefined term "public interest," have yet to be fleshed out.

Right to opt-out of the sale of personal information/ minors' right to opt-in

The CCPA gives California residents a right to opt-out of having their information sold, and requires affirmative opt-in consent from minors.

The statute provides that a "consumer shall have the right, at any time, to direct a business that sells personal information about the consumer to third parties not to sell the consumer's personal information," referred to as the "right to opt-out."[70]

A business that sells consumers' personal information is required to notify California residents of their right to opt out. This notification must be provided through "a clear and conspicuous link on the business's Internet home page, titled 'Do Not Sell My Personal Information,' " which must link to an "Internet Web page that enables a consumer" "to opt out of the sale of the consumer's personal information."[71] A business can maintain a separate homepage for California consumers with the required link if the business "takes reasonable steps to ensure that California consumers are directed" to that homepage and "not the homepage made available to the public generally."[72] A business cannot require a consumer to create an account in order to opt-out.[73] A business that sells consumers' personal information must ensure

---

[69]Cal. Civ. Code §§ 1798.105(d)(4), (6). *Research* is narrowly limited to studies "[c]ompatible with the business purpose for which the personal information was collected," and that are "[n]ot for any commercial purpose," among other limitations. Cal. Civ. Code § 1798.140(s).

[70]Cal. Civ. Code § 1798.120(a).

[71]Cal. Civ. Code § 1798.135(a)(1).

[72]Cal. Civ. Code § 1798.135(b).

[73]Cal. Civ. Code § 1798.135(a)(1).

that its customer service representatives are aware of consumers' right to opt-out and how to exercise that right.[74] After a consumer has opted out, a business is prohibited from requesting that the consumer reauthorize the sale of his or her data for "at least 12 months."[75]

With respect to minors, the CCPA prohibits businesses from selling personal information from consumers "if the business has actual knowledge that the consumer is less than 16 years of age," unless, for "consumers between 13 and 16 years of age" the consumer affirmatively authorizes the sale, or the parent or guardian of a consumer under 13 years of age affirmatively authorizes the sale.[76] The CCPA provides that a "business that willfully disregards the consumer's age shall be deemed to have actual knowledge of the consumer's age."[77] The CCPA refers to the prohibition on the sale of minors' personal information without consent as the "right to opt-in."[78]

The requirement for parental consent for children under age 13 is consistent with the federal Child Online Privacy Protection Act (COPPA).[79] Federal law does not generally regulate child privacy for those aged 13 and older, although the FTC has identified minors in this age group as deserving of closer attention.[80] The CCPA provides special protection for this class of people, although inartful draftsmanship makes it unclear whether the law covers those who are 16 and on its face appears to exclude minors who are age 13, which presumably was not the drafters' intent. Presumably, the CCPA's opt-in right should apply to teenagers aged 13, 14 and 15, but the language of the statute is not entirely clear.[81]

---

[74]Cal. Civ. Code § 1798.135(a)(3).

[75]Cal. Civ. Code § 1798.135(a)(5).

[76]Cal. Civ. Code § 1798.120(c).

[77]Cal. Civ. Code § 1798.120(c).

[78]Cal. Civ. Code § 1798.120(c).

[79]15 U.S.C.A. §§ 6501 to 6506; 16 C.F.R. §§ 312.1 to 312.13; *see generally supra* § 26.13[2].

[80]*See supra* § 26.13[2][H].

[81]*See* Cal. Civ. Code § 1798.120(c); Eric Goldman, *California Amends the Consumer Privacy Act (CCPA); Fixes About 0.01% of its Problems*, Technology & Marketing Law Blog (Oct. 4, 2018), available at https://blog.ericgoldman.org/archives/2018/10/california-amends-the-consumer-

Nondiscrimination and Financial incentives

The CCPA generally prohibits businesses from discriminating against consumers based on their exercise of any rights provided in the statute.[82] Discrimination includes denying a consumer goods or services, charging different prices or rates, providing a different level or quality of goods or services, and/or suggesting that a consumer will receive a different price, rate, or level or quality of goods or services.[83] However, the CCPA also provides that businesses are not prohibited from "charging a consumer a different price or rate, or from providing a different level or quality of goods or services to the consumer, if that difference is reasonably related to the value provided to the consumer by the consumer's data."[84]

