LITIGATION RISKS AND COMPLIANCE OBLIGATIONS UNDER THE CALIFORNIA CONSUMER PRIVACY ACT

Excerpted from Chapter 26 (Data Privacy) from the April 2020 updates to
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)

STRATEGIES FOR DEFENDING CCPA AND OTHER CYBERSECURITY CLASS ACTION LITIGATION

9TH ANNUAL BCLT PRIVACY LAW FORUM
BERKELEY CENTER FOR LAW & TECHNOLOGY
OCTOBER 9, 2020

Ian C. Ballon
Greenberg Traurig, LLP

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

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 April 2020 Annual Update), a 5-volume legal treatise by Ian C. Ballon, published by West, (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

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
Suite 1900
Los Angeles, CA 90067
T 310.586.6575
F 310.586.0575

Ian C. Ballon is Co-Chair of Greenberg Traurig LLP's Global Intellectual Property & Technology Practice Group and represents companies in intellectual property litigation (including copyright, trademark, trade secret, patent, right of publicity, DMCA, domain name, platform defense, fair use, CDA and database/screen scraping) and in the defense of data privacy, cybersecurity breach and TCPA class action suits. A list of selected recent cases may be found here.

Ian is also the author of the leading treatise on internet and mobile law, *E-Commerce and Internet Law: Treatise with Forms 2d edition*, the 5-volume set published by West (www.IanBallon.net) and available on Westlaw, which includes extensive coverage of data privacy and cybersecurity breach issues, including a novel transactional approach to handling security breaches and exhaustive treatment of trends in data privacy, security breach and TCPA class action suits. In addition, he serves as Executive Director of Stanford University Law School's Center for the Digital Economy. He also chairs PLI's annual Advanced Defending Data Privacy, Security Breach and TCPA Class Action Litigation conference. Ian previously served as an Advisor to ALI's Intellectual Property: Principles Governing Jurisdiction, Choice of Law, and Judgments in Transactional Disputes (ALI Principles of the Law 2007) and is a member of the consultative group for the Data Privacy Principles of Law project (ALI Principles of Law Tentative Draft 2019).

Ian was named the Lawyer of the Year for Information Technology Law in the 2021, 2020, 2019, 2018, 2016 and 2013 editions of Best Lawyers in America and was recognized as the 2012 New Media Lawyer of the Year by the Century City Bar Association. In 2020, 2019 and 2018 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 for winning a series of TCPA cases. In addition, he was the recipient of the California State Bar Intellectual Property Law section's Vanguard Award for significant contributions to the development of intellectual property law. 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 has been recognized as one of the Top 75 intellectual property litigators in California by the *Los Angeles and San Francisco Daily Journal* in every year that the list has been published (2009 through 2020). Ian was also listed in *Variety's* "Legal Impact Report: 50 Game-Changing Attorneys" (2012), was recognized as one of the top 100 lawyers in L.A. by the *Los Angeles Business Journal* and is both a Northern California and Southern California Super Lawyer.

Ian holds JD and LLM degrees and the CIPP/US certification from the International Association of Privacy Professionals (IAPP).

E-COMMERCE & INTERNET LAW

Treatise with Forms—2d Edition

IAN C. BALLON

Volume 3

THOMSON REUTERS®

For Customer Assistance Call 1-800-328-4880

Mat #42478435

of a consumer[8] with whom the business does not have a direct relationship."[9]

The California statute, and proposed implementing regulations, are reprinted in Appendices 8 and 9 to chapter 26 and are analyzed in section 26.13A.

Vermont's data broker security law is analyzed in chapter 27, in section 27.04[6][J], and reprinted in section 27.09[49]. Guidelines for drafting a written information security program are set forth in section 27.13.

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

In General

The California Consumer Privacy Act (CCPA)[2] was hastily enacted in June 2018 to avoid a more inflexible ballot initiative that would have been next to impossible to amend.[3] The CCPA is a complex law with many aspects left unresolved,

---

or licensee of the data to identify or authenticate the consumer, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data;

(vii) name or address of a member of the consumer's immediate family or household;

(viii) Social Security number or other government-issued identification number; or

(ix) other information that, alone or in combination with the other information sold or licensed, would allow a reasonable person to identify the consumer with reasonable certainty.

Vt. Stat. Ann. tit. 9, § 2430(1)(A). *Brokered personal information* does not include "publicly available information to the extent that it is related to a consumer's business or profession." *Id.* § 2430(1)(B).

[8]A *consumer* is defined as an individual resident of Vermont. *See* Vt. Stat. Ann. tit. 9, § 2430(3).

[9]Vt. Stat. Ann. tit. 9, § 2430(4)(A). Examples of a *direct relationship* with a business include "if the consumer is a past or present: (i) customer, client, subscriber, user, or registered user of the business's goods or services; (ii) employee, contractor, or agent of the business; (iii) investor in the business; or (iv) donor to the business." *Id.* § 2430(4)(B).

[Section 26.13A]

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

which the California Attorney General estimated in August 2019 would cost California businesses up to $55 Billion (or 1.8% of California's Gross State Product) to implement by January 1, 2020 (with ongoing compliance costs over the next decade estimated to range from $467 million to more than $16 billion).[4] The CCPA was influenced by the GDPR,[5] 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, which became ef-

---

ity 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. Some but not all of these problems were addressed by legislative amendments in September 2018 and October 2019, and by proposed draft regulations released by the Attorney General in October 2019, and in February and March 2020, which will be issued in final form at some point in the first half of 2020 to take effect on July 1, 2020.

Mactaggart has proposed a new ballot initiative for the November 2020 ballot—dubbed *CCPA 2.0*—to strengthen the CCPA and expand its scope.

[4]*See* California Department of Justice—Office of the Attorney General, *Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations* (Aug. 2019), http://www.dof.ca.gov/Forecasting/Economics/Major_Regulations/Major_Regulations_Table/documents/CCPA_Regulations-SRIA-DOF.pdf

[5]*See supra* § 26.04. While the CCPA is, like the GDPR, a regulatory scheme that requires affected companies to adapt their practices and procedures—rather than simply modifying a posted privacy statement—they share both similarities and differences. The GDPR, for example, refers to *data subjects*, *controllers*, and *processors*, whereas the CCPA refers to *consumers*, *businesses*, *third parties*, and *service providers*. The CCPA definition of *personal information* is broader than *personal data* under the GDPR, although the GDPR restricts uses of certain information without opt-in consent or lawful permission, whereas the CCPA typically requires disclosure (except for information from minors who are teenagers not otherwise subject to federal COPPA regulations).

fective on January 1, 2020,[6] will be supplemented by regulations that will become effective on July 1, 2020 (but apply retroactively in some instances),[7] and may at some point 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[8] (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 and October 2019 and effective January 1, 2020, is reprinted at the end of this chapter at Appendix 8. The Attorney General's February 2020 draft regulations are reprinted in Appendix 9 and the subsequent March 2020 draft regulations are analyzed in this section 26.13A. These draft regulations will be superseded by final regulations that will be issued on or before July 1, 2020 and will take effect on July 1, 2020 (with some retroactive application, as noted in this section).

Subject to enumerated exclusions discussed later in this section (including businesses subject to federal financial services and health care privacy regulations), the CCPA broadly addresses the use of personal information about California residents—not merely consumers.[9] Rather than regulating the collection, use, and dissemination of information obtained *by companies from consumers*, as past consumer laws did,

---

[6]*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).

[7]The March 2020 draft regulations, which are analyzed in this section, may be accessed at https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-text-of-second-set-clean-031120.pdf? The final version will be published on or before July 1, 2020, and will be accessible at https://oag.ca.gov/privacy/ccpa

[8]15 U.S.C.A. §§ 7701 to 7713; *see infra* § 29.03.

[9]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."). The California Code of Regulations contains a lengthy definition of who is a *resident*, which provides in part that:

> The term "resident," as defined in the law, includes (1) every individual who is in the State for other than a temporary or transitory purpose, and (2) every individual who is domiciled in the State who is outside the State for a temporary or transitory purpose. All other individuals are nonresidents.

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

---

Under this definition, an individual may be a resident although not domiciled in this State, and, conversely, may be domiciled in this State without being a resident. The purpose of this definition is to include in the category of individuals who are taxable upon their entire net income, regardless of whether derived from sources within or without the State, all individuals who are physically present in this State enjoying the benefit and protection of its laws and government, except individuals who are here temporarily, and to exclude from this category all individuals who, although domiciled in this State, are outside this State for other than temporary or transitory purposes, and, hence, do not obtain the benefits accorded by the laws and Government of this State.

