LITIGATION RISKS AND COMPLIANCE OBLIGATIONS UNDER THE CALIFORNIA PRIVACY RIGHTS ACT OF 2020

Excerpted from the forthcoming 2023 update to Chapter 26 (Data Privacy)
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)

(These excerpts are unrevised page proofs for the current update and may contain errors. Please email the author at ballon@gtlaw.com for a complimentary copy of the final published version.)

INTERNET AND MOBILE LAW AND LITIGATION TRENDS

SNAP INC.

JANUARY 30, 2023

Ian C. Ballon
Greenberg Traurig, LLP

Los Angeles:	Silicon Valley:	Washington, D.C.:
1840 Century Park East, Ste. 1900	1900 University Avenue, 5th Fl.	2101 L Street, N.W., Ste. 1000
Los Angeles, CA 90067	East Palo Alto, CA 914303	Washington, D.C. 20037
Direct Dial: (310) 586-6575	Direct Dial: (650) 289-7881	Direct Dial: (202) 331-3138
Direct Fax: (310) 586-0575	Direct Fax: (650) 462-7881	Fax: (202) 331-3101

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 forthcoming 2023 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

Los Angeles
1840 Century Park East
Suite 1900
Los Angeles, CA 90067
T 310.586.6575
F 310.586.0575

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

Washington, D.C.
2101 L Street, N.W.
Suite 1000
Washington, DC 20037
T 202.331.3138
F 202.331.3101

Ian C. Ballon is a litigator who is Co-Chair of Greenberg Traurig LLP's Global Intellectual Property & Technology Practice Group and represents internet, mobile, entertainment and technology companies in intellectual property and technology-related litigation and in the defense of data privacy, security breach and AdTech class action suits.

Ian has been named by the *LA and San Francisco Daily Journal* as one of the Top 75 intellectual property litigators in California in every year that the list has been published (2009 through 2022). He has been listed in Best Lawyers in America consistently every year since 2003 and was named Lawyer of the Year for Information Technology in 2023, 2022, 2020, 2019, 2018, 2016 and 2013. In 2022, 2021, 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 2022, Ian was named to Lawdragon's list of the Top 500 Lawyers in America and he has been included on the *Daily Journal's* annual list of the Top 100 Lawyers in California. 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. He was also recognized as the 2012 New Media Lawyer of the Year by the Century City Bar Association. In 2010, 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. Ian was listed in *Variety's* "Legal Impact Report: 50 Game-Changing Attorneys" and has been named a Northern California Super Lawyer every year from 2004 through 2021 and a Southern California Super Lawyer for every year from 2007-2021. He has also been 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.

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 intellectual property law issues. In addition, he is the author of *The Complete CAN-SPAM Act Handbook* (West 2008) and *The Complete State Security Breach Notification Compliance Handbook* (West 2009). 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 as a member of the consultative group for ALI's Principles of Data Privacy Law (ALI Principles of Law 2020).

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

Personal Information Transfers to Third Parties for Direct Marketing Purposes (the "Shine the Light" Law)
26.13[6][E] Collection of PII and Zip Code Information in Connection with Credit Card Transactions
26.13[6][F] California Bus. & Prof. Code § 22580—California's "Online Eraser" Law for Minors
26.13[6][G] The IMDb Age Law
26.13[7] Minnesota ISP Privacy Law
26.13[8] Texas Privacy Policy Law
26.13[8.5] Delaware's Privacy Policy Law
26.13[9] Maine's Broadband Internet Privacy Law and [Now Repealed] Predatory Marketing Practices Against Minors Act
26.13[10] Video Rental Records, the VPPA and Equivalent State Laws
26.13[11] Driver's Records under the DPPA
26.13[12] Biometric and Genetic Data
26.13[12][A] In General
26.13[12][B] The Illinois Biometric Information Privacy Act
26.13[12][C] Texas Law on the Capture or Use of Biometric Identifier
26.13[12][D] Washington Law on the use of biometric data for a commercial purpose
26.13[13] Data Broker Laws
26.13A The California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA)
26.13A[1] The CCPA and CPRA—In General—and What Constitutes *Personal Information*
26.13A[2] The CCPA's Required Privacy Policy and 3 Other Notices to consumers Required by the CCPA

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

26.13A[2][A] Required Notices and Their Style/Format—In General
26.13A[2][B] Privacy Policy
26.13A[2][C] Notice at Collection
26.13A[2][D] Notice of the Right to Opt-Out
26.13A[2][E] Notice of Financial Incentive (or price or service difference)
26.13A[3] Business Obligations to Provide for and Process Verifiable Consumer Requests to Know or Delete Information
26.13A[3][A] In General
26.13A[3][B] Right to the disclosure of the categories and specific pieces of personal information collected—The "Right to Know" In General
26.13A[3][C] Right to the disclosure of the categories of personal information *sold* or *disclosed for a Business Purpose*—In General
26.13A[3][D] Responding to Requests to Know
26.13A[4] Right to the deletion of personal information
26.13A[5] Verification and Confirmation of Informational and Deletion Requests
26.13A[5][A] Verification—In General
26.13A[5][B] Verification—for Password-Protected Accounts
26.13A[5][C] Verification Where There Is No Password-Protected Account or it Can't Be Accessed
26.13A[5][D] If A Business is Unable to Verify a Request

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

26.13A[6] Requests to Know or Delete Household Information
26.13A[7] The Timing for Responding to Requests to Know or Delete Information, and the Format and Permissible Charges for Disclosures
26.13A[8] Business obligations in implementing consumers' right to opt-out of the sale of personal information and minors' right to opt-in
26.13A[9] Minors
26.13A[9][A] In General
26.13A[9][B] Consumers 13-15 Years Old
26.13A[9][C] Consumers Younger than 13 Years Old
26.13A[10] Nondiscrimination and Financial incentives
26.13A[11] Data Broker Registration
26.13A[12] Scope and exclusions
26.13A[13] Regulatory enforcement
26.13A[14] Private right of action for data breaches
26.13A[15] Non-waiver
26.13B Nevada's Privacy Law
26.13B[1] In General
26.13B[2] Statutory Provisions
26.13C The Virginia Consumer Data Protection Act
26.13C[1] In General
26.13C[2] Statutory Provisions
26.13D Colorado Privacy Act
26.13D[1] Overview
26.13D[2] Statutory Provisions
26.14 Website and Mobile App Privacy Policies
26.14[1] In General
26.14[2] Components of a Privacy Policy
26.14[3] Checklist for Drafting an Internet Privacy Statement

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

and other data brokers and selling the information.

The Nevada law also requires data brokers to make available to consumers a notice containing certain information relating to the collection and sale of covered information. An operator who fails to comply with that requirement is authorized to remedy the failure to comply within 30 days after being informed of the failure, if it is the data broker's first failure to comply. If such an operator remedies a failure to comply within 30 days after being informed of the failure, the operator will be deemed to have not committed a violation for purposes of enforcement by the Attorney General.

Virginia[10] and Colorado[11] privacy laws, while not expressly regulating data brokers, define *controller* in such a way that data brokers could be subject to the laws and their opt-out requirements in response to consumer notices (and requirements for opt-in consent for sensitive data).

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

Nevada's law is addressed in section 26.13B, Virginia's in section 26.13C and Colorado's in section 26.13D.

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 The California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA)[1]

26.13A[1] The CCPA and CPRA—In General—and What Constitutes *Personal Information*

The California Consumer Privacy Act (CCPA)[1] was hastily enacted in June 2018 to avoid a more inflexible ballot initia-

---

[10]Va. Code Ann. §§ 59.1-571 to 59.1-581; *see generally infra* § 26.13C.

[11]Colo. Rev. Stat. Ann. §§ 6-1-1301 to 6-1-113; *see generally infra* § 26.13D.

[Section 26.13A]

[1]The original version of this section, on the CCPA, was co-authored with Greenberg Traurig attorney Rebekah Guyon.

[Section 26.13A[1]]

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

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

tive that would have been next to impossible to amend.[2] The CCPA is a complex law, 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 at the time) 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).[3] The CCPA was influenced by the GDPR,[4] which took effect for

---

[2]Real estate millionaire Alastair Mactaggart had spent $2 million to obtain enough signatures for a ballot initiative that would have created a comprehensive consumer privacy law, enforced through litigation. Because laws enacted through ballot initiatives in California require a supermajority to amend—and therefore are effectively almost impossible to revise—legislative and business leaders worked together to enact a somewhat better version of the law by the deadline set by Mactaggart—5 P.M. on June 28, 2018—which was the last date by which the initiative could be withdrawn from the 2018 California ballot. *See, e.g.*, Nicholas Confessore, *The Unlikely Activist Who Took On Silicon Valley—and Won,* N.Y. TIMES, Aug. 14, 2018. Mactaggart had an incentive to cut a deal because advertising for ballot initiatives is very costly and, even when enacted, many initiatives are subject to legal challenge. The rush to cut a deal with the millionaire backer of the consumer privacy initiative, however, resulted in a statute that was more than 10,000 words long, complex, and contained numerous errors and ambiguities. *See, e.g.,* Eric Goldman, *A First (But Very Incomplete) Crack at Inventorying the California Consumer Privacy Act's Problems*, TECHNOLOGY & MARKETING LAW BLOG, July 24, 2018, available at https://blog.ericgoldman.org/archives/2018/07/a-first-but-very-incomplete-crack-at-inventorying-the-california-consumer-privacy-acts-problems.htm. Some but not all of these problems were addressed by legislative amendments in September 2018, October 2019, September 2020, and October 2021, and by regulations released by the Attorney General in draft form in October 2019, and further revised in drafts issued on February 10 and March 27, 2020, which were adopted in final form on August 14, 2020. Additional amendments to the regulations went into effect on March 15, 2021.

Mactaggart proposed a new ballot initiative for the November 2020 ballot—originally, as the California Privacy Rights and Enforcement Act, but later shortened to just the California Privacy Rights Act (CPRA)--to strengthen the CCPA and expand its scope. The CPRA, which was approved by voters, will become fully operative on January 1, 2023, and is referenced throughout this section 26.13A.

[3]*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

[4]*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—

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

residents (data subjects) located 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 effective on January 1, 2020,[5] was supplemented by regulations that became effective on September 14, 2020 (but applied retroactively in some instances), 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[6] (which was enacted after California adopted 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.[7] A copy of the CCPA, as amended in September 2018, October 2019, September 2020, and October 2021, and in effect as of January 2022, is reprinted at the end of this chapter at Appendix 8. The Attorney General's implementing regulations (as adopted in final form on August 14, 2020 and amended on March 15, 2021) are reprinted in Appendix 9 and are

---

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).

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

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

[7]Following California's enactment of the CCPA, Nevada adopted a privacy law in 2019 that (as subsequently amended) applies to a broader array of businesses than the CCPA but is more narrowly focused. That law is analyzed and reprinted in whole in section 26.13B. Colorado and Virginia subsequently enacted comprehensive laws similar to California's, which are set to take effect in 2023 and are addressed in, respectively, sections 26.13C and 26.13D.

The COVID 19 global pandemic, which resulted in stay at home orders throughout the United States beginning in early 2020 and adjourned or abbreviated state legislative sessions, slowed the advance of draft state data privacy and cybersecurity statutes, which otherwise might have been enacted in a number of states following the entry into force of the CCPA.

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

analyzed in this section 26.13A.[8]

A more stringent law—the California Privacy Rights Act of 2020 (CPRA)—was approved as a ballot initiative by California voters in November 2020 and will take effect on January 1, 2023 (unless preempted by federal legislation), with administrative enforcement set to begin on July 1, 2023 for violations occurring on or after that date. The CPRA amends, rather than replaces, the CCPA, but does so in a number of material respects, although the exact contours of the law will depend on regulations to be adopted by the Attorney General by July 1, 2022[9] and subsequently enforced by the

---

[8]The California Attorney General issued proposed draft regulations, focused largely on procedures for implementing the CCPA, in October 2019, and further modified those regulations (in response to public comments and hearings, and to clarify some (but not all) of the more ambiguous aspects of the statute) in drafts released on February 10 and March 27, 2020, before issuing final regulations in June 2020, which were adopted in large part by the Office of Administrative Law ("OAL") and took effect on August 14, 2020.