The CCPA also allows a business to offer "financial incentives" for the collection, sale, or deletion of personal information. These incentives may only be provided on an opt-in basis, and include "payments to consumers as compensation," or a "different price, rate, level or quality of goods or services to the consumer if that price is directly related to the value provided to the consumer by the consumer's data."[85]

In other words, a business may not discriminate against a consumer who declines to provide consent or requests deletion of personal information, but it may provide financial incentives for a consumer not to do so. Financial incentives must be correlated to the value of a consumer's information.

---

privacy-act-ccpa-fixes-about-0-01-of-its-problems.htm ("The language is inconsistent about 16 year olds (or, if you read the restriction as applying only to 14 and 15 year olds, then it's inconsistent about 13 year olds): 'a business shall not sell the personal information of consumers if the business has actual knowledge that the consumer is **less than 16 years of age**, unless the consumer, in the case of consumers **between 13 and 16 years of age**, or the consumer's parent or guardian, in the case of consumers who are **less than 13 years of age**, has affirmatively authorized the sale of the consumer's personal information.' ").

[82]Cal. Civ. Code § 1798.125(a).

[83]Cal. Civ. Code § 1798.125(a)(1).

[84]Cal. Civ. Code § 1798.125(a)(2). This sentence is inartfully worded but presumably speaks to any difference between the value provided, or price charged, to consumers, and the value of a consumer's personal information. This meaning of this provision is likely to be fleshed out by the California Attorney General.

[85]Cal. Civ. Code §§ 1798.125(b)(1), (3).

De minimis payments for information of great value thus are unlikely to pass muster. What constitutes fair value presumably will be clarified in regulations to be promulgated by the California Attorney General or through enforcement actions by the Attorney General.

Required privacy policy disclosures

The CCPA requires that businesses that collect, sell, or disclose California residents' personal information publicly inform consumers of their rights under the CCPA. These disclosures must be made in a business's "online privacy policy," "in any California-specific description of consumers' privacy rights," or, if the business does not maintain those policies, "on its Internet Web site."[86] A business must update these disclosures "at least once every 12 months."[87] The disclosure must include "one or more designated methods for submitting" disclosure requests under the statute.[88]

Additionally, a business must disclose the categories of personal information that it has collected, sold, or disclosed in the previous 12 months.[89] A business that collects consumers' personal information is required to disclose:

(1) the "categories of personal information it has collected about" consumers;
(2) the "categories of sources from which the personal information is collected";
(3) the "business or commercial purpose for collecting or selling personal information";
(4) the "categories of third parties with whom the business shares personal information"; and
(5) the "specific pieces of personal information the business has collected about that consumer."[90]

A business that sells or discloses consumers' personal in-

---

[86]Cal. Civ. Code § 1798.130(a)(5)

[87]Cal. Civ. Code § 1798.130(a)(5).

[88]Cal. Civ. Code § 1798.130(a)(5)(A).

[89]The "categories of personal information" referred to in the privacy policy disclosure requirements "follow the definition of personal information in Section 1798.140." Cal. Civ. Code § 1798.130(c).

[90]Cal. Civ. Code §§ 1798.110(c)(1)—(5). Although subsection (5) is technically included in the list of public disclosures that a business is required to make pursuant to section 1798.130, its inclusion is likely a mistake. The California legislature presumably did not intend for a business to publicly disclose "specific pieces of personal information" collected about an individual consumer. More likely, it intended to require disclosure

formation is required to disclose separately the categories of personal information that it has sold and disclosed within the last 12 months. Alternatively, if the business has not sold or disclosed consumer personal information in the preceding 12 months, it must "disclose that fact."[91]

A business that sells consumers' personal information must additionally include in its privacy policy, or in a California-specific description of privacy rights, a description of a consumer's rights under the CCPA to opt-out and include the link titled "Do Not Sell My Personal Information" in the document.[92]