If an individual acquires the status of a resident by virtue of being physically present in the State for other than temporary or transitory purposes, he remains a resident even though temporarily absent from the State. If, however, he leaves the State for other than temporary or transitory purposes, he thereupon ceases to be a resident.

If an individual is domiciled in this State, he remains a resident unless he is outside of this State for other than temporary or transitory purposes.

(b) Meaning of Temporary or Transitory Purpose. Whether or not the purpose for which an individual is in this State will be considered temporary or transitory in character will depend to a large extent upon the facts and circumstances of each particular case. It can be stated generally, however, that if an individual is simply passing through this State on his way to another state or country, or is here for a brief rest or vacation, or to complete a particular transaction, or perform a particular contract, or fulfill a particular engagement, which will require his presence in this State for but a short period, he is in this State for temporary or transitory purposes, and will not be a resident by virtue of his presence here.

If, however, an individual is in this State to improve his health and his illness is of such a character as to require a relatively long or indefinite period to recuperate, or he is here for business purposes which will require a long or indefinite period to accomplish, or is employed in a position that may last permanently or indefinitely, or has retired from business and moved to California with no definite intention of leaving shortly thereafter, he is in the State for other than temporary or transitory purposes, and, accordingly, is a resident taxable upon his entire net income even though he may retain his domicile in some other state or country. . . .

The underlying theory of Sections 17014-17016 is that the state with which a person has the closest connection during the taxable year is the state of his residence.

An individual whose presence in California does not exceed an aggregate of six months within the taxable year and who is domiciled without the state and maintains a permanent abode at the place of his domicile, will be considered as being in this state for temporary or transitory purposes providing he does not engage in any activity or conduct within this State other than that of a seasonal visitor, tourist or guest.

An individual may be a seasonal visitor, tourist or guest even though he owns or maintains an abode in California or has a bank account here for the purpose of paying personal expenses or joins local social clubs. . . .

Cal. Code Regs. Tit. 18, § 17014.

specific notices be placed on a business's website, in a business's mobile application, or provided in person, and that 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. Compliance under the CCPA requires ongoing activity to monitor and adjust a company's practices and procedures. Data mapping, while not required, may be helpful in determining what information a business collects, and what it does with it, to evaluate how best to comply with the law. Although it is important for companies that collect, use or disseminate personal information about California residents and are subject to the statute to operationalize the CCPA, in the current regulatory environment—where other states are free to adopt additional or different requirements—businesses need to plan ahead to anticipate trends in the law, rather than merely adhering to compliance deadlines as they arise.

The CCPA is intended to impose compliance obligations on larger business entities and those involved in *selling* customer information (broadly defined). It applies to a business "that collects[10] 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."[11] 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[12] or

---

[10]*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).

[11]Cal. Civ. Code § 1798.140(c)(1).

[12]The focus on consumers, households, or devices, means that a business could be subject to the law even if it does not buy, receive for commercial purposes, or sell the personal information of 50,000 or more consumers, if, for example, it buys, receives for commercial purposes, or sells personal information from multiple devices for many of its consum-

(3) "[d]erives 50 percent or more of its annual revenues from selling consumers' personal information."[13]

The law also potentially applies to parent and subsidiary entities if they operate under common branding and one or the other is subject to the CCPA.[14]

The collection or sale of personal information that takes place "wholly outside of California," however, is not subject to the CCPA.[15]

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[16] pursuant to a written contract, provided that the contract prohibits the entity receiving the information from retain-

---

ers.

[13]Cal. Civ. Code §§ 1798.140(c)(1)(A), 1798.140(c)(1)(B), 1798.140(c)(1)(C) (defining a *business*).

[14]The CCPA applies to an entity "that controls or is controlled by a business . . . and that shares common branding with the business." Cal. Civ. Code § 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.*; *see generally supra* chapter 6 (trademarks, servicemarks and brand management).

[15]Cal. Civ. Code § 1798.145(a)(6).

[16]*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 qual-

ing, 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."[17] 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.[18] A business that discloses personal information to a service

---

ity 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 that the personal information is not disclosed to another third party and is not used to build a profile about a consumer or otherwise alter an individual 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.

[17]Cal. Civ. Code § 1798.140(v).

[18]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

provider will not be liable under the CCPA if the service provider uses the personal information in violation of the 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."[19] A service provider will likewise not be liable under the CCPA for the obligations of a business for which it provides services.[20] Service providers are subject to enforcement actions brought by the California Attorney General[21] and presumably breach of contract actions brought by a contracting business.

Unlike a *third party*,[22] a business is not required to dis-

---

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).

[19]Cal. Civ. Code § 1798.145(k).

[20]Cal. Civ. Code § 1798.145(k).

[21]Cal. Civ. Code § 1798.155(b).

[22]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

close to consumers the categories of service providers to which it provides access to personal information.[23] 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."[24]

As amended in September 2018 and October 2019, 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),[25] affirmatively requires opt-in consent[26]);
- 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

---

> 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).

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

[24]Cal. Civ. Code § 1798.115(d).

[25]15 U.S.C.A. §§ 6501 to 6506; 16 C.F.R. §§ 312.1 to 312.13; *supra* § 26.13[2].

[26]Cal. Civ. Code § 1798.120(c).

be sold and providing an opportunity to opt out.[27]

Personal information includes, but is not limited to, information that "identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked,[28] directly or indirectly, with a particular consumer or household," and a non-exclusive list of qualifying data elements.[29] The data elements identified in the statute,[30] 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.[31]

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

(D) Commercial information, including records of personal property, products or services purchased, obtained, or

---

[27]Cal. Civ. Code § 1798.115(d).

[28]What it means for information to be *reasonably linked* is not defined under the CCPA or in the March 2020 draft regulations. In an older report, the FTC took the position that data is not deemed *reasonably linked* if a company takes reasonable measures to de-identify data, commits not to re-identify it, and prohibits downstream recipients from re-identifying it. *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].

[29]Cal. Civ. Code § 1798.140(o)(1).

[30]Cal. Civ. Code § 1798.185(a)(1). The CCPA does not define *household*. The Attorney General's March 2020 draft regulations would limit "household" to "a person or group of people who: (1) reside at the same address, (2) share a common device or the same service provided by a business, and (3) are identified by the business as sharing the same group account or unique identifier." Proposed text of Cal. Code Regs. § 999.301(k).

[31]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.

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 identified 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.[32]

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 (such as a user's potential interest in diving or other hobbies, likely occupation, or family connection to a particular town), the inferences themselves become personal information, subject to the statute (whether or not the inferences prove to be reliable and accurate).

Personal information excludes *publicly available information*[33] (other than biometric information collected by a business about a consumer without the consumer's knowledge[34]—which constitutes *personal information*). This is an improvement over earlier versions of the statute, which had excluded from the definition of what was *publicly available*

---

[32]Cal. Civ. Code § 1798.140(o)(1).

[33]*Publicly available* means "information that is lawfully made available from federal, state, or local government records." Cal. Civ. Code § 1798.140(o)(2).

[34]Cal. Civ. Code § 1798.140(o)(2).

data used for a purpose not compatible with the purpose for which the data was maintained and made available in government records or for which it was publicly maintained. As amended in October 2019, *publicly available* information can no longer become transmuted into personal information.

Personal information, however, potentially may include deidentified information under certain circumstances. In general, the CCPA excludes from the definition of *personal information*, "consumer information that is deidentified or aggregate consumer information."[35] The statute further provides that the obligations imposed on a business by the CCPA shall not restrict a business's ability to "[c]ollect, use, retain, sell, or disclose consumer information that is deidentified or in the aggregate consumer information."[36] Deidentified consumer information could become *personal information*, however, if a business fails to undertake four protective measures set forth in section 1798.140(h). For deidentified information to not constitute personal information, a business must:

(1) implement technical safeguards that prohibit reidentification of the consumer to whom the information may pertain.
(2) implement business processes that specifically prohibit reidentification of the information.
(3) implement business processes to prevent inadvertent release of deidentified information.
(4) make no attempt to reidentify the information.

Otherwise, the information will be treated as *personal information* (because it will not qualify as *deidentified consumer data* under the statute, and therefore will not be

---

[35]Cal. Civ. Code § 1798.140(o)(3). *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 specified by statute to prevent reidentification of the information, which is discussed in the text. *See id.* § 1798.140(h).

Aggregate consumer information is 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*.