The OAL rejected proposed sections 999.305(a)(5), 999.306(b)(2), 999.315(c), and 999.326(c), which required businesses to obtain express consent from consumers before using previously collected information for a materially different purpose, required businesses substantially interacting with consumers offline to provide notice of right to opt-out via an offline method, established minimum standards for submitting requests to opt-out to businesses, and provided businesses with the ability to deny certain requests from authorized agents.

After the final regulations were approved, the Attorney General issued a further Notice of Proposed Rulemaking Action on October 12, 2020, proposing four additional amendments, which, along with a fifth amendment adding an optional opt-out icon, were adopted in final form on March 15, 2021. The March 2021 final amendments: require notice of the right to opt-out by an offline method for those businesses that collect personal information in the course of interacting with consumers offline (in section 999.306(b)(3)); impose additional requirements on permissible methods that businesses may use to allow consumers to submit opt-out requests (in section 999.315(h)); limit the requirements a business may impose on consumers when requests to know or delete are submitted by authorized agents (in revisions to section 999.326(a)); add an optional opt-out icon in new section 999.306(f), and clarify that a business's process for obtaining consent from minors must be included in the Privacy Policies of businesses subject to section 999.330 (applicable consumers under age 13) and/or 999.331 (applicable to consumers who are 13-15 years old) (in revised section 999.332(a), which changes "and" to "and/or.").

The status of any future proposed regulations may be tracked at https://oag.ca.gov/privacy/ccpa/current.

[9]A nonexclusive list of issues to be considered is set forth in the CPRA, Cal. Civ. Code § 1798.185(a).

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

California Privacy Protection Agency (CPPA), a new agency created by the CPRA. A copy of the CPRA is reprinted at Appendix 11 and is analyzed throughout section 26.13A. To avoid confusion, the CPPA is referred to by its full name or as the Agency in this section, while the two laws—the CCPA and CPRA—are referred to by their acronyms.[10]

The CCPA's name—California *Consumer* Privacy Act—is a bit of a misnomer. Subject to enumerated exclusions discussed later in this section (including businesses subject to federal financial services and health care privacy regulations), the statute broadly addresses the use of personal information about California residents—not merely consumers.[11] Rather than regulating the collection, use, and dissemination of information obtained *by companies from*

---

[10]Earlier versions of the CCPA used the term *opt out* (with no hyphen), but the nomenclature was changed in 2020 to *opt-out* (with a hyphen). Accordingly, both versions may be used in this edition of section 26.13A.

[11]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 definition will remain unchanged after January 1, 2023, under the CPRA. *See id.* § 1798.140(i) (effective Jan. 1, 2023). 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.
>
> 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 circum-

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

consumers, as past consumer laws had done, 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 affected businesses amend their privacy policies to account for the law, but that 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 ad-

---

stances 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.

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

ditional or different requirements and, internationally, different regimes are in place in Europe, Brazil, India, Japan, South Africa and elsewhere—businesses need to plan ahead to anticipate trends in the law, rather than merely adhering to compliance deadlines as they arise.

The CCPA regulates the activities of three types of entities—*businesses, service providers*, and *third parties*. The CPRA will add *contractors* as a new variation of service provider when it takes effect on January 1, 2023.[12] The CCPA is intended to impose compliance obligations on larger busi-

---

[12] A *contractor* under the CPRA is defined as

(1) . . . a person to whom the business makes available a consumer's personal Information for a business purpose pursuant to a written contract with the business, provided that the contract:
  (A) Prohibits the contractor from:
    (i) Selling or sharing the personal Information.
    (ii) Retaining, using, or disclosing the personal information for any purpose other than for the business purposes specified in the contract, including retaining, using, or disclosing the personal Information for a commercial purpose other than the business purposes specified in the contract, or as otherwise permitted by this title.
    (iii) Retaining, using, or disclosing the Information outside of the direct business relationship between the contractor and the business.
    (iv) Combining the personal information which the contractor receives pursuant to a written contract with the business with personal Information which It receives from or on behalf of another person or persons, or collects from Its own interaction with the consumer, provided that the contractor may combine personal Information to perform any business purpose as defined In regulations adopted pursuant to paragraph (10) of subdivision (a) of Section 1798.l85, except as provided for In paragraph (6) of subdivision (e) of this Section and in regulations adopted by the California Privacy Protection Agency.
  (B) Includes a certification made by contractor that the contractor understands the restrictions in subparagraph (A) and will comply with them.
  (C) Permits, subject to agreement with the contractor, the business to monitor the contractor's compliance with the contract through measures including, but not limited to, ongoing manual reviews and automated scans, and regular assessments, audits, or other technical and operational testing at least once every twelve (12) months.
(2) If a contractor engages any other person to assist it in processing personal information for a business purpose on behalf of the business, or if any other person engaged by the contractor en-

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

ness entities and those involved in *selling* customer information (which is broadly defined and, as of January 1, 2023, will be expanded under the CPRA to cover merely *sharing* information[13] for cross-context behavioral advertising[14]). The

---

gages another person to assist in processing personal information for such business purpose, it shall notify the business of such engagement and the engagement shall be pursuant to a written contract binding the other person to observe all the requirements set forth in paragraph (1).

Cal. Civ. Code § 1798.140(j) (effective Jan. 1, 2023). *Service Provider* is given a new and much more detailed definition under the CPRA. *See id.* § 1798.140(ag) (effective Jan. 1, 2023). A *third party*, by contrast, is defined as an entity that is not a *service provider* or *contractor* or "[t]he business with whom the consumer intentionally interacts and that collects personal information from the consumer as part of the consumer's current interaction with the business . . ." under the CPRA. *See id.* § 1798.140(ai) (effective Jan. 1, 2023); *see also id.* § 1798.140(s) (effective Jan. 1, 2023) (defining *intentionally interacts* under the CPRA to mean "when the consumer intends to interact with a person, or disclose personal Information to a person, via one or more deliberate interactions, such as visiting the person's website or purchasing a good or service from the person. Hovering over, muting, pausing, or closing a given piece of content does not constitute a consumer's intent to interact with a person.").

The distinctions between and among a business, service provider, and contractor, are likely to be fleshed out in regulations to be issued by the California Attorney General.

[13]*Sharing* under the CPRA is defined in Cal. Civ. Code § 1798.140(ah) (effective Jan. 1, 2023). That section provides that *share, shared* or *sharing* mean "sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to a third party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration, including transactions between a business and a third party for cross-context behavioral advertising for the benefit of a business in which no money is exchanged." Cal. Civ. Code § 1798.140(ah)(1) (effective Jan. 1, 2023). Notwithstanding this definition, a business will not be deemed to share personal information when:

(A) A consumer uses or directs the business to: (i) intentionally disclose personal information; or (ii) intentionally interact with one or more third parties;

(B) The business uses or shares on identifier for a consumer who has opted out of the sharing of the consumer's personal Information or limited the use of the consumer's sensitive personal information for the purposes of alerting persons that the consumer has opted out of the sharing of the consumer's personal information or limited the use of the consumer's sensitive personal information.; or

(C) The business transfers to a third party the personal information of a consumer as an asset that is part of a merger, acquisition,

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

> 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 this title. 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 this title. 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).

Cal. Civ. Code § 1798.140(ah)(2) (effective Jan. 1, 2023). The term *identifier* connotes something that identifies a person, although it is not explicitly defined but is referenced throughout the CCPA and to an even greater extent in the CPRA. Examples of identifiers used in the definition of *personal information* include "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." *Id.* § 1798.140(v1)(A) (effective Jan. 1, 2023). The definition of *biometric information* similarly refers to an *identifier template*, "such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information." *Id.* § 1798.140(c) (effective Jan. 1, 2023). Similarly, a *consumer* is a natural person who is a California resident, "however identified, including by any unique identifier." *Id.* § 1798.140(c) (effective Jan. 1, 2023).

A *probabilistic identifier* is defined as "the identification of a consumer or a consumer's device to a degree of certainty of more probable than not based on any categories of personal Information included in, or similar to, the categories enumerated in the definition of personal information." *Id.* § 1798.140(x) (effective Jan. 1, 2023).

A *unique identifier* (or *unique personal identifier*) means, in part, "a persistent identifier that can be used to recognize a consumer, a family, or a device that is linked to a consumer or family, over time and across different services, including, but not limited to, a device identifier; an Internet Protocol address; cookies, beacons, pixel tags, mobile ad identifiers, or similar technology; customer number, unique pseudonym, or user alias; telephone numbers, or other forms of persistent or probabilistic identifiers that can be used to identify a particular consumer or device that is linked to a consumer or family." *Id.* § 1798.140(aj) (effective Jan. 1, 2023).

[14]*Cross-contextual behavioral advertising* under the CPRA will mean "the targeting of advertising to a consumer based on the consumer's personal information obtained from the consumer's activity across businesses, distinctly-branded websites, applications, or services, other than

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

CCPA applies to a business "that collects[15] 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 . . . ."[16] A business is subject to the CCPA, however, only if it:

(1) has "annual gross revenues [globally[17]] in excess of twenty-five million dollars"[18]

---

the business, distinctly-branded website, application, or service with which the consumer intentionally interacts." Cal. Civ. Code § 1798.140(k) (effective Jan. 1, 2023).

This definition was intended to resolve any ambiguity under the CCPA over whether certain data-driven digital advertising practices constitute a *sale* requiring a business to afford opt-out rights to a California consumer.

When asked to "clarify the definition of 'sale,' [under the CCPA] including whether [the] use of website cookies shared with third parties are a sale," the Attorney General refused to take a definitive position, stating that whether "the particular situations . . . constitute a 'sale' raises specific legal questions that would require a fact-specific determination, including whether or not there was monetary or other valuable consideration involved, the consumer directed the business to intentionally disclose the information, and whether the parties involved were service providers." *See* Final Statement of Reasons, Appendix A, at Response 47 (June 11, 2020), *available at* https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-fsor-appendix-a.pdf. The Attorney General gave a similar response when asked to state whether the use of Google and Adobe Analytics constitute sales, stating that it "require[s] a fact-specific determination." *Id.* at Response 533.

[15]*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); *see also* Cal. Civ. Code § 1798.140(f) (effective Jan. 1, 2023) (retaining the same definition under the CPRA).

[16]Cal. Civ. Code § 1798.140(c)(1).

[17]Gross revenues in this context is not limited to gross revenue earned in California or from California residents, but, according to California's Attorney General, should be based on a business's global turnover. *See* Final Statement of Reasons, Appendix A at Response 5 (June 11, 2020) ("Civil Code § 1798.140(c)(1)(A) does not limit the revenue threshold to revenue generated in California or from California residents. Any proposed change to limit the threshold to revenue generated only in California or from California residents would be inconsistent with the CCPA."), *available at* https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-fsor-appendix-a.pdf.

[18]The CPRA clarifies that this amount must have been earned in the

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

(2) alone or in combination, annually buys, receives for commercial purposes, or sells the personal information of 50,000 or more consumers, households, or devices[19] or

(3) "[d]erives 50 percent or more of its annual revenues from selling[20] consumers' personal information."[21]

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.[22]

---

preceding calendar year. *See* Cal. Civ. Code § 1798.140(d)(1)(A) (effective Jan. 1, 2023).

[19]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 consumers.

A *household* is defined by regulation as "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." Cal. Code Regs. § 999.301(k). Under the CPRA, a household will be defined as "a group, however identified, of consumers who cohabitate with one another at the same residential address and share use of common device(s) or service(s)." Cal. Civ. Code § 1798.140(q) (effective Jan. 1, 2023).