A business that offers financial incentives for the collection, sale, or deletion of personal information must notify consumers of the incentives in its privacy policy or other public disclosure document.[93]

Scope and exclusions

The California legislature mandated that the CCPA "be liberally construed to effectuate its purposes."[94] It expressly preempts all rules, regulations, codes, ordinances, and other laws adopted by a city, county, city and county, municipality, or local agency regarding the collection and sale of consumers' personal information by a business.[95] The CCPA is intended to supplement federal and state law, if permissible, but is not intended to apply if it would be preempted by, or in conflict with, federal law or the U.S. or California Constitution.[96]

The CCPA provides that compliance with its obligations "shall not restrict a business's ability" to comply with other applicable laws or a civil or criminal investigation, cooperate with law enforcement agencies, or exercise or defend legal claims.[97] The CCPA does not "apply where compliance by the business with the title would violate an evidentiary privilege

---

of the type of personal information it collects generally from consumers.

[91]Cal. Civ. Code §§ 1798.130(a)(5)(C)(i)—(ii).

[92]Cal. Civ. Code § 1798.135(a)(2).

[93]Cal. Civ. Code § 1798.125(b)(2); Cal. Civ. Code § 1798.130(a)(5)(A).

[94]Cal. Civ. Code § 1798.194.

[95]Cal. Civ. Code § 1798.180. Unlike the rest of the CCPA, which is set to take effect on January 1, 2020, this preemption provision became immediately effective upon enactment in 2018. *See id.* § 1798.199.

[96]Cal. Civ. Code § 1798.196.

[97]Cal. Civ. Code §§ 1798.145(a)(1)–(4).

under California law," such as the attorney-client privilege, and the statute further does not apply to medical information or health information that is regulated by federal law, or information collected as part of a clinical trial subject to federal law.[98] The CCPA also does not apply to the sale of personal information "to or from a consumer reporting agency if that information is to be reported in, or used to generate, a consumer report" subject to the Fair Credit Reporting Act, 15 U.S.C. §§ 1681, *et seq.*, or to personal information collected, processed, sold or disclosed pursuant to the Gramm-Leahy-Bliley Act (Public Law 106-102), the California Financial Information Privacy Act, Cal. Fin. Code §§ 4050—4060, or the Driver's Privacy Protection Act, 18 U.S.C. §§ 2721 *et seq.*[99]

The CCPA also may not be applied to infringe upon the noncommercial free speech rights protected by the California Constitution.[100]

Attorney General enforcement

---

[98]Cal. Civ. Code § 1798.145(c)(1).

[99]Cal. Civ. Code §§ 1798.145(d) - (f).

[100]Cal. Civ. Code § 1798.145(k) ("The rights afforded to consumers and the obligations imposed on any business under this title shall not apply to the extent that they infringe on the noncommercial activities of a person or entity described in subdivision (b) of Section 2 of Article I of the California Constitution."). Article I section 2(b) of the California Constitution provides that:

> A publisher, editor, reporter, or other person connected with or employed upon a newspaper, magazine, or other periodical publication, or by a press association or wire service, or any person who has been so connected or employed, shall not be adjudged in contempt by a judicial, legislative, or administrative body, or any other body having the power to issue subpoenas, for refusing to disclose the source of any information procured while so connected or employed for publication in a newspaper, magazine or other periodical publication, or for refusing to disclose any unpublished information obtained or prepared in gathering, receiving or processing of information for communication to the public.
>
> Nor shall a radio or television news reporter or other person connected with or employed by a radio or television station, or any person who has been so connected or employed, be so adjudged in contempt for refusing to disclose the source of any information procured while so connected or employed for news or news commentary purposes on radio or television, or for refusing to disclose any unpublished information obtained or prepared in gathering, receiving or processing of information for communication to the public.
>
> As used in this subdivision, "unpublished information" includes information not disseminated to the public by the person from whom disclosure is sought, whether or not related information has been disseminated and includes, but is not limited to, all notes, outtakes, photographs, tapes or other data of whatever sort not itself disseminated to the public through a medium of communication,

The law delegates to the California Attorney General responsibilities analogous to those given the Federal Trade Commission by Congress under the Children's Online Privacy Protection Act (COPPA),[101] Health Insurance Portability and Accountability Act (HIPAA)[102] and Gramm-Leach-Bliley (GLB).[103] The Attorney General is delegated authority to adopt regulations,[104] provide opinions, and file suit to enforce the law (subject to affording businesses notices and an opportunity to cure within 30 days).[105] Given the number of ambiguities and drafting errors in the statute, and the limited nature of the private right of action (which only relates to security breaches), the Attorney General will have primary responsibility for interpreting and shaping enforcement priorities under the CCPA.