[36]Cal. Civ. Code § 1798.145(a)(5).

excluded from the definition of *personal information*).

Conversely, the CCPA generally does not require re-identification 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 (such as the requirement that a business provide consumers with notice of personal information collected and the purpose for the collection, give consumers the right to opt out of collection, and post on their website an opt out button or link implicitly disclosing that they sell personal information, if they do so).[37] Specifically, 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 information," or to require a business to collect "personal information that it would not otherwise collect," or "retain personal information for longer than it would" in the "ordinary course of business.[38]

The CCPA gives the California Attorney General broad authority to issue regulations interpreting and implementing the law, 'to further . . . [its] purposes . . . .'[39] Proposed draft regulations, focused largely on procedures for imple-

---

[37]The specific format is to be prescribed by the Attorney General in regulations to be promulgated by July 1, 2020, to take effect on July 1, 2020 (with some retroactive provisions, as noted in this section). The graphics proposed by the Attorney General, in the February and March 2020 drafts of the regulations, are comprised of red buttons next to text in black that reads "Do Not Sell My Personal Information" or "Do Not Sell My Info." The graphic is reprinted in Appendix 10 and discussed further later in this section.

[38]Cal. Civ. Code § 1798.145(l).

[39]Cal. Civ. Code § 1798.185. Enumerated among the nonexclusive list of tasks for which the Attorney General has been delegated authority to further the purposes of the CCPA are:

(1) Updating as needed additional categories of personal information to those enumerated in subdivision (c) of Section 1798.130 and subdivision (o) of Section 1798.140 in order to address changes in technology, data collection practices, obstacles to implementation, and privacy concerns.

(2) Updating as needed the definition of unique identifiers to address changes in technology, data collection, obstacles to implementation, and privacy concerns, and additional categories to the definition of designated methods for submitting requests to facilitate a consumer's ability to obtain information from a business pursuant to Section 1798.130.

(3) Establishing any exceptions necessary to comply with state or federal law, including, but not limited to, those relating to trade

menting the CCPA (rather than clarifying ambiguous aspects

---

secrets and intellectual property rights, within one year of passage of this title and as needed thereafter.

(4) Establishing rules and procedures for the following:
   (A) To facilitate and govern the submission of a request by a consumer to opt-out of the sale of personal information pursuant to Section 1798.120.
   (B) To govern business compliance with a consumer's opt-out request.
   (C) For the development and use of a recognizable and uniform opt-out logo or button by all businesses to promote consumer awareness of the opportunity to opt-out of the sale of personal information.

(5) Adjusting the monetary threshold in subparagraph (A) of paragraph (1) of subdivision (c) of Section 1798.140 in January of every odd-numbered year to reflect any increase in the Consumer Price Index.

(6) Establishing rules, procedures, and any exceptions necessary to ensure that the notices and information that businesses are required to provide pursuant to this title are provided in a manner that may be easily understood by the average consumer, are accessible to consumers with disabilities, and are available in the language primarily used to interact with the consumer, including establishing rules and guidelines regarding financial incentive offerings, within one year of passage of this title and as needed thereafter.

(7) Establishing rules and procedures to further the purposes of Sections 1798.110 and 1798.115 and to facilitate a consumer's or the consumer's authorized agent's ability to obtain information pursuant to Section 1798.130, with the goal of minimizing the administrative burden on consumers, taking into account available technology, security concerns, and the burden on the business, to govern a business's determination that a request for information received from a consumer is a verifiable consumer request, including treating a request submitted through a password-protected account maintained by the consumer with the business while the consumer is logged into the account as a verifiable consumer request and providing a mechanism for a consumer who does not maintain an account with the business to request information through the business's authentication of the consumer's identity, within one year of passage of this title and as needed thereafter.

Id. § 1798.185(a).

The Attorney General also is authorized to adopt additional regulations:

(1) To establish rules and procedures on how to process and comply with verifiable consumer requests for specific pieces of personal information relating to a household in order to address obstacles to implementation and privacy concerns.

(2) As necessary to further the purposes of this title.

Id. § 1798.185(b).

of the statute) were issued in October 2019 and further modified in February and March 2020[40] (and the February draft is included in Appendix 9 and 10 to this chapter). The CCPA empowers the AG to begin enforcement six months after the publication of final regulations or by July 1, 2020, whichever is sooner.[41] Given this timeline, final regulations will likely be issued on or before July 1, 2020, to take effect on that day. This section incorporates the March 2020 draft regulations.

Violations of the CCPA will largely be limited to enforcement by the California Attorney General, which is given powers equivalent to those delegated to the Federal Trade Commission under some federal privacy statutes to issue regulations and enforce compliance.[42]

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,[43] as discussed later in this section 26.13A.

Other California privacy laws, many of which were enacted prior to the time the CCPA took 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.[44] 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

---

[40]*California Consumer Privacy Act Regulations—Proposed Text of Regulations*, OAG.CA.gov (Mar. 11, 2020).

[41]*See* Cal. Civ. Code § 1798.185(c).

[42]*See generally supra* §§ 26.13[2][F] (COPPA), 26.13[5] (enforcement actions in general).

[43]Cal. Civ. Code § 1798.150(a).

[44]Cal. Civ. Code § 1798.100(b).

consumer.[45]

The Attorney General has proposed regulations that would govern the format of this and other notices to consumers under the law, including requiring that a notice from a business:

- "[u]se plain, straightforward language and avoid technical or legal jargon;"
- "[u]se a format that draws the consumer's attention to the notice and makes the notice readable, including on smaller screens, if applicable;"
- be available in the languages that the business uses in its ordinary course to communicate with consumers in California;
- be reasonably accessible to consumers with disabilities;[46] and
- "be made readily available where consumers will encounter it at or before the point of collection of any personal information . . . ."[47]

The Attorney General's proposed regulations also would

---

[45]Cal. Civ. Code § 1798.100(b).

[46]The March 2020 regulations further clarified:

> For notices provided online, the business shall follow generally recognized industry standards, such as the Web Content Accessibility Guidelines, version 2.1 of June 5, 2018, from the World Wide Web Consortium, incorporated herein by reference. In other contexts, the business shall provide information on how a consumer with a disability may access the notice in an alternative format.

Proposed text of Cal. Code Regs. § 999.305(a)(2)(d).

Website and mobile app accessibility under federal and state law is analyzed in section 48.06[4] in chapter 48.

[47]Proposed text of Cal. Code Regs. §§ 999.305(a)(2), 999.305(a)(3); *see also id.* § 999.306(a)(2) (same requirements for notice of right to opt out); § 999.307(a)(2) (same for notice of financial incentive); § 999.308(a)(2) (same for privacy policies implemented pursuant to CCPA).

The March 2020 regulations contained several illustrative examples of what it means to provide notice at the point of collection that is readily available where consumers will encounter it:

a. When a business collects consumers' personal information online, it may post a conspicuous link to the notice on the introductory page of the business's website and on all webpages where personal information is collected.

b. When a business collects personal information through a mobile application, it may provide a link to the notice on the mobile application's download page and within the application, such as through the application's settings menu.

c. When a business collects consumers' personal information offline, it may include the notice on printed forms that collect personal in-

require that this notice be separate from a business's privacy policy, since the Attorney General has proposed that the notice "at or before" collection would "link to the business's privacy policy, or in the case of offline notices, where the business's privacy policy can be located online."[48]

Disclosure requirements pursuant to a verifiable consumer request

The CCPA provides California residents with a right to request disclosures of the categories and specific pieces of their personal information that a business has collected, sold, and used.[49] 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 in this section 26.13A, and may in the future be supplemented by the California Attorney General.[50]

---

formation, provide the consumer with a paper version of the notice, or post prominent signage directing consumers to where the notice can be found online.

d. When a business collects personal information over the telephone or in person, it may provide the notice orally.

Id. § 999.305(a)(3).

[48]Proposed text of Cal. Code Regs. § 999.305(b)(4).

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

[50]*See* Cal. Civ. Code §§ 1798.130(c), 1798.140(o), 1798.185(a)(2). In brief, those categories 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.

A business may only provide the required disclosures "upon receipt of a verifiable consumer request."[51] 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 will finalize and implement no later than July 1, 2020.[52] A business is not required to produce personal information if it cannot verify the identity of the requesting party.[53]

The statute allows businesses some flexibility in determining what constitutes reasonable verification. A business may require authentication to confirm the identity of a consumer "that is reasonable in light of the nature of the personal information requested."[54] Draft regulations proposed by the Attorney General would require a business to disclose in its privacy policy the process it will use to verify consumer requests, including any information a consumer must provide in the process.[55]

A business cannot require a consumer to create an account in order to submit a verifiable consumer request, but if a

---

(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 identified 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.