Under the CPRA the threshold for applicability will be changed to cover a business that "alone or in combination annually buys or sells or shares the personal information of 100,000 or more consumers or households . . . ," omitting entirely any reference to "devices." *See id.* § 1798.140(d)(1)(B) (effective Jan. 1, 2023).

[20]This definition will be expanded to "selling or sharing" under the CPRA. *See* Cal. Civ. Code § 1798.140(d)(1)(C) (effective Jan. 1, 2023).

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

[22]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). The CPRA will more narrowly apply to an entity that controls or is controlled by a business that share common branding with the business "and with whom the business shares consumers' personal information." Cal. Civ. Code § 1798.140(d)(2) (effective Jan. 1, 2023).

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." Cal. Civ. Code § 1798.140(c)(2).

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

The collection or sale of personal information is not subject to the CCPA, however, if every aspect of that commercial conduct takes place "wholly outside of California."[23]

Businesses subject to the CCPA must impose on service providers, by contract, use and deletion obligations with respect to personal information. 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[24] pursuant to a written contract, provided that the contract

---

Common branding means "a shared name, servicemark, or trademark." *Id.*; *see generally supra* chapter 6 (trademarks, servicemarks and brand management). This definition will be modified under the CPRA to add the qualifier "such that the average consumer would understand that two or more entities are commonly owned." Cal. Civ. Code § 1798.140(d)(2) (effective Jan. 1, 2023).

A *business* will also be defined under the CPRA as a joint venture or partnership composed of businesses in which each business has at least a 40 percent interest, subject to the caveat that "the joint venture or partnership and each business that composes the joint venture or partnership shall separately be considered a single business, except that personal information in the possession of each business and disclosed to the Joint venture or partnership shall not be shared with the other business." *Id.* § 1798.140(d)(3) (effective Jan. 1, 2023).

A person that does business in California and would not otherwise be treated as a *business* will be deemed to be one if it "voluntarily certifies to the California Privacy Protection Agency that it is in compliance with, and agrees to be bound by, . . ." the CPRA. *See id.* § 1798.140(d)(4) (effective Jan. 1, 2023).

[23]Cal. Civ. Code § 1798.145(a)(6). Under the CPRA this provision will be expanded to encompass collection, sales, or *sharing* a consumer's personal information if every aspect of that commercial conduct takes place outside of California. *See id.* § 1798.145(a)(7) (effective Jan. 1, 2023).

The CPRA will also reverse the CCPA's prohibition on a business "storing, including on a device, personal information about a consumer when the consumer is in California and then collecting that personal information when the consumer and stored personal information is outside of California." *Id.* §§ 1798.145(a)(6) (not permitting this practice under the CCPA), 1798.145(a)(7) (not prohibiting this practice effective Jan. 1, 2023).

[24]*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

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

personal information was collected." Cal. Civ. Code § 1798.140(d). The statute provides seven examples of *business purposes,* which presumably is a non-exclusive list of examples. Those examples are:

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

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

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

(4) Short-term, transient use, provided 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. The definition is modified under the CPRA, and will apply to a business or the operational purposes of a service provider or contractor, subject to regulations that have yet to be promulgated. *See id.* § 1798.140(e) (effective Jan. 1, 2023). *Business purpose* also will be defined to include providing advertising and marketing services to a consumer, except for cross-context behavioral advertising (which is a defined term under the CPRA), "provided that for the purpose of advertising and marketing, a service provider or contractor shall not combine the personal information of opted-out consumers which the service provider or contractor receives from or on behalf of the business with personal information which the service provider or contractor receives from or on behalf of another person or persons, or collects from its own interaction with consumers." *Id.* § 1798.140(e)(6) (effective Jan. 1, 2023); *see also id.* §§ 1798.140(e)(4) (effective Jan. 1, 2023) (defining short-term, transient use, to include "nonpersonalized advertising shown as part of a consumer's current interaction with the business . . ."); 1798.140(t) (effective Jan. 1, 2023) (defining *non-personalized advertising* as "advertising and marketing that is based solely on a consumer's personal information derived from the consumer's

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

prohibits the entity receiving the information from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract for the business, or as otherwise permitted by [the CCPA], including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract with the business."[25] 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.

An entity that provides services to a person or organiza-

---

current interaction with the business, with the exception of the consumer's precise geolocation."); 1798.140(w) (effective Jan. 1, 2023) (defining *precise geolocation* to mean "any data that is derived from a device and that is used or intended to be used to locate a consumer within a geographic area that is equal to or less than the area of a circle with a radius of one thousand, eight hundred and fifty (1,850) feet, except as prescribed by regulations."). These definitions under the CPRA will result in "precise geolocation" not being a permissible business purpose for a service provider seeking to provide short-term, transient nonpersonalized advertising.

Cross-contextual behavioral advertising under the CPRA will mean "the targeting of advertising to a consumer based on the consumer's personal information obtained from the consumer's activity across businesses, distinctly-branded websites, applications, or services, other than the business, distinctly-branded website, application, or service with which the consumer intentionally interacts." *Id.* § 1798.140(k) (effective Jan. 1, 2023). The CPRA also changes the second example of a *business purpose,* which relates to cybersecurity, to "[h]elping to ensure security and integrity to the extent the use of the consumer's personal information is reasonably necessary and proportionate for these purposes." *Id.* § 1798.140(e)(2) (effective Jan. 1, 2023). *Security and integrity* are defined to mean "the ability: (1) of a network or an information system to detect security incidents that compromise the availability, authenticity, integrity, and confidentiality of stored or transmitted personal information; (2) to detect security incidents, resist malicious, deceptive, fraudulent, or illegal actions, and to help prosecute those responsible for such actions; and (3) a business to ensure the physical safety of natural persons." *Id.* § 1798.140(ac).

[25]Cal. Civ. Code § 1798.140(v). As noted earlier, the definition of *service provider* is modified in the CPRA, which effective January 1, 2023, also will include a separate category for *contractors*. *See id.* §§ 1798.140(j) (contractor), 1798.140(ag) (service provider) (effective Jan. 1, 2023).

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

tion that is not a *business* under the CCPA and its implementing regulations, and that would otherwise meet the requirements and obligations of a service provider, likewise will be deemed a *service provider*.[26]

To the extent that a business directs a second entity to collect personal information directly from a consumer, or about a consumer, on the first business's behalf, and the second entity would otherwise meet the requirements and obligations of a *service provider* under the CCPA and its implementing regulations, the second entity will be deemed a service provider of the first business for purposes of the CCPA.[27]

A service provider must certify to its compliance with the CCPA, in its written contract with a business.[28]

A service provider may not retain, use, or disclose personal information obtained in the course of providing services except:

(1) To process or maintain personal information on behalf of the business that provided the personal information or directed the service provider to collect the personal information, and in compliance with the written contract for services required by the CCPA;
(2) To retain and employ another service provider as a subcontractor, where the subcontractor meets the requirements for a service provider under the CCPA and these regulations;
(3) For internal use by the service provider to build or improve the quality of its services, provided that the

---

[26]Cal. Code Regs. § 999.314(a).

[27]Cal. Code Regs. § 999.314(b).

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

A service provider may not sell data on behalf of a business when a consumer has opted-out of the sale of their personal information with the business. Cal. Code Regs. § 999.314(d).

If a service provider receives a request from a consumer to know what personal information is collected or a request to delete it, the service provider must either act on behalf of the business in responding to the request or inform the consumer that the request cannot be acted upon because the request has been sent to a service provider. *Id.* § 999.314(e).

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

use does not include building or modifying household or consumer profiles to use in providing services to another business, or correcting or augmenting data acquired from another source;

(4) To detect data security incidents or protect against fraudulent or illegal activity; or

(5) For the purposes enumerated in Civil Code § 1798.145(a)(1) through 1798.145(a)(4).[29]

---

[29]Cal. Code Regs. § 999.314(c). Civil Code sections 1798.145(a)(1) through 1798.145(a)(4) provide that the CCPA shall not restrict a business' ability to:

(1) Comply with federal, state, or local laws.

(2) Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities.

(3) Cooperate with law enforcement agencies concerning conduct or activity that the business, service provider, or third party reasonably and in good faith believes may violate federal, state, or local law.

(4) Exercise or defend legal claims.

Cal. Civil Code § 1798.145(a)(1).

The CCPA also excludes from the scope of section 1798.120 (which otherwise affords consumers the right to opt-out of the sale or sharing of personal information) vehicle information or ownership information retained or shared between a new motor vehicle dealer and vehicle manufacturer, if the information is shared "for the purpose of effectuating, or in anticipation of effectuating, a vehicle repair covered by a vehicle warranty or a recall . . . ," provided that the new motor vehicle dealer or vehicle manufacturer with which that vehicle information or ownership information is shared does not sell, share, or use that information for any other purpose. Cal. Civil Code § 1798.145(g)(1). It also excludes vessel information or ownership information retained or shared between a vessel dealer and the vessel's manufacturer, if the vessel information or ownership information is shared for the purpose of effectuating, or in anticipation of effectuating, a vessel repair covered by a vessel warranty or a recall, provided that the vessel dealer or vessel manufacturer does not sell, share, or use that information for any other purposes. *Id.* § 1798.145(g)(2). These exclusions will remain unchanged under the CPRA. *See id.* § 1798.145(g) (effective Jan. 1, 2023).

These exceptions are codified and expanded with respect to law enforcement activities and cooperation with a government agency request for emergency access under the CPRA, effective January 1, 2023. *See id.* § 1798.145(a) (effective Jan. 1, 2023). Exceptions are also carved out to allow "activity involving the collection, maintenance, disclosure, sale, communication, or use of any personal information bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by a consumer reporting agency," as defined in 15 U.S.C.A. § 1681a(f), by a furnisher of information, as set forth in 15 U.S.C.A. § 1681s-2, "who provides information for

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

The CPRA expands somewhat on the list of provisions that a business must include in its contract with a service provider, effective January 1, 2023.[30] Given that contracts today may extend into 2023, businesses should consider when, whether, and how to amend their service provider contracts to account for these new provisions. The CPRA further will require specific contractual provisions where a ser-

---

use in a consumer report, as defined in" 15 U.S.C.A. § 1681a(d), and by a user of a consumer report as set forth in 15 U.S.C.A. § 1681b, but only to the extent this activity involves "the collection, maintenance, disclosure, sale, communication or use of such information by that agency, furnisher, or user . . . subject to regulation under the Fair Credit Reporting Act," 15 U.S.C.A. §§ 1681 *et seq*., "and the information is not collected, maintained, used, communicated, disclosed or sold except as authorized by the Fair Credit Reporting Act." *See* Cal. Civil Code § 1798.145(d) (effective Jan. 1, 2023). This exclusion, however, does not apply to the private cause of action for certain security breaches created by section 1798.150. *See id.* § 1798.145(d)(3) (effective Jan. 1, 2023); *see generally infra* § 26.13A[14] (analyzing the private right of action under 1798.150).

[30]The CPRA provides that, to qualify as a *service provider* under the CPRA, a person who processes personal information on behalf of a business and which receives from or on behalf of the business a consumer's personal information for a business purpose, must be restricted by contract from:

(A) selling or sharing the personal information;

(B) retaining, using, or disclosing the personal information for any purpose other than for the business purposes specified in the contract for the business, including retaining, using, or disclosing the personal information for a commercial purpose other than the business purposes specified in the contract with the business, or as otherwise permitted by this title;

(C) retaining, using, or disclosing the information outside of the direct business relationship between the service provider and the business; and

(D) combining the personal information which the service provider receives from or on behalf of the business, with personal information which it receives from or on behalf of another person or persons, or collects from its own interaction with the consumer, provided that the service provider may combine personal Information to perform any business purpose as defined in regulations . . . [to be adopted pursuant to Cal. Civ. Code § 1798.185(a)(10)], except as provided for in paragraph (6) of subdivision (e) of this Section and in regulations adopted by the California Privacy Protection Agency.