The statute contemplates that any business or third party may seek the opinion of the Attorney General for guidance on how to comply with the CCPA.[106]

The law also authorizes the Attorney General to bring a civil action against businesses, service providers, or any other person that violates the CCPA.[107] A business "shall be in violation" if it "fails to cure any alleged violation within 30 days after being notified of noncompliance."[108] The Attorney General may seek injunctive relief and a civil penalty of not more than two thousand five hundred dollars ($2,500) for each violation or seven thousand five hundred dollars ($7,500) for each intentional violation.[109] While the penalties *per violation* are small, it remains to be seen how the Attorney General construes the term *violation*. Whether a violation is defined in terms of an incident or a single act or omission, for example, or the number of people impacted,

---

whether or not published information based upon or related to such material has been disseminated.

Cal. Const. Art. I § 2(b).

[101] *See supra* § 26.13[2][F].

[102] *See supra* § 26.11.

[103] *See supra* § 26.12[2]; *see generally supra* § 26.13[5] (analyzing FTC enforcement actions).

[104] *See* Cal. Civ. Code § 1798.185.

[105] *See* Cal. Civ. Code § 1798.155.

[106] Cal. Civ. Code § 1798.155(a).

[107] Cal. Civ. Code § 1798.155(b).

[108] Cal. Civ. Code § 1798.155(a).

[109] Cal. Civ. Code § 1798.155(b).

will be significant.

Revenue from litigation will be allocated to a Consumer Privacy Fund, which may be used exclusively to offset costs incurred by state courts and the California Attorney General in connection with the CCPA.[110] This creates a potential conflict of interest, in that unless the legislature allocates funds expressly for all the new work to be done under the statute, there will be added pressure on the Attorney General's Office to pursue litigation—and to recover penalties in litigation.

Private right of action for data breaches

The CCPA creates a private right of action, with the possibility of recovering statutory damages, for consumers "whose nonencrypted or nonredacted personal information . . . is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices . . . ."[111] The private right of action created by the CCPA may be brought only for data

---

[110]Cal. Civ. Code § 1798.160.

[111]Cal. Civ. Code § 1798.150(a)(1). *Personal information* in this section is defined by reference section 1798.81.5, which is narrower in scope than the CCPA's definition in section 1798.140(o). *Personal information* under section 1798.81.5 means either of the following:

(A) 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 data elements are not encrypted or redacted:
  (i) Social security number.
  (ii) Driver's license number or California identification card number.
  (iii) 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.
  (iv) Medical information.
  (v) Health insurance information.

(B) A username or email address in combination with a password or security question and answer that would permit access to an online account.

Cal. Bus. & Prof. Code § 1798.81.5(d)(1). *Personal information* does not include "publicly available information that is lawfully made available to the general public from federal, state, or local government records." *Id.* § 1798.81.5(d)(4).

Medical information means any individually identifiable information, in electronic or physical form, regarding the individual's medical his-

breaches arising from a business's failure to maintain reasonable security measures, and not any other failures to comply with the CCPA.[112] What constitutes a *reasonable* security measure is not defined in the statute. Hence, unless the term is narrowed by regulations to be promulgated by the Attorney General, any time a California business suffers a security breach it will likely be sued in a lawsuit where plaintiffs will challenge both the security measures adopted and a business's adherence to those measures. In such cases, where the issue is contested, causation may raise factual questions that could make a case difficult to resolve on motion practice.