These categories are analyzed in greater depth earlier in this section 26.13A.

[51]Cal. Civ. Code § 1798.100(c), Cal. Civ. Code § 1798.130(a)(2).

[52]Cal. Civ. Code § 1798.140(y).

[53]Cal. Civ. Code § 1798.140(y).

[54]Cal. Civ. Code § 1798.130(a)(2).

[55]Proposed text of Cal. Code Regs. § 999.308(c)(1)(c). The Attorney General's March 2020 draft regulations would allow a business to require written authorization from a consumer before acting pursuant to a request submitted by an authorized agent, or alternatively require the consumer to verify his or her own identity even if acting through an authorized agent, unless the agent has power of attorney pursuant to the Probate Code. *Id.* §§ 999.326(a), 999.326(b). The regulations also propose to allow a business to deny a request, absent proof that an agent is authorized by a consumer. *Id.* § 999.326(c).

consumer has an account with the business, "the business may require the consumer to submit the request through that account."[56] In the case of non-account holders (who nonetheless have rights under the CCPA), the Attorney General's proposed regulations would allow a business to verify a consumer request by matching data points provided by the consumer with data points maintained by the business.[57]

A business is required to disclose the information requested within "45 days of receiving a verifiable consumer request from the consumer."[58] The 45 day time period may be extended once by an additional 45 days.[59] Additionally, a business may take up to "90 additional days where necessary, taking into account the complexity and number of the requests" to respond.[60] A business is required to notify the consumer of the extension within 45 days of receiving the

---

The proposed regulations would require that authorized agents register to conduct business in California with the Secretary of State. *See* Proposed text of Cal. Code Regs. § 999.301(c).

The draft regulations also address how to handle a consumer request submitted ostensibly on behalf of a *household*. The proposed regulations provide that a business shall not comply with a request on behalf of a household unless

(1) all consumers of the household jointly request access to specific pieces of information for the household or deletion of household personal information; and

(2) the business individually verifies all the members of the household and also verifies that each member making the request is currently a member of the household; or

(3) if a consumer has password-protected account with a business that collects information about a household, the request can be processed through the business's existing business practice that comply with the regulations.

Id. §§ 999.318(a), 999.318(b).

If the household includes a minor under the age of 13, a business must obtain verifiable parental consent before complying with a request to access or delete the minor's personal information pursuant to the Attorney General's proposed regulations. *Id.* § 999.318(c).

[56]Cal. Civ. Code § 1798.130(a)(2).

[57]Proposed text of Cal. Code Regs. §§ 999.325(b), 999.325(c), 999.325(d). The Attorney General's proposed regulations would also require a business to inform a consumer when it cannot verify the consumer's identity and explain why it has "no reasonable method by which it can verify the identity of the requestor" (and evaluate annually whether a method could be developed). *Id.* § 999.325(g).

[58]Cal. Civ. Code § 1798.130(a)(2).

[59]Cal. Civ. Code § 1798.130(a)(2).

[60]Cal. Civ. Code § 1798.145(j)(1). Draft regulations proposed by the

request and, for extensions beyond the additional 45 days, the business must provide the reason for the delay.[61] A business is not required, however, to provide personal information requested to a consumer more than twice in a 12-month period.[62]

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.[63] The disclosure "shall cover the 12-month period preceding the business's receipt of the verifiable consumer request".[64] 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.[65] 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.[66]

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."[67]

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,

---

Attorney General would require a business to respond to all CCPA requests within ten (10) days of receipt with at least information "about how the business will process the request" pursuant to a verification process and "when the consumer should expect a response." Proposed text of Cal. Code Regs. § 999.313(a). The regulations also seemingly conflict with Cal. Civ. Code § 1798.145(j)(1) of the CCPA in that the regulations only allow a business to extend the time for its response for a "maximum total of 90 days from the day the request was received." *Id.* § 999.313(b). The Attorney General's proposed regulations allow a business to deny a request if it cannot verify the request within 45 days. *Id.* § 999.313(b).

[61]Cal. Civ. Code §§ 1798.130(a)(2), 1798.145(j)(1).

[62]Cal. Civ. Code § 1798.100(d).

[63]Cal. Civ. Code § 1798.100(d); Cal. Civ. Code § 1798.145(j)(3).

[64]Cal. Civ. Code § 1798.130(a)(2).

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

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

[67]Cal. Civ. Code § 1798.145(j)(2).

and if the business maintains an Internet Web site, a Web site address."[68] However, a business that "operates exclusively online and has a direct relationship with a consumer from whom it collects personal information" is only required to provide an email address for consumers to submit requests for information under the CCPA.[69] Any business subject to the CCPA that maintains a website must make the website "available to consumers to submit requests for information required to be disclosed" pursuant to the CCPA.[70] 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.[71]

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

The CCPA provides that a "consumer shall have the right 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."[72] 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"

---

[68]Cal. Civ. Code § 1798.130(a)(1)

[69]Cal. Civ. Code § 1798.130(a)(1)(A).

The Attorney General's proposed regulations would require a business to "consider the methods by which it interacts with the consumer when determining which methods to provide for submitting requests to know and requests to delete," and a business that interacts with consumers in person "shall consider providing an in-person method such as a printed form the consumer can directly submit by mail, a tablet or computer portal that allows the consumer to complete and submit an online form, or a telephone by which the consumer can call the business' toll-free number." Proposed text of Cal. Code Regs. § 999.312(c).

The March 2020 proposed regulations would also require a business to respond to a consumer's request under the CCPA (either honoring it or providing the consumer with specific directions on how to submit a valid request) if the request is not made through "one of the designated methods of submission" or is "deficient in some manner unrelated to the verification process . . . ." *Id.* § 999.312(e).

[70]Cal. Civ. Code § 1798.130(a)(1)(B).

[71]Cal. Civ. Code § 1798.130(a)(6).

[72]Cal. Civ. Code § 1798.100(a).

(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."[73]

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.[74] 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."[75] 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*.[76]

The March 2020 draft regulations would prohibit a busi-

---

[73]Cal. Civ. Code §§ 1798.110(a)(1)(5) to 1798.110(a)(5). The draft regulations would require a business to provide a response unique to each individual request even for the *categories* of personal information collected, sold, and used from a specific consumer, "unless its response would be the same for all consumers and the privacy policy discloses all information that is otherwise required to be in a response to a request to know such categories." Proposed text of Cal. Code Regs. § 999.313(c)(9). Many businesses may elect to standardize their practices to avoid the administrative burden of providing an individualized list of categories in response to each request submitted pursuant to the CCPA.

[74]Cal. Civ. Code § 1798.110(d)(1).

[75]Cal. Civ. Code § 1798.100(e).

[76]Similarly, section 1798.110, which further specifies a business's duty to disclose personal information collected, more broadly states that a

ness from ever disclosing a "consumer's Social Security number, driver's license number or other government-issued identification number, financial account number, any health insurance or medical identification number, an account password, or the security of the business's systems or networks," even in response to a verifiable consumer request, however, a business must inform the consumer with "sufficient particularity that it has collected the type of information," such as informing the consumer that it collects " 'unique biometric data including a fingerprint scan' without disclosing the actual fingerprint scan data."[77]

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.[78] *Sell* is not limited in the statute to the exchange of personal information for money, but instead is broadly defined to cover any transfer "by the business to another business or a third party for monetary or other valuable consideration."[79] The CCPA further provides that courts examining compliance with its provisions should take a liberal approach to determining

---

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).

[77]Proposed text of Cal. Code Regs. § 999.313(c)(4).

[78]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).

[79]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.

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."[80]

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 category of third parties to whom the personal information was sold"; and

(3) the "categories of personal information that the busi-

(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 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).

[80]Cal. Civ. Code § 1798.190.

ness disclosed about the consumer for a business purpose."[81]

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.[82]

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 about the consumer which the business has collected from the consumer."[83] When a business receives a "verifiable consumer request[84] 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.[85]

---

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

[82]Cal. Civ. Code § 1798.130(a)(4).

[83]Cal. Civ. Code § 1798.105(a).

[84]What constitutes a verifiable request is analyzed earlier in this section 26.13A in connection with verifiable requests for information disclosures.