The contract may, subject to agreement with the service provider, permit the business to monitor the service provider's compliance with the contract through measures including, but not limited to, ongoing manual reviews and automated scans, and regular assessments, audits, or other technical and operational testing at least once every twelve (12) months.

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

vice provider subcontracts out its work.[31]

A service provider that is also a business must comply with the CCPA and its implementing regulations in its capacity as a business, with respect to any personal information that it collects, maintains, or sells outside of its role as a service provider.[32]

A business that discloses personal information to a service provider will not be liable under the CCPA if the service provider uses the personal information in violation of the 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."[33] A service provider likewise will not be liable under the CCPA for the obligations of a business for which it provides services.[34] Service providers are subject to enforcement actions brought by the California Attorney General[35] and presumably breach of contract actions brought by a contracting business.[36]

While a business generally must, upon request, disclose

---

[31]The CPRA provides that "if a service provider engages any other person to assist it in processing personal information for a business purpose on behalf of the business, or if any other person engaged by the service provider engages another person to assist in processing personal information for such business purpose, it shall notify the business of such engagement, and the engagement shall be pursuant to a written contract binding the other person to observe all the requirements . . ." of section 1798.104(ag). Cal. Civ. Code § 1798.140(ag)(2) (effective Jan. 1, 2023). Cal. Civ. Code § 1798.140(ag)(1) (effective Jan. 1, 2023).

[32]Cal. Code Regs. § 999.314(f).

[33]Cal. Civ. Code § 1798.145(j); *see also id.* §§ 1798.145(i)(1) (effective Jan. 1, 2023) (retaining the provision under the CPRA), 1798.135(g) (effective Jan. 1, 2023) (providing analogous protection under the CPRA where a business communicates a consumer's opt-out request and the person receiving that request violates the restrictions imposed under the CPRA, where the business does not have actual knowledge, or reason to believe, that the person intends to commit the violation, and making void any provision of a contract or agreement that purports "to waive or limit in any way" this provision).

[34]Cal. Civ. Code § 1798.145(j); *see also id.* § 1798.145(i)(1) (effective Jan. 1, 2023) (retaining the provision under the CPRA and extending it to both service providers *and contractors*, subject to the caveat that service providers and contractors shall be liable for their own violations of the CPRA).

[35]Cal. Civ. Code § 1798.155(b).

[36]For liability limitation provisions under the CPRA, *see, e.g.,* Cal. Civ. Code §§ 1798.135(g) (no liability under certain circumstances for a

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

the categories of information sold to another business or a *third party*,[37] a business is not required to disclose to consumers the service providers to which it provides access to personal information or categories of personal information it provides them.[38] 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 pur-

---

business communicating opt-out requests that are not acted upon), 1798.145(i) (no liability for a business disclosing, in compliance with the CPRA, personal information to a service provider or contractor that subsequently fails to treat it in accordance with the law)

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

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

(2)

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

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

(I) Selling the personal information.

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

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

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

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

Cal. Civ. Code § 1798.140(w).

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

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

suant to Section 1798.120."[39]

The CCPA 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;[40]
- 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),[41] affirmatively requires opt-in consent[42]); and
- 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

---

[39]Cal. Civ. Code § 1798.115(d).

[40]Cal. Civ. Code § 1798.100(b).

[41]15 U.S.C.A. §§ 6501 to 6506; 16 C.F.R. §§ 312.1 to 312.13; *supra* § 26.13[2].

[42]Cal. Civ. Code § 1798.120(c); *see generally infra* § 26.13A[8] (addressing verifiable parental consent). *Consent* is not expressly defined under the CCPA but under the CPRA, effective January 1, 2023, will mean

> any freely given, specific, informed and unambiguous indication of the consumer's wishes by which he or she, or his or her legal guardian, by a person who has power of attorney or is acting as a conservator for the consumer, such as by a statement or by a clear affirmative action, signifies agreement to the processing of personal information relating to him or her for a narrowly defined particular purpose. Acceptance of a general or broad terms of use or similar document that contains descriptions of personal information processing along with other, unrelated information, does not constitute consent. Hovering over, muting, pausing, or closing a given piece of content does not constitute consent. Likewise, agreement obtained through use of dark patterns does not constitute consent.

Cal. Civ. Code § 1798.140(h) (effective Jan. 1, 2023). A *dark pattern* under the CPRA will mean "a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice, as further defined by regulation." *Id.* § 1798.140(l) (effective Jan. 1, 2023).

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

information purchased from another business without explicitly notifying the consumers whose information would be sold and providing an opportunity to opt-out.[43]

Under the CPRA, consumers, effective January 1, 2023, will have broader deletion rights, a right to correct inaccurate or incomplete information, a right to opt-out of secondary use of *sensitive personal information,* and a right to prevent sharing, in addition to sales, of personal information.[44]

Personal information under the CCPA is "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[45] It includes, but is not limited to, a non-exclusive list of qualifying data elements, if the element "identifies, relates to, describes, is reasonably capable of being associated with, or

---

[43]Cal. Civ. Code § 1798.115(d).

[44]*See, e.g.,* Cal. Civ. Code §§ 1798.100 (general duties of a business that collects personal information; requiring a business that controls the collection of a consumer's personal information, at or before the point of collection, to inform consumers of the categories of personal information collected or used, and whether the information is sold or shared, setting rules around the collection of sensitive personal information, among other provisions), 1798.105 (consumer right to delete personal information), 1798.106 (creating a new right to correct inaccurate personal information), 1798.110 (right to know and right to access, expanded to cover sharing), 1798.115 (right to know what personal information is sold or shared), 1798.120 (right to opt-out of selling or sharing), 1798.121 (new right to limit use and disclosure of sensitive information) (effective Jan. 1, 2023).

The rights to deletion, correction of inaccurate personal information, and right to know and access what is collected, set forth in sections 1798.105, 1798.106, and 1798.110, will not, however, apply to household data. *See* Cal. Civ. Code § 1798.145(p) (effective Jan. 1, 2023).

The right to deletion also will not apply to student grades, educational scores, or educational test results that a business holds on behalf of a local educational agency at which the student whose records are at issue is currently enrolled. *See id.* § 1798.145(q)(1) (effective Jan. 1, 2023). Likewise, the right to know and access set forth in section 1798.110 does not extend to certain educational assessments. *See id.* § 1798.145(q)(2) (effective Jan. 1, 2023).

Limitations are also placed on a consumer's right to delete or opt out under sections 1798.105 and 1798.120 where consent had been obtained for use in a physical item such as a yearbook. *See id.* § 1798.145(r) (effective Jan. 1, 2023).

[45]Cal. Civ. Code § 1798.140(o)(1).

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

could be reasonably linked,[46] directly or indirectly, with a particular consumer or household . . . ."[47] The data elements identified in the statute (in section 1798.140(o)(1)),

---

[46]What it means for information to be *reasonably linked* to a particular consumer or household is not defined under the CCPA, the final regulations, or the CPRA. 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].

[47]Cal. Civ. Code § 1798.140(o)(1). As previously noted, *household,* which is not defined in the statute, is limited under the CCPA regulations 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." Cal. Code Regs. § 999.301(k). A *unique identifier* (or *unique personal identifier*) is defined under the CCPA as

> a persistent identifier that can be used to recognize a consumer, a family, or a device that is linked to a consumer or family, over time and across different services, including, but not limited to, a device identifier; an Internet Protocol address; cookies, beacons, pixel tags, mobile ad identifiers, or similar technology; customer number, unique pseudonym, or user alias; telephone numbers, or other forms of persistent or probabilistic identifiers that can be used to identify a particular consumer or device. For purposes of this subdivision, "family" means a custodial parent or guardian and any minor children over which the parent or guardian has custody.

Cal. Civ. Code § 1798.140(x). Session cookies generally do not qualify as "persistent identifiers" and therefore typically are not "personal information." The Attorney General clarified that "[i]f a session cookie cannot be used to recognize a consumer, family, or device that is linked to a consumer or family, over time and across services, it would not fall within this definition." *See* Final Statement of Reasons, Appendix A, at Response 892 (June 11, 2020), *available at* https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-fsor-appendix-a.pdf.

A *probabilistic identifier* is "the identification of a consumer or a device to a degree of certainty of more probable than not based on any categories of personal information included in, or similar to, the categories enumerated in the definition of personal information." *Id.* § 1798.140(p).

These definitions will be modified in minor respects under the CPRA (in renumbered subsections) effective January 1, 2023. *See id.* §§ 1798.140(q) (defining *household* as "a group, however identified, of consumers who cohabitate with one another at the same residential address and share use of common device(s) or service(s)."), 1798.140(x) (defining *probabilistic identifier* as under the CCPA but adding "consumer's" before "device"), 1798.140(aj) (defining *unique identifier* as under the CCPA but qualifying "device" to be one "that is linked to a consumer or family" and changing "minor children" to "children under 18 years of age") (effective Jan. 1, 2023).

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

which may be expanded by future regulation,[48] 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.[49]

(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.[50]

(F) Internet or other electronic network activity informa-

When a privacy policy governs *personal information*, a court applying California law may construe the term coextensively with the definition set forth in section 1798.140. *See, e.g., Calhoun v. Google LLC,* 526 F. Supp. 3d 605, 622 (N.D. Cal. 2021) (construing a privacy policy governed by California law that defined *personal information* as "information that you provide to us which personally identifies you, such as your name, email address, or billing information, or other data that can reasonably be linked to such information by Google, such as information we associate with your Google account" to encompass those data elements subject to section 1798.140, including potentially unique persistent cookie identifiers, browsing history, a user's X-Client data header, post communications, and a user's IP address and User-Agent information about their device).

[48]Cal. Civ. Code § 1798.185(a)(1). This authority will continue, and be expanded, under the CPRA.

[49]Cal. Civ. Code § 1798.80(e) defines *collects*, *collected* or *collection*, but expressly references personal information *pertaining to a consumer*, including information received from a consumer "either actively or passively, or by observing the consumer's behavior."

[50]*Biometric information* is defined in Cal. Civ. Code § 1798.140(b). The definition of what constitutes biometric information will be expanded somewhat under the CPRA, effective January 1, 2023, in renumbered subsection 1798.140(c). Under the CCPA, biometric information presently means

> an individual's physiological, biological, or behavioral characteristics, including an individual's deoxyribonucleic acid (DNA), that can be used, singly or in combination with each other or with other identifying data, to establish individual identity. Biometric information includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms,

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

tion, 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.[51]

Under the CPRA, this list will be expanded, as of January 1, 2023, to include sensitive personal information.[52]

The definition of *personal information* is quite broad. For

---

gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.

Cal. Civ. Code § 1798.140(b).

[51]Cal. Civ. Code § 1798.140(o)(1).

[52]Cal. Civ. Code § 1798.140(v)(1) (effective Jan. 1, 2023). *Sensitive personal information* is defined under the CPRA to mean:

(l) personal information that reveals (A) a consumer's social security, driver's license, state identification card, or passport number; (B) a consumer's account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account; (C) a consumer's precise geolocation; (D) a consumer's racial or ethnic origin, religious or philosophical beliefs, or union membership; (E) the contents of a consumer's mail, email and text messages, unless the business is the intended recipient of the communication; (F) a consumer's genetic data; and (2)(A) the processing of biometric information for the purpose of uniquely identifying a consumer; (B) personal information collected and analyzed concerning a consumer's health; or (C) personal information collected and analyzed concerning a consumer's sex life or sexual orientation.