A person harmed by the data breach may bring an action to recover statutory damages in the range of $100 - $750 "per consumer per incident or actual damages, whichever is greater, injunctive or declaratory relief, and any other relief that a court deems proper.[113] In assessing the amount of statutory damages, the court shall consider "any one or more of the relevant circumstances presented by any of the parties to the case, including, but not limited to, the nature and seriousness of the misconduct, the number of violations, the persistence of the misconduct, the length of time over which the misconduct occurred, the willfulness of the defendant's misconduct, and the defendant's assets, liabilities, and net worth."[114] Nevertheless, a data breach impacting 100,000 consumers could invite putative class action suits seeking up to $7,500,000, which seems disproportionate. And a breach impacting 1,000,000 state residents could result in a putative class action suit seeking $750,000,000, where the plaintiffs, if successful, would be entitled to at least $100,000,000. Given the wide range of exposure, the private cause of action created by the CCPA is likely to generate substantial litigation.

To bring a claim for statutory damages, either individually

---

tory or medical treatment or diagnosis by a health care professional. *Id.* § 1798.81.5(d)(2).

Health insurance information means an individual's 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. *Id.* § 1798.81.5(d)(3).

[112]Cal. Civ. Code § 1798.150(c).

[113]Cal. Civ. Code § 1798.150(a)(1).

[114]Cal. Civ. Code § 1798.150(a)(2).

or as a putative class action suit, a consumer must provide a business "30 days' written notice identifying the specific provisions of this title the consumer alleges have been or are being violated," and allow the business 30 days to cure the violations. If within the 30 days the business actually cures the noticed violation (assuming a cure is possible) and provides the consumer an express written statement that the violations have been cured and that no further violations shall occur, then no action for individual statutory damages or class-wide statutory damages may be initiated against the business.[115]

This provision tracks the 30 day notice and cure period in the California Consumer Legal Remedies Act,[116] a statute popular with class action counsel. Under that statute, some class action lawyers have become adept at framing claims for which a "cure" is impossible. It is unclear how, if at all, a breach which has occurred could be cured. Indeed, the statute acknowledges that possibility in framing requirements "[i]n the event a cure is possible . . . ."[117] It remains to be seen whether the Attorney General will promulgate regulations to elaborate on the type of "cure" that would meet this requirement of the statute (such as measures to mitigate the consequences of a breach and minimize the risk of similar future breaches) or whether the issue will be fleshed out in litigation. Given the size of potential exposure and the ambiguity surrounding what constitutes *reasonable security,* a merely symbolic right to cure would be concerning.

If a business is able to cure and provides an express written statement to a consumer, but operates in breach of the express written statement, the consumer may initiate an action against the business to enforce the written statement and may pursue statutory damages for each breach of the express written statement, as well as any other violation of the title that postdates the written statement.[118]

No notice, however, is required for an individual consumer to initiate an action solely for actual pecuniary damages suf-

---

[115]Cal. Civ. Code § 1798.150(b).

[116]Cal. Civ. Code § 1782; *Laster v. T-Mobile USA, Inc.*, 407 F. Supp. 2d 1181, 1196 (S.D. Cal. 2005) (dismissing plaintiff's claim with prejudice because of plaintiff's failure to provide notice to defendants pursuant to section 1782(a)); *see generally supra* § 25.04[3].

[117]Cal. Civ. Code § 1798.150(b).

[118]Cal. Civ. Code § 1798.150(b).

fered as a result of an alleged violation.[119]

Significantly, the cause of action established by section 1798.150 applies "only to violations as defined in subdivision (a) and shall not be based on violations of any other section of this title. Nothing in this title shall be interpreted to serve as the basis for a private right of action under any other law."[120] What this means is that a violation of the statute could *not* form the basis for a claim under California's notorious section 17200, which typically affords a cause of action for violation of other statutes, laws or regulations.[121] The private enforcement right created by the CCPA thus is actually quite narrow. Nevertheless, the potential availability of statutory damages means that it will be heavily litigated by class action counsel seeking a generous settlement or award on behalf of a putative class of those whose information was exposed in a security breach. Further, the ambiguous nature of the standard of care—to "implement and maintain reasonable security procedures and practices"—means that regardless of culpability, any time a business experiences a security breach that exposes the information of California residents, class action counsel will have an incentive to file suit.