[85]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). Additionally, the Attorney General's March 2020 draft regulations would require service providers to comply with deletion requests under the CCPA even if the service provider is not otherwise subject to the CCPA. *Id.* § 999.314(d).

Regulations proposed by the Attorney General would require a business to deny a request for deletion if the business cannot verify the identity of the requestor. *Id.* § 999.313(d)(1). However, if a business cannot process the deletion request because the requestor cannot be verified, the business must inform the consumer that his or her identity cannot be verified. *Id*. § 999.313(d)(1). Moreover, for all deletion requests that a business denies, regardless of the reason, the business must ask the consumer if he or she would like to opt out of the sale of their personal information and include

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 or fulfill the terms of a written warranty or product recall conducted in accordance with federal law.[86] 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."[87] A business may also retain consumer information for the purpose of detecting "security incidents," protecting against or prosecuting malicious and fraudulent activity,[88] debugging,[89] and to comply with the California Electronic Communications Privacy Act, Cal. Penal Code § 1546 or another "legal obligation."[90] 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 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."[91] 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.

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

---

the contents of, or a link to, the consumer's notice of right to opt-out. *Id.* § 999.313(d)(7).

[86]Cal. Civ. Code § 1798.105(d)(1).

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

[88]Cal. Civ. Code § 1798.105(d)(2).

[89]Cal. Civ. Code § 1798.105(d)(3).

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

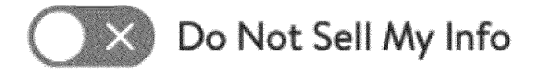
[91]Cal. Civ. Code §§ 1798.105(d)(4), (6). *Research* is narrowly limited to studies "[c]ompatible with the business purpose for which the personal information was collected," and that are "[n]ot for any commercial purpose," among other limitations. Cal. Civ. Code § 1798.140(s).

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."[92]

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."[93] 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."[94]

The Attorney General's February and March 2020 draft regulations require those selling information, within the meaning of the CCPA, to display a red button next to text in black that reads "Do Not Sell My Personal Information" or "Do Not Sell My Info." The prescribed graphic would appear as follows:



[92]Cal. Civ. Code § 1798.120(a).

[93]Cal. Civ. Code § 1798.135(a)(1).

[94]Cal. Civ. Code § 1798.135(b).

A business cannot require a consumer to create an account in order to opt-out.[95] A business also would be required, pursuant to the March 2020 draft regulations proposed by the Attorney General, to treat "user-enabled global privacy controls, such as a browser plugin or privacy setting, device setting, or other mechanism" that communicates a "choice to opt-out of the sale of" personal information as a valid opt-out request under the CCPA.[96]

A business that sells consumers' personal information must ensure that its customer service representatives are aware of consumers' right to opt-out and how to exercise that right.[97] 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."[98]

The requirement that a business provide a website link with the caption "Do Not Sell My Personal Information" creates an incentive for businesses that can do so to avoid being characterized as *selling* personal information under the CCPA. This link could be off-putting for some consumers—especially if the opt out right is made available only to California residents.

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 at least 13 years of age and less than 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

---

[95]Cal. Civ. Code § 1798.135(a)(1).

[96]Proposed text of Cal. Code Regs. § 999.315(d). The Attorney General's proposed regulations would also require a business to communicate the opt-out request to any third parties that it has sold the personal information to direct those third parties not to sell that consumer's information. *Id*. § 999.315(f).

The draft regulations would also require opt-out methods to be "easy for consumers to execute" and have "minimal steps to allow the consumer to opt-out." *Id*. § 999.315(c). The regulations would prohibit a business from using a "method that is designed with the purpose or has the substantial effect of subverting or impairing a consumer's decision to opt-out." *Id*.

[97]Cal. Civ. Code § 1798.135(a)(3).

[98]Cal. Civ. Code § 1798.135(a)(5).

the sale.[99] 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."[100] The CCPA refers to the prohibition on the sale of minors' personal information without consent as the "right to opt-in."[101]

The Attorney General's March 2020 draft regulations propose that the opt-in process must be "two-step[s]" "for consumers 13 years and older" "whereby the consumer shall first, clearly request to opt-in and then second, separately confirm their choice to opt-in."[102] During this two-step process, a business would be required to remind the parent or guardian of their right to opt out in the future and the process for doing so.[103]

The March 2020 draft regulations would also require a business that has "actual knowledge that it collects or maintains the personal information of children under the age of 13" to "establish, document, and comply with a reasonable method for determining that the person affirmatively authorizing the sale . . . is the parent or guardian of that child."[104]

The requirement for parental consent for children under age 13 is consistent with the federal Child Online Privacy Protection Act (COPPA).[105] 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.[106]

In addition to deletion requests under the CCPA (for businesses subject to the CCPA), California's "Online Eraser" Law purports to require any business with an online presence that markets products to minors or allows minors to post content to limit its advertising practices, and allow

---

[99]Cal. Civ. Code § 1798.120(c).

[100]Cal. Civ. Code § 1798.120(c).

[101]Cal. Civ. Code § 1798.120(c).

[102]Proposed text of Cal. Code Regs. § 999.301(a).

[103]Proposed text of Cal. Code Regs. § 999.330(b).

[104]Proposed text of Cal. Code Regs. § 999.330(a)(1).

[105]15 U.S.C.A. §§ 6501 to 6506; 16 C.F.R. §§ 312.1 to 312.13; *see generally supra* § 26.13[2].

[106]*See supra* § 26.13[2][H].

complete erasure of content posted by the minor.[107] The Constitutionality of this provision has yet to be fully tested.

Nondiscrimination and Financial incentives

The CCPA generally prohibits businesses from discriminating against consumers based on their exercise of any rights provided in the statute.[108] 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.[109] However, the CCPA 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 business by the consumer's data."[110]

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 business by the consumer's data."[111]

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. *De minimis* payments for information of great value thus are unlikely to pass muster.

The Attorney General's March 2020 proposed regulations would require businesses to provide extremely robust disclosures regarding any financial incentives offered in

---

[107] *See* Cal. Bus. & Prof. Code § 22580; *supra* § 26.13[6][F].

[108] Cal. Civ. Code § 1798.125(a).

[109] Cal. Civ. Code § 1798.125(a)(1).

[110] 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.

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

exchange for personal information. The proposed regulations would require businesses to disclose a summary of the financial incentive(s) offered, "a description of the material terms of the financial incentive" "including the categories of personal information that are implicated by the financial incentive," an explanation of how the financial incentive or price or service difference is reasonably related to the value of the consumer's data," a "good-faith estimate of the value of the consumer's data that forms the basis for offering the financial incentive or price or service difference," and a "description of the method the business used to calculate the value of the consumer's data."[112] The Attorney General has proposed a list of eight methods that a business can use to estimate the fair value of a consumer's data, which are:

(1) The marginal value to the business of the sale, collection, or deletion of a consumer's data;
(2) The average value to the business of the sale, collection, or deletion of a consumer's data or a typical consumer's data;
(3) The aggregate value to the business of the sale, collection, or deletion of consumers' data divided by the total number of consumers;
(4) Revenue generated by the business from sale, collection, or retention of consumers' personal information;
(5) Expenses related to the sale, collection, or retention of consumers' personal information;
(6) Expenses related to the offer, provision, or imposition of any financial incentive or price or service difference.
(7) Profit generated by the business from the sale, collection, or retention of consumers' personal information;
(8) Any other practical and reasonably reliable method of calculation used in good faith.[113]

Because the method of calculation and a justification for the incentive must be disclosed to consumers and in many cases may be complex to determine, many businesses may simply elect to not offer financial incentives.

Required privacy policy disclosures

The CCPA requires that businesses that collect, sell, or disclose California residents' personal information publicly

[112]Proposed text of Cal. Code Regs. § 999.307(b)(5).

[113]Proposed text of Cal. Code Regs. § 999.337(a).

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."[114] A business must update these disclosures "at least once every 12 months."[115] The disclosure must include "one or more designated methods for submitting" disclosure requests under the statute.[116]

Additionally, a business must disclose the categories of personal information that it has collected, sold, or disclosed in the previous 12 months.[117] 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) "[t]hat a consumer has the right to request the specific pieces of personal information the business has collected about that consumer."[118]

A business that sells or discloses consumers' personal information 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 pre-

---

[114]Cal. Civ. Code § 1798.130(a)(5)

[115]Cal. Civ. Code § 1798.130(a)(5).

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

[117]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).