Id. § 1798.140(ae) (effective Jan. 1, 2023). *Precise geolocation* means "any data that is derived from a device and that is used or intended to be used to locate a consumer within a geographic area that is equal to or less than the area of a circle with a radius of one thousand, eight hundred and fifty (1,850) feet, except as prescribed by regulations." *Id.* § 1798.140(w) (effective Jan. 1, 2023). The Attorney General is directed to issues regulations by July 1, 2022 further defining *precise geolocation* "such as where the size defined Is not sufficient to protect consumer privacy in sparsely

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

example, the inclusion of "[i]nferences drawn from the information identified in this subdivision to create a profile about a consumer" in subsection (K) means that 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*[53] (other than biometric information collected by a business about a consumer without the consumer's knowledge[54]—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* data used for a purpose not compatible with the purpose for

---

populated areas, or when the personal Information Is used for normal operational purposes, such as billing." *Id.* § 1798.185(a)(13) (effective Jan. 1, 2023).

Sensitive personal information that is *publicly available* within the meaning of section 1798.140(v)(2) will not be considered sensitive personal information or personal information under the CPRA. *Id.* (effective Jan. 1, 2023).

[53]*Publicly available* means "information that is lawfully made available from federal, state, or local government records." Cal. Civ. Code § 1798.140(o)(2). Except for biometric information collected by a business about a consumer without the consumer's knowledge, for purposes of section 1798.140(o)(2), "publicly available" means "information that is lawfully made available from federal, state, or local government records." *Id.*

Under the CPRA, this exclusion from the definition of *personal information* will be expanded to also encompass "lawfully obtained, truthful information that is a matter of public concern." *Id.* § 1798.140(v)(2) (effective Jan. 1, 2023).

With respect to what is "publicly available" for purposes of the exclusion from the definition of personal information, the CPRA defines *publicly available* to mean (subject to the same exclusion as under the CCPA for biometric information collected by a business about a consumer without the consumer's knowledge):

> Information that is lawfully made available from federal, state, or local government records, or information that a business has a reasonable basis to believe is lawfully made available to the general public by the consumer or from widely distributed media, or by the consumer; or information made available by a person to whom the consumer has disclosed the information if the consumer has not restricted the information to a specific audience."

Id. § 1798.140(v)(2) (effective Jan. 1, 2023).

[54]Cal. Civ. Code § 1798.140(o)(2). This exclusion remains without change under the CPRA in renumbered subsection 1798.140(v)(2) (effective Jan. 1, 2023).

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

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 cannot become transmuted into personal information.[55]

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."[56] 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."[57] 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 reiden-

---

[55]The CPRA goes even further, extending the definition of *publicly available* information to include "information that a business has a reasonable basis to believe is lawfully made available to the general public by the consumer or from widely distributed media, or by the consumer; or information made available by a person to whom the consumer has disclosed the information if the consumer has not restricted the information to a specific audience." Cal Civ. Code § 1798.140(v)(2) (effective Jan. 1, 2023).

[56]Cal. Civ. Code § 1798.140(o)(3); *see also id.* § 1798.140(v)(2) (effective Jan. 1, 2023).

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). The definition of *deidentified* under the CPRA, which will be codified at Cal. Civ. Code § 1798.140(m) effective January 1, 2023, is discussed later in this section.

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.* This definition will remain unchanged under the CPRA but will be renumbered as section 1798.140(b).

[57]Cal. Civ. Code § 1798.145(a)(5); *see also id.* (effective Jan. 1, 2023) (expanding the provision to also address sharing).

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

tification 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.[58]

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 excluded from the definition of *personal information*).

Conversely, the CCPA generally does not require reidentification or de-anonymization of deidentified or aggregate consumer data so that the information would be subject to the requirements imposed on *personal information* under the law (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).[59] Specifically, the CCPA may not be construed to require "a business to reidentify or otherwise

---

[58]This 4-part test is deleted from new section 1798.140(m), which will define *deidentified* under the CPRA to mean information that cannot reasonably be used to infer information about, or otherwise be linked to, a particular consumer, provided that the business that possesses the information: (A) takes reasonable measures to ensure that the information cannot be associated with a consumer or household; (B) publicly commits to maintain and use the information in deidentified form and not to attempt to reidentify the information, except that the business may attempt to reidentify the information solely for the purpose of determining whether its deidentification processes satisfy the requirements of this subdivision; and (C) contractually obligates any recipients of the information to comply with all provisions of this subdivision. Cal. Civ. Code § 1798.140(m) (effective Jan. 1, 2023).

[59]The Attorney General opted not to require a specific format in the final CCPA regulations, but in amended final regulations that took effect on March 15, 2021, authorized the optional use of the following icon in addition to, rather than in lieu of, posting the notice of the right to opt out or a "Do Not Sell My Personal Information" link (provided the icon is approximately the same size as any other icons used by the business on its webpage):

Cal. Code Regs. § 999.306(f).

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

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.[60] The regulations further state that "[i]f a business maintains consumer information that is deidentified, a business is not obligated to provide or delete this information in response to a consumer request or to re-identify individual data to verify a consumer request."[61]

The CCPA gives the California Attorney General broad authority to issue regulations interpreting and implementing the law, 'to further . . . [its] purposes . . . .'[62] Final

---

[60]Cal. Civ. Code § 1798.145(k). This provision will be expanded under the CPRA to provide, effective January 1, 2023, that the CPRA may not be construed

> to require a business, service provider, or contractor to: (1) reidentify or otherwise link information that, in the ordinary course of business, is not maintained in a manner that would be considered personal information; (2) retain any personal information about a consumer if, in the ordinary course of business, that information about the consumer would not be retained; or (3) maintain information in identifiable, linkable or associable form, or collect, obtain, retain, or access any data or technology, in order to be capable of linking or associating a verifiable consumer request with personal information.

Id. § 1798.145(j) (effective Jan. 1, 2023).

[61]Cal. Code Regs. § 999.323(f).

[62]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 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.

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

regulations dated August 14, 2020, as amended on March 15, 2021, are included in Appendix 9 at the end of this chapter. Information on further rulemaking may be found on the California Attorney General's website at: https://oag.ca.gov/privacy/ccpa/current.

While the CCPA will remain in effect until December 31,

(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).

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

2022, rulemaking under the CPRA will begin prior to that time, with final regulations to be adopted by July 1, 2022, which is also the time that the California Privacy Protection Agency (CPPA) will take over responsibility for rulemaking under the CPRA. CPRA regulations will tackle a number of new issues, including access and opt-out rights with respect to businesses' use of automated decision-making technology, including profiling.[63] The Governor of California, the Attorney General and state government leaders announced the first appointments to the CPPA on March 17, 2021.[64]

Violations of the CCPA are largely enforced 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 compel compliance.[65] The CCPA empowered the Attorney General to begin enforcement on July 1, 2020,[66] and the Office of the Attorney General in fact sent out its first enforcement letters shortly thereafter. Under the CPRA this authority will be transitioned to the California Privacy Protection Agency (CPPA), a new agency created by the CPRA.[67] Administrative enforcement is addressed in subsection 26.13A[13].

---

[63]*See* Cal. Civ. Code § 1798.185 (effective Jan. 1, 2023) (setting forth the scope of rulemaking authority under the CPRA). A copy of the CPRA, as adopted by California voters in November 2020, is reprinted in Appendix 11 to this chapter.

Profiling is defined under the CPRA to mean "any form of automated processing of personal information, as further defined by regulations pursuant to . . . [Cal. Civ. Code § 1798.185(a)(16)], to evaluate certain personal aspects relating to a natural person, and in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements." Cal. Civ. Code § 1798.140(z) (effective Jan. 1, 2023).

[64]*See* Press Release, Office of Governor Gavin Newsom, "California Officials Announce California Privacy Protection Agency Board Appointments" (Mar. 17, 2021), *available at* https://www.gov.ca.gov/2021/03/17/california-officials-announce-california-privacy-protection-agency-board-appointments/ (announcing the appointment of Jennifer M. Urban, John Christopher Thompson, Angela Sierra, Lydia de la Torre, and Vinhcent Le as CPPA Board Members).

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

[66]*See* Cal. Civ. Code § 1798.185(c) (permitting enforcement to begin on the earlier of six months after publication of final regulations or July 1, 2020).

[67]*See* Cal. Civ. Code §§ 1798.199.10 to 1798.199.100.

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

The CCPA also authorizes a private right of action and provides for statutory damages for certain security breaches involving unredacted and unencrypted information, resulting from a business's failure to implement and maintain reasonable security procedures, subject to a 30 day right to cure,[68] as discussed in section 26.13A[14]. Litigation has been allowed since January 1, 2020 and will be largely unchanged under the CPRA provision that will take effect on January 1, 2023, as analyzed in section 26.13A[14] (although, among other things, litigation will now also be available for certain breaches that involve a consumer's "email address in combination with a password or security question and answer that would permit access to the account."[69]).

While the CCPA has been amended by the legislature multiple times, amendments to the CPRA, once it takes effect, will only be permitted to the extent they are "consistent with and further the purpose and intent of the Act . . . ," which is a material restriction on legislative power imposed by the ballot initiative which resulted in the CPRA taking effect.[70]

Persons and entities not subject to the CCPA also may be subject to other California privacy laws, many of which were enacted prior to the time the CCPA took effect, and which are analyzed in section 26.13[6]. For persons and entities subject to the CCPA, those laws potentially impose additional obligations.

26.13A[2] The CCPA's Required Privacy Policy and 3 Other Notices to consumers Required by the CCPA

26.13A[2][A] Required Notices and Their Style/Format—In General

The CCPA requires businesses to provide four basic types of notices.

First, every business that is required to comply with the CCPA must provide a privacy policy that complies with the CCPA and the requirements of California Code of Regula-

---

[68]Cal. Civ. Code § 1798.150(a).

[69]Cal. Civ. Code § 1798.150(a) (effective Jan. 1, 2023).

[70]*See* Consumer Privacy Rights Act (Proposition 24) §§ 3 (purpose and intent), 25(a) (limitation on legislative amendment) (Nov. 2020); *see generally infra* Appendix 11,

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

tions section 999.308.[1]

Second, a business that collects personal information from a consumer must provide a *notice at collection*[2] in accordance with the provisions of the CCPA and California Code of Regulations section 999.35.

Third, a business that *sells* personal information must provide a notice of the right to opt-out[3] in accordance with the CCPA and California Code of Regulations section 999.306.

Fourth, a business that offers a *financial incentive*[4] or *price or service difference*[5] must provide a notice of financial incentive[6] in accordance with the CCPA and California Code of

---

[Section 26.13A[2][A]]

[1]*Privacy policy*, as referred to in Cal. Civil Code § 1798.130(a)(5), means "the statement that a business shall make available to consumers describing the business's practices, both online and offline, regarding the collection, use, disclosure, and sale of personal information, and of the rights of consumers regarding their own personal information."

[2]*Notice at collection* has a somewhat circular definition. The term is defined to mean "the notice given by a business to a consumer at or before the point at which a business collects personal information from the consumer as required by Civil Code section 1798.100, subdivision (b), and specified in these regulations." Cal. Code Regs. § 999.301(l).

[3]The CCPA uses the term *notice of right to opt-out*, which means "the notice given by a business informing consumers of their right to opt-out of the sale of their personal information as required by Civil Code sections 1798.120 and 1798.135 and specified in these regulations." Cal. Code Regs. § 999.301(m).

[4]A *financial incentive* is "a program, benefit, or other offering, including payments to consumers, related to the collection, deletion, or sale of personal information." Cal. Code Regs. § 999.301(j).

[5]*Price or service difference* means

(1) any difference in the price or rate charged for any goods or services to any consumer related to the collection, retention, or sale of personal information, including through the use of discounts, financial payments, or other benefits or penalties; or

(2) any difference in the level or quality of any goods or services offered to any consumer related to the collection, retention, or sale of personal information, including the denial of goods or services to the consumer.

Cal. Code Regs. § 999.301(o).