California law currently provides that any customer injured by a violation of its security breach notification statute may institute a civil action to recover damages[122] or injunctive relief,[123] in addition to any other remedies that may be available.[124] Among other things, the breach of the notification statute itself could be actionable as an unfair trade practice under California law if damages can be

---

[119]Cal. Civ. Code § 1798.150(b).

[120]Cal. Civ. Code § 1798.150(c).

[121]Cal. Bus. & Prof. §§ 17200 *et seq*. Section 17200 "borrows" violations from other laws by making them independently actionable as unfair competitive claims. *Korea Supply Co. v. Lockheed Martin Corp*., 29 Cal. 4th 1134, 1143–45, 131 Cal. Rptr. 2d 29 (Cal. 2003). Under section 17200, "[u]nlawful acts are 'anything that can properly be called a business practice and that at the same time is forbidden by law . . . be it civil, criminal, federal, state, or municipal, statutory, regulatory, or court-made,' where court-made law is, 'for example a violation of a prior court order.' " *Sybersound Records, Inc. v. UAV Corp*., 517 F.3d 1137, 1151–52 (9th Cir. 2008) (citations omitted); *see generally supra* § 25.04[3].

[122]Cal. Civil Code § 1798.84(b).

[123]Cal. Civil Code § 1798.84(e).

[124]Cal. Civil Code § 1798.84(g).

shown.[125] Absent any injury traceable to a company's failure to reasonably notify customers of a data breach, however, a plaintiff may not have standing to bring suit for a defendant's alleged failure to maintain reasonable security measures, at least in federal court.[126] The new cause of action created by the CCPA, by providing a remedy of statutory damages, will likely dramatically increase the number of California putative class action suits brought following a security breach. Given the liberal standing requirements for security breach cases in the Ninth Circuit,[127] some of these claims will be brought in federal court, although suits by California residents against California companies likely would need to be brought in state court, because of the lack of diversity jurisdiction, unless plaintiffs are able to also sue for violations of federal statutes.

The CCPA's requirement for contractual undertakings and obligations by service providers and third parties means it is also likely that the CCPA, if it takes effect, will result in litigation between or among *businesses*, *service providers* and *third parties*, as those terms are defined under the statute.

Data privacy class action litigation is analyzed in section

---

[125]*See* Cal. Bus. & Prof. Code §§ 17200 *et seq*.; *see generally supra* §§ 27.01, 27.04[6] (discussing how the breach of an unrelated statute may be actionable under § 17200).

[126]*See, e.g., Cahen v. Toyota Motor Corp.,* 717 F. App'x 720 (9th Cir. 2017) (affirming the lower court's ruling finding no standing to assert claims that car manufacturers equipped their vehicles with software that was susceptible to being hacked by third parties); *Antman v. Uber Technologies, Inc*., Case No. 3:15-cv-01175-LB, 2018 WL 2151231 (N.D. Cal. May 10, 2018) (dismissing, with prejudice, plaintiff's claims, arising out of a security breach, for allegedly (1) failing to implement and maintain reasonable security procedures to protect Uber drivers' personal information and promptly notify affected drivers, in violation of Cal. Civ. Code §§ 1798.81, 1798.81.5, and 1798.82; (2) unfair, fraudulent, and unlawful business practices, in violation of California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200; (3) negligence; and (4) breach of implied contract, for lack of Article III standing, where plaintiff could not allege injury sufficient to establish Article III standing); *see generally infra* § 27.07 (analyzing claims raised in security breach litigation).

[127]*See, e.g., In re Zappos.com, Inc.,* 888 F.3d 1020, 1023-30 (9th Cir. 2018) (holding that plaintiffs, whose information had been stolen by a hacker but who had not been victims of identity theft or financial fraud, nevertheless had Article III standing to maintain suit in federal court); *see generally infra* § 27.07 (comparing the relatively liberal standing requirements for security breach cases in the Ninth Circuit to case law from other circuits).