[118]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 of the type of personal information it collects generally from consumers.

ceding 12 months, it must "disclose that fact."[119]

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.[120]

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.[121]

Record Keeping

The Attorney General's March 2020 draft regulations would place additional requirements on businesses that process a high volume of consumer information. The proposed regulations would require a business that "annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, the personal information of 10,000,000 or more consumers in a calendar year" to compile metrics, including the number of requests that it received pursuant to the CCPA per year and the median number of days within which it took the business to respond to the various types of requests received.[122] A business subject to the regulations would be required to disclose these metrics in its privacy policy or on its website by July 1 of every calendar year.[123] Further, a business subject to the regulations would be required to implement a customer training program, training individuals responsible for handling consumer requests about the CCPA and the business's compliance with the statute, and document compliance with the training program.[124]

Data Broker Registration

Pursuant to the 2019 law enacted in tandem with amendments to the CCPA, California imposes additional requirements on *data brokers,* which are defined as businesses that

---

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

[120]Cal. Civ. Code § 1798.135(a)(2).

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

[122]Proposed text of Cal. Code Regs. § 999.317(g)(1).

[123]*Id.* § 999.317(g)(2).

[124]*Id.* § 999.317(g)(5).

collect and sell consumers' personal information, but do not have direct relationships with consumers.[125] The statute requires data brokers to register with the Attorney General "[o]n or before January 31 following each year in which a business meets the definition of data broker."[126] A data broker is required to provide the Attorney General with its name and primary location, email address, and internet website, but providing the Attorney General with any other information about the broker's "data collection practices" is optional.[127]

Failure to comply with this provision may result in civil penalties of $100 "for each day the data broker fails to register" and any expenses the Attorney General incurs in investigating and prosecuting the data broker—a potentially large fine for businesses that allow their registrations to lapse.[128] The Attorney General will publicly list all registered data brokers on its website.[129]

Data brokers generally are not subject to many of the notice requirements otherwise imposed by the CCPA (because they do not collect data directly from consumers). The March 2020 regulations, however, mandate that, to avoid having to provide notice to consumers at the time of collection, data brokers registered with the California Attorney General pursuant to Cal. Civ. Code §§ 1798.99.80 *et seq.* must include in their registration with the Attorney General a link to their online privacy policies that "includes instructions on how a consumer can submit a request to opt-out."[130]

Additionally, the Attorney General's proposed regulations clarify that a business that neither collects nor sells consumers' personal information need not provide notice to consumers at the time of collection.[131]

Scope and exclusions

The California legislature mandated that the CCPA "be

---

[125] *See* Cal. Civ. Code § 1798.99.80.

[126] Cal. Civ. Code § 1798.99.82.

[127] Cal. Civ. Code §§ 1798.99.82(a), 1798.99.82(b).

[128] Cal. Civ. Code § 1798.99.82(c).

[129] Cal. Civ. Code § 1798.99.84.

[130] Proposed text of Cal. Code Regs. § 999.305(e); *see also infra* § 27.04[6] (analyzing state laws governing data brokers in Vermont and elsewhere).

[131] Proposed text of Cal. Code Regs. § 999.305(d).

liberally construed to effectuate its purposes."[132] 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.[133] 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.[134]

The CCPA provides that compliance with its obligations "shall not restrict a business' ability" to comply with other applicable laws or a civil or criminal investigation, cooperate with law enforcement agencies, or exercise or defend legal claims.[135] It likewise does not "apply where compliance by the business with the title would violate an evidentiary privilege under California law," such as the attorney-client privilege[136]

The CCPA excludes data subject to certain financial and health care privacy statutes and DMV records. Specifically, it does not apply to the sale of personal information "bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living" as defined in the Fair Credit Reporting Act, 15 U.S.C. §§ 1681, *et seq.*, unless the information is not otherwise regulated by the Fair Credit Reporting Act or if a business discloses, uses, or sells the information beyond what is authorized under the Act.[137]

The CCPA similarly does not apply 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, the Driver's Privacy Protection Act, 18 U.S.C. §§ 2721 *et seq.*, or vehicle or ownership information shared between a "new motor vehicle dealer" and "the vehicle's manufacturer," as may be necessary for effectuating a repair

---

[132]Cal. Civ. Code § 1798.194.

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

[134]Cal. Civ. Code § 1798.196.

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

[136]Cal. Civ. Code § 1798.145(b).

[137]Cal. Civ. Code §§ 1798.145(d)(1), 1798.145(d)(2).

covered by a vehicle warranty or a recall pursuant to federal law.[138] It likewise does not apply to certain medical information or health information that is regulated by federal law, or information collected as part of a clinical trial subject to federal law.[139]

The CCPA also temporarily excludes from its scope personal information collected from job applicants or employees, including information necessary for a business to administer benefits, but only until January 1, 2021.[140] A business is still required to disclose the categories of personal information that it collects from employees and job applicants pursuant to the CCPA before other obligations with respect to that information go into effect next year.[141]

The CCPA further may not be applied to infringe upon the noncommercial free speech rights protected by the California Constitution.[142]

---

[138]Cal. Civ. Code §§ 1798.145(e), 1798.145(f), 1798.145(g).

[139]Cal. Civ. Code § 1798.145(c)(1). The exclusions apply to medical information governed by the Confidentiality of Medical Information Act or protected health information that is collected by a covered entity or business associate governed by the privacy, security, and breach notification rules issued by the U.S. Department of Health and Human Services, pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act. *Id.* § 1798.145(c)(1)(A).

Specifically, the CCPA excludes a provider of health care governed by the Confidentiality of Medical Information Act or a covered entity governed by the privacy, security, and breach notification rules issued by the U.S. Department of Health and Human Services, pursuant to HIPAA, to the extent the provider or covered entity maintains patient information in the same manner as medical information or protected health information as described in subparagraph (A). *Id.* § 1798.145(c)(1)(B).

The statute also excludes information collected as part of a clinical trial subject to the Federal Policy for the Protection of Human Subjects, also known as the Common Rule, pursuant to good clinical practice guidelines issued by the International Council for Harmonisation or pursuant to human subject protection requirements of the U.S. Food and Drug Administration. *Id.* § 1798.145(c)(1)(B).

[140]*See* Cal. Civ. Code §§ 1798.145(h), 1798.145(o).

[141]*See* Cal. Civ. Code §§ 1798.145(h)(3), 1798.145(o)(3).

[142]Cal. Civ. Code § 1798.145(n) ("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:

Attorney General enforcement

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),[143] Health Insurance Portability and Accountability Act (HIPAA)[144] and Gramm-Leach-Bliley (GLB).[145] The Attorney General is delegated authority to adopt regulations,[146] provide opinions, and file suit to enforce the law (subject to affording businesses notices and an opportunity to cure within 30 days).[147] 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

---

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

Cal. Const. Art. I § 2(b).

[143]*See supra* § 26.13[2][F].

[144]*See supra* § 26.11.

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

[146]*See* Cal. Civ. Code § 1798.185.

[147]*See* Cal. Civ. Code § 1798.155.

on how to comply with the CCPA.[148]

The law also authorizes the Attorney General to bring a civil action against businesses, service providers, or any other person that violates the CCPA.[149] A business "shall be in violation" if it "fails to cure any alleged violation within 30 days after being notified of noncompliance."[150] 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.[151] While the penalties *per violation* are small, it remains to be seen how the Attorney General will construe the term *violation* in regulatory enforcement actions. Whether a violation is defined in terms of an incident or a single act or omission, for example, or the number of people impacted, 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.[152] 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 and 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 . . . ."[153] The private right of action created by the CCPA may be brought only for data

---

[148]Cal. Civ. Code § 1798.155(a).

[149]Cal. Civ. Code § 1798.155(b).

[150]Cal. Civ. Code § 1798.155(a).

[151]Cal. Civ. Code § 1798.155(b).

[152]Cal. Civ. Code § 1798.160.

[153]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:

breaches arising from a business's failure to maintain reasonable security measures, and not any other failures to comply with the CCPA.[154] What constitutes a *reasonable* security measure is not defined in the statute. Hence, any time a California business suffers a security breach, it may 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 legitimately contested, causation may raise factual questions that could make a case difficult to resolve on motion practice.

(A) An individual's first name or first initial and the individual's 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, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual.
  (iii) Account number or 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.
  (vi) Unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual. Unique biometric data does not include a physical or digital photograph, unless used or stored for facial recognition purposes.

(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 history 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).

[154]Cal. Civ. Code § 1798.150(c).