[6]*Notice of financial incentive* means "the notice given by a business explaining each financial incentive or price or service difference as required by Civil Code section 1798.125, subdivision (b), and specified in these regulations." Cal. Code Regs. § 999.301(n).

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

Regulations section 999.307.[7]

Under the CPRA, effective January 1, 2023, a business that collects personal information about consumers will also be required to disclose that consumers have the right to request correction of inaccurate personal information (and use commercially reasonable efforts to correct inaccurate personal information when directed to do so by a consumer, subject to additional provisions to be set forth in regulations that will be issued by July 1, 2022).[8]

The purpose of the privacy policy required by the CCPA "is to provide consumers with a comprehensive description of a business's online and offline practices regarding the collection, use, disclosure, and sale of personal information and of the rights of consumers regarding their personal information."[9]

With respect to notice at the point of collection (referred to in the CCPA regulations as *notice at collection*), the purpose "is to provide consumers with timely notice, at or before the point of collection, about the categories of personal information to be collected from them and the purposes for which the personal information will be used."[10]

Notice of the right to opt-out is intended to "inform consumers of their right to direct a business that sells their personal information to stop selling their personal information."[11]

A notice of financial incentive is intended to "explain to the consumer the material terms of a financial incentive or price or service difference the business is offering so that the consumer may make an informed decision about whether to participate."[12] A business that does not offer a financial incentive or price or service difference is not required to provide a notice of financial incentive.[13]

CCPA regulations govern the format of notices from businesses to consumers (at the point of collection, of the right to

---

[7] *See* Cal. Code Regs. § 999.304.

[8] *See* Cal. Civ. Code § 1798.106 (effective Jan. 1, 2023).

[9] Cal. Code Regs. § 999.308(a)(1).

[10] Cal. Code Regs. § 999.305(a)(1).

[11] Cal. Code Regs. § 999.306(a)(1).

[12] Cal. Code Regs. § 999.307(a)(1).

[13] Cal. Code Regs. § 999.307(a)(1).

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

opt-out, of financial incentives, and of its CCPA-compliant privacy policy) and require that any such notice be "designed and presented in a way that is easy to ready and understandable to consumers" and:

- "[u]se plain, straightforward language and avoid technical or legal jargon;"[14]
- "[u]se a format that draws the consumer's attention to the notice and makes the notice readable, including on smaller screens, if applicable;"[15]
- be available in the languages in which the business in its ordinary course provides contracts, disclaimers, sales announcements, and other information to consumers in California;[16]
- be reasonably accessible to consumers with disabilities;[17] and
- "be made readily available where consumers will encounter it at or before the point of collection of any personal information . . . ."[18]

These requirements may change when CPRA regulations

---

[14]Cal. Code Regs. §§ 999.305(a)(2)(a), 999.306(a)(2)(a).

[15]Cal. Code Regs. §§ 999.305(a)(2)(b), 999.306(a)(2)(b).

[16]Cal. Code Regs. §§ 999.305(a)(2)(c), 999.306(a)(2)(c).

[17]Cal. Code Regs. §§ 999.305(a)(2)(d), 999.306(a)(2)(d), 999.307(a)(2)(d), 999.308(a)(2)(d). "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." *Id.* Those guidelines may be accessed at https://www.w3.org/TR/2018/REC-WCAG21-20180605/

"In other contexts, the business shall provide information on how a consumer with a disability may access the notice in an alternative format." Cal. Code Regs. §§ 999.305(a)(2)(d), 999.306(a)(2)(d), 999.307(a)(2)(d), 999.308(a)(2)(d); *see generally infra* § 48.06[4] (analyzing website and mobile accessibility).

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

[18]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 CCPA regulations contained several illustrative examples of what it means to provide notice at 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 PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

are issued on or before July 1, 2022.

26.13A[2][B] Privacy Policy

The CCPA requires that businesses that collect, sell, or disclose California residents' personal information publicly inform consumers of their rights under the CCPA in an "online privacy policy," "in any California-specific description of consumers' privacy rights," or, if the business does not maintain those policies, "on its Internet website . . . ."[1] A business must update these disclosures "at least once every 12 months."[2]

What must be included in the Privacy Policy is set forth in the statute and in more granular detail in the regulations.

The disclosure must include "one or more designated methods for submitting" disclosure requests under the statute.[3] Additionally, a business must disclose the categories of personal information that it has collected, sold, or disclosed in the previous 12 months.[4]

A business that collects consumers' personal information

---

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 information, 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).

[Section 26.13A[2][B]]

[1]14 Cal. Civ. Code § 1798.130(a)(5). As noted earlier, a *Privacy policy*, as referred to in Cal. Civil Code § 1798.130(a)(5), means "the statement that a business shall make available to consumers describing the business's practices, both online and offline, regarding the collection, use, disclosure, and sale of personal information, and of the rights of consumers regarding their own personal information."

[2]15 Cal. Civ. Code § 1798.130(a)(5).

[3]16 Cal. Civ. Code § 1798.130(a)(5)(A).

[4]17 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).

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

is required by the statute to disclose:

(1) the "categories of personal information it has collected about" consumers;
(2) the "categories of sources[5] 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[6] 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."[7]

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-

---

Effective January 1, 2023, regulations may provide for a longer time period than 12 months for personal information collected on or after January 1, 2022. *See* Cal. Civ. Code § 1798.130(a)(2)(B). CPRA regulations will be propounded on or by July 1, 2022. A nonexclusive list of issues to be considered is set forth in the CPRA, Cal. Civ. Code § 1798.185(a).

[5]*Categories of sources* means "types or groupings of persons or entities from which a business collects personal information about consumers, described with enough particularity to provide consumers with a meaningful understanding of the type of person or entity." Cal. Code Regs. § 999.301(d). They may include "the consumer directly, advertising networks, internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, and data brokers." *Id.*

[6]*Categories of third parties* means "types or groupings of third parties with whom the business shares personal information, described with enough particularity to provide consumers with a meaningful understanding of the type of third party." Cal. Code Regs. § 999.301(e). They may include "advertising networks, internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, and data brokers." *Id.*

[7]18 Cal. Civ. Code §§ 1798.110(c)(1) to 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.

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

ceding 12 months, it must "disclose that fact."[8]

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.[9]

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.[10]

The regulations provide that the Privacy Policy, in addition to being easy to read and understandable to consumers[11] (as discussed above in section 26.13A[2][A]), must be posted online "through a conspicuous link using the word 'privacy' on the business's website homepage or on the download or landing page of a mobile application. If the business has a California-specific description of consumers' privacy rights on its website, then the privacy policy shall be included in that description."[12] A business that does not operate a website must make its privacy policy conspicuously available to consumers.[13] A mobile application may include a link to

---

[8]19 Cal. Civ. Code §§ 1798.130(a)(5)(C)(i), 1798.130(a)(5)(C)(ii). As noted above, the CPRA authorizes the adoption of regulations to require disclosure for a longer period than 12 months, for personal information collected on or after January 1, 2022. *See* Cal. Civ. Code § 1798.130(a)(2)(B) (effective Jan. 1, 2023).

[9]20 Cal. Civ. Code § 1798.135(a)(2). As noted earlier in section 26.13A[1], the Attorney General opted not to require a specific format in the final CCPA regulations, but authorized the optional use of the following icon in addition to posting the notice of right to opt-out but not in lieu of any requirement to post the notice of right to opt-out or a "Do Not Sell My Personal Information" link (provided that icon is approximately the same size as any other icons used by the business on its webpage)

Cal. Code Regs. § 999.306(f).

[10]21 Cal. Civ. Code §§ 1798.125(b)(2), 1798.130(a)(5)(A).

[11]*See* Cal. Code Regs. § 999.308(a)(2); *see generally supra* § 26.13A[2][A] (addressing general style and format requirements).

[12]Cal. Code Regs. § 999.308(b).

[13]Cal. Code Regs. § 999.308(b).

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

the privacy policy in the application's settings menu.[14]

The regulations provide that a privacy policy must include the following information:

(1) Right to Know About Personal Information Collected, Disclosed, or Sold.
   a. Explanation that a consumer has the right to request that the business disclose what personal information it collects, uses, discloses, and sells.
   b. Instructions for submitting a verifiable consumer request to know and links to an online request form or portal for making the request, if offered by the business.
   c. General description of the process the business will use to verify the consumer request, including any information the consumer must provide.
   d. Identification of the categories of personal information the business has collected about consumers in the preceding 12 months. The categories shall be described in a manner that provides consumers a meaningful understanding of the information being collected.
   e. Identification of the categories of sources from which the personal information is collected.
   f. Identification of the business or commercial purpose for collecting or selling personal information. The purpose shall be described in a manner that provides consumers a meaningful understanding of why the information is collected or sold.
   g. Disclosure or Sale of Personal Information.
      1. Identification of the categories of personal information, if any, that the business has disclosed for a business purpose or sold to third parties in the preceding 12 months.
      2. For each category of personal information identified, the categories of third parties to whom the information was disclosed or sold.
      3. Statement regarding whether the business has actual knowledge that it sells the personal information of consumers under 16 years of age.

(2) Right to Request Deletion of Personal Information.

[14]Cal. Code Regs. § 999.308(b).

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

a. Explanation that the consumer has a right to request the deletion of their personal information collected by the business.
b. Instructions for submitting a verifiable consumer request to delete and links to an online request form or portal for making the request, if offered by the business.
c. General description of the process the business will use to verify the consumer request, including any information the consumer must provide.

(3) Right to Opt-Out of the Sale of Personal Information.
a. Explanation that the consumer has a right to opt-out of the sale of their personal information by a business.
b. Statement regarding whether or not the business sells personal information. If the business sells personal information, include either the contents of the notice of right to opt-out or a link to it in accordance with section 999.306.

(4) Right to Non-Discrimination for the Exercise of a Consumer's Privacy Rights.
a. Explanation that the consumer has a right not to receive discriminatory treatment by the business for the exercise of the privacy rights conferred by the CCPA.

(5) Authorized Agent.
a. Instructions on how an authorized agent can make a request under the CCPA on the consumer's behalf.

(6) Contact for More Information.
a. A contact for questions or concerns about the business's privacy policies and practices using a method reflecting the manner in which the business primarily interacts with the consumer.

(7) Date the privacy policy was last updated.

(8) If subject to the requirements set forth in section 999.317, subsection (g), the information compiled in section 999.317, subsection (g)(1), or a link to it.[15]

(9) If the business has actual knowledge that it sells the

[15]As discussed in greater length in section 26.13A[8], Cal. Code Regs. § 999.317(g) requires that a business "that knows or reasonably should know that it, alone or in combination, buys, receives for the business's commercial purposes, sells, or shares for commercial purposes the personal

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

personal information of consumers under 16 years of age, a description of the processes required by sections 999.330 and 999.331.[16]

The CCPA was further amended in 2020 to require disclosures by certain businesses that sell or disclose deidentified patient information. Specifically, a business that sells or discloses deidentified patient information that was deidentified pursuant to 45 C.F.R. § 164.514 (and therefore is excluded from the scope of the CCPA by Cal. Civ. Code § 1798.146(a)(4)(A)(i)) must disclose whether it sells or discloses "deidentified patient information derived from patient information and, if so, whether that patient information was deidentified pursuant to" the deidentification methodology described in 45 C.F.R. § 164.514(b)(1) (commonly known as the HIPAA expert determination method) and/or the deidentification methodology described in 45 C.F.R. § 164.514(b)(2) (commonly known as the HIPAA safe harbor method).[17]

As set forth below in section 26.13A[9], additional disclosures are required in a Privacy Policy when information is collected from minors younger than 16 years old.

26.13A[2][C] Notice at Collection

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.[1] 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

---

information of 10,000,000 or more consumers in a calendar year" must, among other things, compile metrics on the number of requests for information, requests to delete information, and requests to opt-out of sales, for the prior calendar year, and disclosure these metrics in its Privacy Policy or on its website, by July 1 of every calendar year.