26.15. Security breach class action suits are analyzed in section 27.07.

E-COMMERCE & INTERNET LAW: TREATISE WITH FORMS 2D 2019

Ian C. Ballon

NEW AND IMPORTANT FEATURES FOR 2019 NOT FOUND ELSEWHERE

The Preeminent Internet and Mobile Law Treatise from a leading Internet litigator — now a 5 volume set!

To order call **1-888-728-7677**
or visit **legalsolutions.thomsonreuters.com**

Key Features of E-Commerce & Internet Law

- The California Consumer Privacy Act, GDPR, California IoT security statute, Vermont data broker registration law, Ohio safe harbor statute and other important privacy and cybersecurity laws
- Understanding conflicting law on mobile contract formation, unconscionability and enforcement of arbitration and class action waiver clauses
- The most comprehensive analysis of the TCPA's application to text messaging and its impact on litigation found anywhere
- Complete analysis of the Cybersecurity Information Sharing Act (CISA), state security breach statutes and regulations, and Defend Trade Secrets Act (DTSA) and their impact on screen scraping and database protection, cybersecurity information sharing and trade secret protection, privacy obligations and the impact that Terms of Use and other internet and mobile contracts may have in limiting the broad exemption from liability otherwise available under CISA
- Comprehensive and comparative analysis of the platform liability of Internet, mobile and cloud site owners, and service providers, for user content and misconduct under state and federal law
- Understanding the laws governing SEO and SEM and their impact on e-commerce vendors, including major developments involving internet advertising and embedded and sponsored links
- AI, screen scraping and database protection
- Strategies for defending cybersecurity breach and data privacy class action suits
- Copyright and Lanham Act fair use, patentable subject matter, combating genericide, right of publicity laws governing the use of a person's images and attributes, initial interest confusion, software copyrightability, damages in internet and mobile cases, the use of icons in mobile marketing, new rules governing fee awards, and the applicability and scope of federal and state safe harbors and exemptions
- How to enforce judgments against foreign domain name registrants
- Valuing domain name registrations from sales data
- Compelling the disclosure of the identity of anonymous and pseudonymous tortfeasors and infringers
- Exhaustive statutory and case law analysis of the Digital Millennium Copyright Act, the Communications Decency Act (including exclusions created by FOSTA-SESTA), the Video Privacy Protection Act, and Illinois Biometric Privacy Act
- Analysis of the CLOUD Act, BOTS Act, SPEECH Act, Consumer Review Fairness Act, N.J. Truth-in-Consumer Contract, Warranty and Notice Act, Family Movie Act and more
- Practical tips, checklists and forms that go beyond the typical legal treatise
- Clear, concise, and practical analysis

AN ESSENTIAL RESOURCE FOR ANY INTERNET AND MOBILE, INTELLECTUAL PROPERTY OR DATA PRIVACY/ CYBERSECURITY PRACTICE

E-Commerce & Internet Law is a comprehensive, authoritative work covering law, legal analysis, regulatory issues, emerging trends, and practical strategies. It includes practice tips and forms, nearly 10,000 detailed footnotes, and references to 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 five sectioned volumes, the 59 chapters cover:

- Sources of Internet Law and Practice
- Intellectual Property
- Licenses and Contracts
- Data Privacy, Cybersecurity 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
- Platform liability for Internet Sites and Services (Including Social Networks, Blogs and Cloud services)
- Civil Jurisdiction and Litigation

Distinguishing Features

- Clear, well written and with a practical perspective based on how issues actually play out in court (not available anywhere else)
- Exhaustive analysis of circuit splits and changes in the law combined with a common sense, practical approach for resolving legal issues, doing deals, documenting transactions and litigating and winning disputes
- Covers laws specific to the Internet and explains how the laws of the physical world apply to internet and mobile transactions and liability risks
- Addresses both law and best practices
- Comprehensive treatment of intellectual property, data privacy and mobile and Internet security breach law

SUMMARY OF CONTENTS

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

****
ABOUT THE AUTHOR
****

IAN C. BALLON

Ian Ballon is Co-Chair of Greenberg Traurig LLP's Global Intellectual Property and Technology Practice Group and is a litigator based in the firm's Silicon Valley and Los Angeles offices. He defends data privacy, cybersecurity breach, TCPA, and other Internet and mobile class action suits and litigates copyright, trademark, patent, trade secret, right of publicity, database and other intellectual property matters, including disputes involving Internet-related safe harbors and exemptions and platform liability.