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.[155] 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."[156] Nevertheless, a data breach impacting 100,000 consumers could invite putative class action suits seeking up to $75,000,000, 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. These calculations are wildly disproportionate to the harm experienced in most cases. They also are disproportionate when compared to the actual amounts paid by companies to settle nation-wide cybersecurity breach class action suits (as analyzed in section 27.07 in chapter 27).[157] Given the potential for large awards in putative class action suits, the private cause of action created by the CCPA is likely to generate substantial litigation.

To bring a claim for statutory damages, either individually 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

---

[155]Cal. Civ. Code § 1798.150(a)(1).

[156]Cal. Civ. Code § 1798.150(a)(2).

[157]*See infra* § 27.07. Grossly disproportionate awards potentially could be challenged on Due Process grounds. *See, e.g.*, *Golan v. FreeEats.com, Inc.*, 930 F.3d 950, 962-63 (8th Cir. 2019) (ruling that $500 minimum statutory damage awards totaling $1.6 Billion (based on 3.2 million phone calls allegedly placed in the course of one week), under the Telephone Consumer Protection Act, violated Due Process).

or class-wide statutory damages may be initiated against the business.[158]

This provision tracks the 30 day notice and cure period in the California Consumer Legal Remedies Act,[159] 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 . . . ."[160] 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 statutory damage awards and the ambiguity surrounding what constitutes *reasonable security,* a merely symbolic right to cure would be of little benefit to businesses.

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 CCPA that postdates the written statement.[161]

No notice, however, is required for an individual consumer to initiate an action solely for actual pecuniary damages suffered as a result of an alleged violation.[162]

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

---

[158]Cal. Civ. Code § 1798.150(b).

[159]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].

[160]Cal. Civ. Code § 1798.150(b).

[161]Cal. Civ. Code § 1798.150(b).

[162]Cal. Civ. Code § 1798.150(b).

law."[163] 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.[164] 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.

While section 1798.150 insulates companies from private causes of action for violations of the CCPA other than for security breaches, this protection would not apply to claims brought by residents of other states against companies that adopt the CCPA across the board, and not merely for personal information from California residents. Businesses therefore need to weigh the pros and cons of implementing the CCPA narrowly, only for California residents, or more broadly. While a broad application may make sense for some companies from an operational perspective or for customer relations, it also potentially could expose a company to greater liability from residents of states other than California, whose laws would not provide any safe harbor from litigation. Although a claim by a resident of another state could not be premised on a violation of the CCPA *per se,* the failure of a business to adhere to its stated practices or procedures potentially could be actionable under theories of

---

[163]Cal. Civ. Code § 1798.150(c).

[164]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].

express or implied contract or unfair competition.[165]

The CCPA also leaves in place an array of other California privacy laws, which could form the basis for litigation against a business on grounds other than a security breach—even if noncompliance with the CCPA itself would not be actionable in a private lawsuit.[166] Section 1798.150 precludes other claims premised on CCPA violations, but does not preclude claims based on other theories of law. For example, regardless of whether a business is subject to the CCPA, if it has an online presence, it must nonetheless post a privacy policy that complies with Cal-OPPA, Cal. Bus. & Prof. Code §§ 22575, *et seq*. Presumably the requirement that a business disclose "personally identifiable information" that it collects under Cal-OPPA would overlap with a business's disclosure requirements under the CCPA, given the extremely broad definition of *personal information* in section 1798.140(h) of the CCPA.[167] Indeed, Cal-OPPA mandates additional disclosure requirements in an online privacy policy that do not completely coincide with the CCPA, such as allowing consumers to "request changes to any personally identifiable information collected," if a business provides that option, how a business responds to "do not track" signals, and whether use of the website might allow third-parties to collect additional information, for example, through the use of cookies.[168] Unlike the CCPA, Cal-OPPA provides a private right of action[169] and potentially could support a claim for a violation of California's unfair competition statute, Cal. Bus. & Prof. Code § 17200.[170]

Similarly, businesses (including even small businesses not subject to the CCPA, if they have at least 20 employees) are still required to disclose if their personal information is shared with others for direct marketing, and if so allow customers to opt out, pursuant to the "Shine the Light" Law.[171] Disclosures under the Shine the Light Law must be, in at least some ways, more fulsome than pursuant to the

---

[165]*See generally infra* §§ 26.14, 26.15.

[166]*See generally supra* § 26.13[6].

[167]*See* Cal. Bus. & Prof. Code § 22577(a); *supra* § 26.13[6][B].

[168]*See* Cal. Bus. & Prof. Code § 22575(b).

[169]*See* Cal. Bus. & Prof. Code § 22576.

[170]*See Svenson v. Google Inc.*, Case No. 13-cv-04080-BLF, 2015 WL 1503429, at *8-10 (N.D. Cal. Apr. 1, 2015); *see generally supra* § 26.13[6].

[171]*See* Cal. Civ. Code § 1798.83; *supra* § 26.13[6][D].

CCPA because the law requires businesses to disclose the "names and addresses" of third parties that have received a customer's personal information, and "examples of the products or services marketed" to customers, "if known," "sufficient to give the customer a reasonable indication of the nature of the third parties' business."[172] Further, a business is afforded less time—only 30 days—to comply with a disclosure request under the Shine the Light Law[173] than under the CCPA. The Shine the Light Law, unlike the CCPA, provides a private right of action for customers injured by a violation (although injury in most cases may be difficult to prove).[174]

Security breach claims under the CCPA potentially may be joined by other causes of action in litigation. California law predating the CCPA provides that any customer injured by a violation of its security breach notification statute may institute a civil action to recover damages[175] or injunctive relief,[176] in addition to any other remedies that may be available.[177] 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 shown.[178] 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.[179] CCPA and other California law claims, of course, could be brought in California state courts.

---

[172]Cal. Civ. Code § 1798.83(b)(3).

[173]Cal. Civ. Code § 1798.83(b)(1)(C).

[174]*See* Cal. Civ. Code § 1798.84; *see generally supra* § 26.13[6][D].

[175]Cal. Civil Code § 1798.84(b).

[176]Cal. Civil Code § 1798.84(e).

[177]Cal. Civil Code § 1798.84(g).

[178]*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).

[179]*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 informa-

Other claims typically joined in security breach and privacy litigation include claims for breach of contract (if there is a contract, or if a privacy policy is incorporated by reference in a user agreement and allegedly breached), breach of the covenant of good faith and fair dealing (if the claim isn't directly prohibited by the contract), breach of implied contract (if there is no express contract), breach of fiduciary duty, negligence, fraud, and claims under other states' cybersecurity laws.[180]

The cause of action created by the CCPA, by providing a remedy of statutory damages, will likely 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,[181] 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.

To minimize the risk of class action litigation arising under the CCPA, businesses should enter into binding contracts with consumers that contain enforceable arbitration provisions governed by the Federal Arbitration Act (which preempts state law), including a delegation clause to maximize its potential enforceability.[182] Crafting a binding and enforceable arbitration provision is addressed in section

---

tion 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).

[180]*See generally infra* §§ 26.15 (data privacy litigation), 27.04[6] (state data security laws), 27.07 (cybersecurity breach litigation), 27.08[10] (remedies under state and U.S. territorial security breach notification statutes).

[181]*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).

[182]*See, e.g., Henry Schein, Inc. v. Archer & White Sales, Inc.*, 139 S. Ct. 524, 529 (2019) (holding that "[w]hen the parties' contract delegates the

22.05[2][M] in chapter 22, which also includes a sample form. Ensuring that contract formation for online and mobile agreements conforms to the law in those jurisdictions most hostile to electronic contracting is analyzed extensively in section 21.03 in chapter 21. Where a business does not have privity of contract with consumers but could be sued for violating the CCPA, it should seek to become an intended beneficiary of the arbitration clauses in effect between its business partners and consumers who could file suit. It should also ensure that its partners' arbitration provisions and processes for online and mobile contract formation conform to best practices. Businesses also may wish to explore whether they have adequate insurance coverage (and the right to select counsel).

Beyond class action litigation, the CCPA's requirement for contractual undertakings and obligations by service providers and third parties means it is also likely that the CCPA will result in litigation between or among *businesses*, *service providers* and *third parties*, as those terms are defined under the statute. To anticipate potential claims, entities should pay close attention to indemnification provisions in these contracts (including potential indemnification for litigation and regulatory enforcement actions brought by the California Attorney General).