[16]Cal. Code Regs. § 999.308(c).

[17]*See* Cal. Civ. Code § 1798.135(a)(5)(D).

[Section 26.13A[2][C]]

[1]Cal. Civ. Code § 1798.100(b).

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

consumer.[2]

The regulations provide that if a business does not give notice at collection to a consumer "at or before the point of collection of their personal information, . . ." it may not collect personal information from the consumer.[3] This notice must be separate from a business's privacy policy, given that the notice "at or before" collection must "link to the privacy policy, or in the case of offline notices, where the business's privacy policy can be found online."[4]

A business, in its notice at collection, must include, in a way that (as discussed above in section 26.13A[2][A]) is easy to read and understandable to consumers:[5]

(1) A list of the categories of personal information about consumers to be collected. Each category of personal information shall be written in a manner that provides consumers a meaningful understanding of the information being collected.
(2) The business or commercial purpose(s) for which the categories of personal information will be used.
(3) If the business sells personal information, the link titled "Do Not Sell My Personal Information" required by section 999.315, subsection (a), or in the case of offline notices, where the webpage can be found online.[6]
(4) A link to the business's privacy policy, or in the case of offline notices, where the privacy policy can be found online.[7]

Where personal information is collected from a consumer

---

[2]Cal. Civ. Code § 1798.100(b).

[3]Cal. Code Regs. § 999.305(a)(6).

[4]Cal. Code Regs. § 999.305(b)(4).

[5]*See* Cal. Code Regs. § 999.308(a)(2); *see generally supra* § 26.13A[2][A] (addressing general style and format requirements).

[6]The Attorney General opted not to require a specific format in the final CCPA regulations, but authorized the optional use of the following icon in addition to posting the notice of right to opt-out but not in lieu of any requirement to post the notice of right to opt-out or a "Do Not Sell My Personal Information" link (provided that icon is approximately the same size as any other icons used by the business on its webpage):

Cal. Code Regs. § 999.306(f).

[7]Cal. Code Regs. § 999.305(b).

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

online, a business may provide notice at collection to a consumer by providing a link to the section of the business's privacy policy that contains this information.[8]

On the other hand, a business that does not collect personal information directly from a consumer does not need to provide a notice at collection to the consumer if it does not sell the consumer's personal information.[9]

A registered data broker likewise does not need to provide a notice at collection to a consumer if it has included in its registration submission a link to its online privacy policy that includes instructions on how a consumer can submit a request to opt-out.[10]

When a business collects personal information from a consumer's mobile device for a purpose that the consumer would not reasonably expect, it must "provide a just-in-time notice containing a summary of the categories of personal information being collected and a link to the full notice at collection."[11] As an example, the regulations provide that if the business offers a flashlight application and the application collects geolocation information, the business must provide a just-in-time notice, such as through a pop-up window when the consumer opens the application, containing the required disclosures.[12]

The requirements for notice at collection set forth in section 999.305 apply to a business's collection of employment-related information[13] except that, through January 1, 2021 or January 1, 2022,[14] (1) the notice at collection of employment-related information does not need to include the

---

[8]Cal. Code Regs. § 999.305(c).

[9]Cal. Code Regs. § 999.305(d).

[10]Cal. Code Regs. § 999.305(e). Data brokers and data broker registration are discussed later in this section.

[11]Cal. Code Regs. § 999.305(a)(4).

[12]*See* Cal. Code Regs. § 999.305(a)(4).

[13]*Employment-related information* means personal information that is collected by the business about a natural person for the reasons identified in Cal. Civil Code § 1798.145(h)(1). Cal. Code Regs. § 999.301(i). The collection of employment-related information, including for the purpose of administering employment benefits, is to be considered a business purpose. *Id.*

[14]California A.B. 1281, which was signed into law on September 29, 2020, extended the effective date of Cal. Civ. Code § 1798.145 applicable to employee data to January 1, 2022, rather than January 1, 2021, but "only

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

link or web address to the link titled "Do Not Sell My Personal Information" and (2) the notice at collection of employment-related information is not required to provide a link to the business's privacy policy.[15] The purpose of this sunset provision was to allow time for the legislature to better address employee privacy issues. In fact, unless extended by the legislature or otherwise amended, it may simply have the effect of deferring employer obligations to fully comply with the CCPA.

26.13A[2][D] Notice of the Right to Opt-Out

A business does not need to provide notice of a consumer's right to opt-out if it: (1) does not sell personal information; and (2) states in its privacy policy that it does not sell personal information.[1]

A business that sells the personal information of consumers, however, must provide notice of their right to opt-out by posting the notice "on the Internet webpage to which the consumer is directed after clicking on the 'Do Not Sell My Personal Information' link on the website homepage or the download or landing page of a mobile application."[2] In addition, a business that collects personal information through a mobile application may provide a link to the notice within the application, such as through the application's settings menu.[3] The notice must include, in a way that (as discussed above in section 26.13A[2][A]) is easy to read and understandable to consumers,[4] the information specified in section 999.306(c) of the regulations or link to the section of the

---

if the voters do not approve any ballot proposition that amends Section 1798.145 of the Civil Code at the November 3, 2020, statewide general election." Because Proposition 24—the California Privacy Rights Act (CPRA)—was adopted, the moratorium was extended to December 31, 2022 (the last day before the CPRA takes effect).

[15]Cal. Code Regs. §§ 999.305(f), 999.305(g).

[Section 26.13A[2][D]]

[1]Cal. Code Regs. § 999.306(d).

[2]Cal. Code Regs. § 999.306(b). The CCPA uses the term *notice of right to opt-out*, which means "the notice given by a business informing consumers of their right to opt-out of the sale of their personal information as required by Civil Code sections 1798.120 and 1798.135 and specified in these regulations." Cal. Code Regs. § 999.301(m).

[3]Cal. Code Regs. § 999.306(b).

[4]*See* Cal. Code Regs. § 999.308(a)(2); *see generally supra* § 26.13A[2][A] (addressing general style and format requirements).

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

business's privacy policy that contains the same information.[5] Section 999.306(c) requires:

(1) A description of the consumer's right to opt-out of the sale of their personal information by the business;
(2) The interactive form by which the consumer can submit their request to opt-out online, as required by section 999.315, subsection (a), or if the business does not operate a website, the offline method by which the consumer can submit their request to opt-out; and
(3) Instructions for any other method by which the consumer may submit their request to opt-out.[6]

No special format is required for the "Do Not Sell" link. In the February 2020 draft of the regulations, the Attorney General had proposed red buttons next to text in black that read "Do Not Sell My Personal Information" or "Do Not Sell My Info," but ultimately opted not to require a specific format in the final version of the CCPA regulations and withdrew the option for a business to use the shorthand "Do Not Sell My Info" in place of the longer phrase, "Do Not Sell My Personal Information." The graphics proposed but ultimately withdrawn from the final regulations are reprinted in Appendix 10.

In additional amendments to the final regulations, which took effect on March 15, 2021, the Attorney General authorized the optional use of the following blue-tinted icon, in addition to, but not in lieu of any requirement to post the notice of right to opt-out or a "Do Not Sell My Personal Information" link (and provided the icon is approximately the same size as any other icons used by the business on its webpage)[7]:

[5]Cal. Code Regs. § 999.306(b).

[6]Cal. Code Regs. § 999.306(c).

[7]Cal. Code Regs. § 999.306(f).

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

The March 2021 amended regulations also added the requirement for notice of the right to opt-out by an offline method for those businesses that collect personal information in the course of interacting with consumers offline.[8]

Under the CPRA, effective January 1, 2023, the "Do Not Sell" link must be changed to say "Do Not Sell *or Share* My Personal Information," consistent with the CPRA's expansion of coverage beyond mere selling, and where sensitive personal information is collected, a business must provide a clear and conspicuous link, titled "Limit the Use of My Sensitive Personal Information," to enable a consumer (or person authorized by a consumer) to limit the use or disclosure of sensitive personal information (or alternatively the business may use a single clearly-labeled link to opt-out of the sale or sharing of personal information and limit the use or disclosure of sensitive personal information).[9]

A business that does not provide the requisite notice, may not sell the personal information it collected during the time it did not have a notice of the right to opt-out posted, unless it obtains a consumer's affirmative authorization.[10] Thus, a business that previously failed to provide notice but begins to do so, may only sell personal information collected

---

[8]*See* Cal. Code Regs. § 999.306(b)(3). That amended rule states:

> (3) A business that sells personal information that it collects in the course of interacting with consumers offline shall also inform consumers by an offline method of their right to opt-out and provide instructions on how to submit a request to opt-out. Illustrative examples follow:
>
> a. A business that sells personal information that it collects from consumers in a brick-and-mortar store may inform consumers of their right to opt-out on the paper forms that collect the personal information or by posting signage in the area where the personal information is collected directing consumers to where the opt-out information can be found online.
>
> b. A business that sells personal information that it collects over the phone may inform consumers of their right to opt-out orally during the call when the information is collected.

Id.

[9]*See* Cal. Civ. Code § 1798.135(a) (effective Jan. 1, 2023). A business may avoid this requirement if it provides consumers an opt-out preference signal, pursuant to technical provisions to be established by regulation. *See id.* § 1798.135(b) (effective Jan. 1, 2023). Provisions governing sensitive personal information are set forth in new section 1798.121, which will take effect on January 1, 2023.

[10]Cal. Code Regs. § 999.306(e).

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

prospectively from the time it began providing the requisite notice, or earlier-collected personal information if it obtains affirmative authorization. *Affirmative authorization* means "an action that demonstrates the intentional decision by the consumer to opt-in to the sale of personal information" and, for consumers 13 years and older, is "demonstrated though a two-step process whereby the consumer shall first, clearly request to opt-in and then second, separately confirm their choice to opt-in."[11] The requirements for obtaining authorization from minors is separately addressed in section 26.13A[8].

26.13A[2][E] Notice of Financial Incentive (or price or service difference)

A notice of financial incentive, where required, must "explain to the consumer the material terms of a financial incentive or price or service difference the business is offering so that the consumer may make an informed decision about whether to participate."[1] A business that does not offer a financial incentive or price or service difference is not required to provide a notice of financial incentive.[2] Those businesses that do, however, must include in a notice of financial incentive (or, for those that offer a financial incentive or price or service difference online, by providing a link to the section of a business's privacy policy that contains this information[3]), in a way that (as discussed above in section 26.13A[2][A]) is easy to read and understandable to consumers,[4] the following details:

(1) A succinct summary of the financial incentive or price or service difference offered;

---

[11] Cal. Code Regs. § 999.301(a). For a consumer under 13 years of age, *affirmative authorization* means that "the parent or guardian has provided consent to the sale of the consumer's personal information in accordance with the methods set forth in section 999.330." *Id.*

Request to opt-in means "the affirmative authorization that the business may sell personal information about the consumer by a parent or guardian of a consumer less than 13 years of age, by a consumer at least 13 and less than 16 years of age, or by a consumer who had previously opted out of the sale of their personal information." *Id*. § 999.301(s).

[Section 26.13A[2][E]]

[1] Cal. Code Regs. § 999.307(a)(1).

[2] Cal. Code Regs. § 999.307(a)(1).

[3] Cal. Code Regs. § 999.307(a)(3).

[4] *See* Cal. Code Regs. § 999.308(a)(2); *see generally supra* § 26.13A[2][A] (addressing general style and format requirements).