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 Los Angeles and San Francisco Daily Journal* as one of the Top 75 Intellectual Property litigators, Top Cybersecurity and Artificial Intelligence (AI) lawyers, and Top 100 lawyers in California.

In 2017 Mr. Ballon was named a "Groundbreaker" by *The Recorder* at its 2017 Bay Area Litigation Departments of the Year awards ceremony and was selected as an "Intellectual Property Trailblazer" by the *National Law Journal*.

Mr. Ballon was named as the Lawyer of the Year for information technology law in the 2019, 2018, 2016 and 2013 editions of *The Best Lawyers in America* and 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 serves as Executive Director of Stanford University Law School's Center for E-Commerce in Palo Alto.

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./U.S. certification from the International Association of Privacy Professionals (IAPP).

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 Twitter and LinkedIn (@IanBallon).

Contributing authors: Parry Aftab, Ed Chansky, Francoise Gilbert, Tucker McCrady, Josh Raskin, Tom Smedinghoff and Emilio Varanini.

NEW AND IMPORTANT FEATURES FOR 2019

- A comprehensive analysis of the **California Consumer Information Privacy Act**, **California's Internet of Things (IoT) security statute**, **Vermont's data broker registration law**, **Ohio's safe harbor** for companies with written information security programs, and other new state laws governing cybersecurity (chapter 27) and data privacy (chapter 26)
- An exhaustive analysis of **FOSTA-SESTA** and what companies should do to maximize CDA protection in light of these new laws (chapter 37)
- The **CLOUD Act** (chapter 50)
- Understanding **the TCPA after *ACA Int'l*** and significant new cases & circuit splits (chapter 29)
- Fully updated **50-state compendium** of security breach notification laws, with a **strategic approach** to handling notice to consumers and state agencies (chapter 27)
- **Platform liability and statutory exemptions and immunities** (including a comparison of "but for" liability under the CDA and DMCA, and the latest law on secondary trademark and patent liability) (chapter 49)
- Applying **the single publication rule** to websites, links and uses on social media (chapter 37)
- The complex array of potential liability risks from, and remedies for, **screen scraping, database protection and use of AI to gather data and information online** (chapter 5)
- State online dating and revenge porn laws (chapter 51)
- **Circuit splits on Article III standing in cybersecurity litigation** (chapter 27)
- Revisiting **sponsored link, SEO and SEM practices and liability** (chapter 9)
- **Website and mobile accessibility** (chapter 48)
- **The Music Modernization Act's Impact on copyright preemption and DMCA protection for pre-1972 musical works** (chapter 4)
- **Compelling the disclosure of passwords and biometric information to unlock a mobile phone, tablet or storage device** (chapter 50)
- Cutting through the jargon to make sense of ***clickwrap*, *browsewrap*, *scrollwrap* and *sign-in wrap* agreements (and what many courts and lawyers get wrong about online contract formation)** (chapter 21)
- The latest case law, trends and strategy for **defending cybersecurity and data privacy class action suits** (chapters 25, 26, 27)
- **Click fraud** (chapter 28)
- Updated **Defend Trade Secrets Act** and UTSA case law (chapter 10)
- **Drafting enforceable arbitration clauses and class action waivers** (with new sample provisions) (chapter 22)
- **Applying the First Sale Doctrine to the sale of digital goods and information** (chapter 16)
- **The GDPR, ePrivacy Directive and transferring data from the EU/EEA** (by Francoise Gilbert) (chapter 26)
- **Patent law** (updated by Josh Raskin) (chapter 8)
- **Music licensing** (updated by Tucker McCrady) (chapter 17)
- **Mobile, Internet and Social Media contests & promotions** (updated by Ed Chansky) (chapter 28)
- **Conducting a risk assessment and creating a Written Information Security Assessment Plan (WISP)** (by Thomas J. Smedinghoff) (chapter 27)