It is possible that, at some point, Congress may act to preempt the CCPA. The statute also may be challenged, to the extent it regulates interstate commerce, under the dormant Commerce Clause, although the drafters of the CCPA were careful to provide that the collection or sale of information that takes place "wholly outside of California," is not subject to the CCPA.[183] Dormant Commerce Clause arguments thus far have been rebuffed in lower court chal-

---

arbitrability question to an arbitrator, a court may not override the contract" and "possesses no power to decide the arbitrability issue . . . even if the court thinks that the argument that the arbitration agreement applies to a particular dispute is wholly groundless"); *Rent-A-Center, West v. Jackson*, 561 U.S. 63 (2010); *see generally supra* § 22.05[2][M].

[183]*See* Cal. Civ. Code § 1798.145(a)(6). A state law that regulates wholly out-of-state conduct may be struck down under the dormant Commerce Clause. *See, e.g., Publius v. Boyer-Vine,* 237 F. Supp. 3d 997 (E.D. Cal. 2017) (holding that a California law that purported to prohibit a Massachusetts blogger from compiling and posting the names, home addresses, and phone numbers, of members of the California legislature who voted in favor of gun control measures, likely violated the dormant Commerce Clause).

lenges to various state privacy laws[184]—albeit ones substantially less burdensome or expensive for out-of-state companies to comply with. The cost of compliance—estimated by the California Attorney General to be up to $55 Billion initially, with ongoing compliance costs from 2020 to 2030 estimated to range from $467 million to more than $16 billion[185]—suggests there potentially could be merit to an argument that the CCPA burdens interstate commerce. Dormant Commerce Clause case law is analyzed in chapter 35.

Data privacy class action litigation is analyzed in section 26.15. Security breach class action suits are analyzed in section 27.07.

---

[184]*See, e.g., Ades v. Omni Hotels Management Corp.*, 46 F. Supp. 3d 999 (C.D. Cal. 2014) (holding that the California Invasion of Privacy Act regulated only calls with a nexus to the state and had the purpose of preventing privacy harms to Californians. Accordingly, it did not merit strict scrutiny under the dormant Commerce Clause, even though it might create incentives for parties to alter their nationwide behavior because those effects were deemed incidental); *see also, e.g., In re Facebook Biometric Information Privacy Litig.*, Case No. 3:15-cv-0373-JD, 2018 WL 2197546, at *4 (N.D. Cal. May 14, 2018) (denying summary judgment based on the argument that subjecting the defendant to liability under the Illinois Biometric Information Privacy Act for processing facial recognition data on servers located exclusively outside of Illinois violated the dormant Commerce Clause, because liability under the statute would not force the defendant "to change its practices with respect to residents of other states."); *Monroy v. Shutterfly, Inc.,* Case No. 16 C 10984, 2017 WL 4099846, at *7-8 (N.D. Ill. Sept. 15, 2017) (denying defendant's motion to dismiss plaintiff's suit under the dormant Commerce Clause; "Monroy's suit, as well as his proposed class, is confined to individuals whose biometric data was obtained from photographs uploaded to Shutterfly in Illinois. Applying BIPA in this case would not entail any regulation of Shutterfly's gathering and storage of biometric data obtained outside of Illinois. It is true that the statute requires Shutterfly to comply with certain regulations if it wishes to operate in Illinois. But that is very different from controlling Shutterfly's conduct in other states."); *see generally infra* §§ 35.01 *et seq.* (analyzing the application of the dormant Commerce Clause to internet statutes).

[185]*See* California Department of Justice—Office of the Attorney General, *Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations* (Aug. 2019), http://www.dof.ca.gov/Forecasting/Economics/Major_Regulations/Major_Regulations_Table/documents/CCPA_Regulations-SRIA-DOF.pdf

E-COMMERCE & INTERNET LAW: TREATISE WITH FORMS 2D 2020

Ian C. Ballon

APRIL 2020 UPDATES – INCLUDING NEW AND IMPORTANT FEATURES

The Preeminent Internet and Mobile Law Treatise from a leading Internet litigator –
a 5 volume-set & On Westlaw!

To order call **1-888-728-7677**
or visit **IanBallon.net**

Key Features of E-Commerce & Internet Law

- Antitrust in the era of techlash
- The California Consumer Privacy Act, GDPR, California IoT security statute, state data broker laws, and other privacy and cybersecurity laws
- Artificial intelligence & machine learning
- Mobile and online contract formation, unconscionability and enforcement of arbitration and class action waiver clauses
- TCPA law and litigation - the most comprehensive analysis of the statute, regulations, and conflicting case law found anywhere
- The Cybersecurity Information Sharing Act (CISA), state security breach statutes and regulations, and the Defend Trade Secrets Act (DTSA) -- and their impact on screen scraping and database protection, cybersecurity information sharing and trade secret protection, & privacy
- Platform moderation and liability, safe harbors, and defenses
- Dormant Commerce Clause restrictions on state law regulation of online and mobile commerce
- The law of SEO and SEM – and its impact on e-commerce vendors
- AI, screen scraping and database protection
- Defending cybersecurity breach and data privacy class action suits – case law, trends & strategy
- IP issues including Copyright and Lanham Act fair use, patentable subject matter, negative trade secrets, rights 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 hashtags in social media marketing, new rules governing fee awards, and the applicability and scope of federal and state safe harbors and exemptions
- Online anonymity and pseudonymity – state and federal laws governing permissible disclosures and subpoenas
- Sponsored links, embedded links, and internet, mobile and social media advertising
- Enforcing judgments against foreign domain name registrants
- Valuing domain name registrations from sales data
- Applying the First Sale Doctrine to virtual goods
- Exhaustive statutory and case law analysis of the Digital Millennium Copyright Act, the Communications Decency Act (including exclusions for certain IP & 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
- Click fraud
- Copyright and Lanham Act fair use
- 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/ AI/ 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
- Includes the hottest issues, such as IP and privacy aspects of artificial intelligence & machine learning, social media advertising, cloud storage, platform liability, and more!
- Comprehensive treatment of intellectual property, data privacy and mobile and Internet security breach law

SUMMARY OF CONTENTS

Volume 1

Volume 2

Volume 3

Volume 4

Volume 5

"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 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 cases, including disputes involving safe harbors and exemptions, platform liability and fair use.

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 Intellectual Property litigators (2009-2020), Top Cybersecurity and Artificial Intelligence (AI) lawyers, and Top 100 lawyers in California.

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 selected as the Lawyer of the Year for information technology law in the 2020, 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 the Digital Economy.

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, Viola Bensinger, Ed Chansky, Francoise Gilbert, Rebekah Guyon, Tucker McCrady, Josh Raskin, & Tom Smedinghoff.

NEW AND IMPORTANT FEATURES FOR 2020

- **Antitrust in the era of techlash** (chapter 34)
- **Platform moderation and liability, safe harbors and defenses** (ch. 49, 4, 6, 8, 37)
- **Privacy and IP aspects of Artificial Intelligence (AI) and machine learning** (ch. 5, 26)
- 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)
- **FOSTA-SESTA** and ways to maximize CDA protection (ch 37)
- **IP aspects of the use of #hashtags** in social media (ch 6)
- The **CLOUD Act** (chapter 50)
- Making sense of the Circuit Split under the **TCPA (3d, 7th and 11th vs. 2d and 9th)** & other significant new case law (ch. 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)
- Copyright, patent, ADA and other **troll litigation – and ways to combat it** (ch. 4, 8, 48)
- Applying **the single publication rule** to websites, links and uses on social media (chapter 37)
- **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)
- **Expanding and contracting anti-SLAPP case law** construing different state laws (ch 37)
- **Circuit-by-circuit, claim-by-claim analysis of CDA opinions**
- **eSIGN case law** (chapter 15)
- **Website and mobile accessibility** under the ADA and state laws (chapter 48)
- **Online and mobile Contract formation – common mistakes by courts and counsel** (chapter 21)
- **Defending cybersecurity and data privacy class action suits -** case law, trends and strategy (chapters 25, 26, 27)
- **The Music Modernization Act's Impact on copyright preemption, the CDA, and DMCA protection for pre-1972 musical works** (ch 4, 37, 49)
- **Cybersafety standards and best practices for youth audiences in social media, apps, games & networks** (by Parry Aftab) (ch. 51)
- 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)
- **The GDPR, ePrivacy Directive and transferring data from the EU/EEA** (by Francoise Gilbert and Viola Bensinger) (ch. 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)
- **Idea protection & misappropriation** (ch 13)
- Revisiting **links, embedded links, sponsored links, and SEO/SEM practices and liability** (chapter 9)