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

(2) A description of the material terms of the financial incentive or price or service difference, including the categories of personal information that are implicated by the financial incentive or price or service difference and the value of the consumer's data;
(3) How the consumer can opt-in to the financial incentive or price or service difference;
(4) A statement of the consumer's right to withdraw from the financial incentive at any time and how the consumer may exercise that right; and
(5) An explanation of how the financial incentive or price or service difference is reasonably related to the value of the consumer's data, including:
   a. 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
   b. A description of the method the business used to calculate the value of the consumer's data.[5]

26.13A[3] Business Obligations to Provide for and Process Verifiable Consumer Requests to Know or Delete Information

26.13A[3][A] In General

Businesses subject to the CCPA must respond to verifiable consumer requests to know what information about them a business has collected, sold, and used, and/or to delete this information, upon request. The statute and regulations set forth in greater detail what must be provided, how a business must respond, and how a business must verify the identity of the requestor. The requirements for providing notice are addressed separately in section 26.13A[2]. The requirements for requests to know and requests to delete information include some parallel provisions, as well as different requirements. Likewise, as addressed in the following subsections, somewhat different requirements apply when information is sold, as opposed to merely collected or used.

The CPRA, effective January 1, 2023, will expand these obligations to cover information *shared*, rather than merely sold, and encompass circumstances when a business collects personal information, directly *or indirectly, including though or by a service provider or contractor* (and contractors and

[5]Cal. Code Regs. § 999.307(b).

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

third parties will be required to provide assistance to a business in responding to a verifiable consumer request).[1]

The CPRA will also create new consumer rights, and impose corresponding obligations on businesses, to limit use and disclosure of sensitive personal information (including the right to opt-out of secondary use) and correct inaccurate or incomplete personal information, in addition to providing generally broader deletion rights.[2]

26.13A[3[B] Right to the disclosure of the categories and specific pieces of personal information collected—The "Right to Know" In General

The CCPA provides that a "consumer shall have the right to request that a business that collects a consumer's personal

---

[Section 26.13A[3][A]]

[1]*See, e.g.*, Cal. Civ. Code § 1798.130(a)(3)(A) (effective Jan. 1, 2023). The CPRA authorizes the adoption of regulations to require disclosure for a longer period than 12 months, for personal information collected on or after January 1, 2022. *See id.* § 1798.130(a)(2)(B) (effective Jan. 1, 2023).

[2]*See, e.g.*, Cal. Civ. Code §§ 1798.100 (general duties of a business that collects personal information; requiring a business that controls the collection of a consumer's personal information, at or before the point of collection, to inform consumers of the categories of personal information collected or used, and whether the information is sold or shared, setting rules around the collection of sensitive personal information, among other provisions), 1798.105 (consumer right to delete personal information), 1798.106 (creating a new right to correct inaccurate personal information), 1798.110 (right to know and right to access, expanded to cover sharing), 1798.115 (right to know what personal information is sold or shared), 1798.120 (right to opt-out of selling or sharing), 1798.121 (new right to limit use and disclosure of sensitive information) (effective Jan. 1, 2023).

The rights to deletion, correction of inaccurate personal information, and right to know and access what is collected, set forth in sections 1798.105, 1798.106, and 1798.110, will not, however, apply to household data. *See* Cal. Civ. Code § 1798.145(p) (effective Jan. 1, 2023).

The right to deletion also will not apply to student grades, educational scores, or educational test results that a business holds on behalf of a local educational agency at which the student whose records are at issue is currently enrolled. *See id.* § 1798.145(q)(1) (effective Jan. 1, 2023). Likewise, the right to know and access set forth in section 1798.110 does not extend to certain educational assessments. *See id.* § 1798.145(q)(2) (effective Jan. 1, 2023).

Limitations are also placed on a consumer's right to delete or opt out under sections 1798.105 and 1798.120 where consent had been obtained for use in a physical item such as a yearbook. *See id.* § 1798.145(r) (effective Jan. 1, 2023).

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

information disclose to that consumer the categories and specific pieces of personal information the business has collected."[1]

A business must provide consumers "two or more designated methods for submitting" disclosure requests, which must include, "at a minimum, a toll-free telephone number" and, if the business maintains an internet website, the business must make it available to consumers to submit requests.[2] 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.[3]

A business must also ensure that its customer service

[Section 26.13A[3[B]]

[1]Cal. Civ. Code § 1798.100(a).

[2]Cal. Civ. Code § 1798.130(a)(1). Effective January 1, 2023, the CPRA will provide that a business "that operates exclusively online and has a direct relationship with a consumer from whom it collects personal information shall only be required to provide an email address for submitting requests for information required to be disclosed pursuant to Sections 1798.1.10 and 1798.115, or for requests for deletion or correction pursuant to Sections 1798.105 and 1798.106, respectively." Cal. Civ. Code § 1798.130(a)(1)(A) (effective Jan. 1, 2023). However, if the business maintains an internet website, it will also be required to "make the internet website available to consumers to submit requests for information required to be disclosed pursuant to Sections 1798.110 and 1798.115, or requests for deletion or correction pursuant to Sections 1798,105 and 1798.106, respectively." *Id.* § 1798.130(a)(1)(B) (effective Jan. 1, 2023).

[3]Cal. Code Regs. § 999.312(a). This will be codified under the CPRA in new section 1798.130(a)(1)(A), but the CPRA also appears to require that a business that maintains a website "make the internet website available to consumers to submit requests for information required to be disclosed pursuant to Sections 1798.110 and 1798.115, or requests for deletion or correction pursuant to Sections 1798,105 and 1798.106, respectively." *Id.* § 1798.130(a)(1)(B) (effective Jan. 1, 2023). This point will likely be fleshed out in regulations construing the CPRA expected by July 1, 2023.

The final CCPA regulations 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 with which the consumer can call the business's toll-free number." Cal. Code Regs. § 999.312(c).

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

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.[4]

Pursuant to section 1798.110, a consumer has the right to request that a business disclose:

(1) "the categories of personal information it has collected about that consumer"
(2) "the categories of sources[5] 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[6] with whom the business shares personal information" and
(5) "the specific pieces of personal information it has collected about that consumer."[7]

The regulations provide that in responding to a verified

The final CCPA regulations 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).

[4]Cal. Civ. Code § 1798.130(a)(6).

[5]*Categories of sources* means "types or groupings of persons or entities from which a business collects personal information about consumers, described with enough particularity to provide consumers with a meaningful understanding of the type of person or entity." Cal. Code Regs. § 999.301(d). They may include "the consumer directly, advertising networks, internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, and data brokers." *Id.*

[6]*Categories of third parties* means "types or groupings of third parties with whom the business shares personal information, described with enough particularity to provide consumers with a meaningful understanding of the type of third party." Cal. Code Regs. § 999.301(e). They may include "advertising networks, internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, and data brokers." *Id.*

[7]Cal. Civ. Code §§ 1798.110(a)(1) to 1798.110(a)(5). The regulations require a business to provide a response unique to each individual verified request to know the categories of personal information, categories of sources, and/or categories of third parties collected, sold, and used from a specific consumer, except that it may refer the consumer to the businesses' general practices outlined in its privacy policy if "its response would be

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

request to know the categories of personal information, a business shall provide categories 1-4 above *and* (a) the categories of personal information that the business sold in the preceding 12 months, and for each category identified, the categories of third parties to whom it sold that particular category of personal information; and (b) the categories of personal information that the business disclosed for a business purpose in the preceding 12 months, and for each category identified, the categories of third parties to whom it disclosed that particular category of personal information.[8] The regulations thus require that any request to know cover information that is collected, sold, and/or disclosed for a business purpose.[9] Further, the regulations require that the information must be provided "in a manner that provides consumers a meaningful understanding of the categories listed."[10]

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.[11] 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

---

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." 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.

As previously noted, the CPRA will expand these obligations beyond sales to instances where personal information is merely shared.

[8]Cal. Civ. Code §§ 1798.110(a)(1), 1798.130(a)(B), 1798.130(a)(C); Cal. Code Regs. § 999.313(c)(10).

[9]Because the regulations conflate some of the requirements for the right to the disclosure of the categories and specific pieces of information *collected* under Cal. Civ. Code § 1798.110(a) with those for the right to the disclosure of the categories and specific pieces of information sold or *disclosed for a business purpose* under Cal. Civ. Code § 1798.115(a), this subsection should be read in conjunction with section 26.13A[3][C].

[10]Cal. Code Regs. § 999.313(c)(11).

[11]Cal. Civ. Code § 1798.110(d)(1).

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

by the business or [used] to reidentify or otherwise link information that is not maintained in a manner that would be considered personal information."[12] 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*.[13]

The implementing regulations prohibit a business 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, security questions and answers, or unique biometric data generated from measurements or technical analysis of human characteristics . . . ," 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."[14]

As noted below in section 26.13A[3][D], the 12 month lookback period provided for by the CCPA will be expanded by the CPRA (effective January 1, 2023) beyond the 12 month period, upon request of a consumer, for any information collected on or after January 1, 2022, where it is not "impossible" and does not involve a "disproportionate effort" to provide the information, if it has been retained.[15]

---

[12]Cal. Civ. Code § 1798.100(e).

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

[14]Cal. Code Regs. § 999.313(c)(4). *Biometric information* is defined in Cal. Civ. Code § 1798.140(b). The definition of what constitutes biometric information will be expanded somewhat under the CPRA, effective January 1, 2023, in renumbered subsection 1798.140(c).

[15]*See* Cal. Civ. Code § 1798.130(a)(2)(B) (effective Jan. 1, 2023); *infra*

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

26.13A[3][C] Right to the disclosure of the categories of personal information *sold* or *disclosed for a Business Purpose*—In General

In addition to the right to know what categories and specific pieces of information a business has collected about a consumer (as discussed above in section 26.13A[3][B]), 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.[1] *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."[2] The statute further provides that courts examining compliance with its pro-

---

§ 26.13A[3][D].

[Section 26.13A[3][C]]

[1]Cal. Civ. Code § 1798.115(a). What constitutes a *business purpose* is discussed earlier in section 26.13A[1] and is defined in Cal. Civ. Code § 1798.140(d).

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

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

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

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

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

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

(D) The business transfers to a third party the personal information of a consumer as an asset that is part of a merger, acquisition,

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

visions should take a liberal approach to determining whether a transaction is a sale subject to its regulation. The CCPA mandates that, where a series of "steps or transactions" are taken "with the intention of avoiding the reach of this title, including the disclosure of information by a business to a third party in order to avoid the definition of sell, a court shall disregard the intermediate steps or transactions for purposes of effectuating the purposes of this title."[3]

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

---

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). Under the CPRA, subpart (A) provides that a business does not sell personal information when a consumer "uses or directs the business to: (i) intentionally disclose personal information; or (ii) intentionally interact with a one or more third parties . . . ." *Id.* § 1798.140(ad)(2)(A) (effective Jan. 1, 2023). The exception in subpart (B) is expanded to also provide an exception to restrictions on limited use of a consumer's sensitive personal information.*Id.* § 1798.140(ad)(2)(B) (effective Jan. 1, 2023). Subpart (C) is deleted from the CPRA.

[3]Cal. Civ. Code § 1798.190. This provision is expanded under the CPRA, effective January 1, 2023, to apply to both a court or agency and to further require a court or agency to disregard the intermediate steps or transactions for purposes of effectuating the purposes of the CPRA if steps or transactions were taken to purposefully avoid the definition of *sell* or *share* by eliminating any monetary or other valuable consideration, including entering into contracts that do not include an exchange for monetary or other valuable consideration, but where a party is obtaining something of value or use. *See id.* (effective Jan. 1, 2023).

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

third parties[4] 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 business disclosed about the consumer for a business purpose."[5]

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.[6]

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.[7] 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 section 26.13A[1], and may in the future be supplemented by the California Attorney General.[8]

Because the regulations conflate some of the requirements

---

[4]*Categories of third parties* means "types or groupings of third parties with whom the business shares personal information, described with enough particularity to provide consumers with a meaningful understanding of the type of third party." Cal. Code Regs. § 999.301(e). They may include "advertising networks, internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, and data brokers." *Id.*

[5]1 Cal. Civ. Code §§ 1798.115(a)(1)-(3).

[6]2 Cal. Civ. Code § 1798.130(a)(4).

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

[8]*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.

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

for the right to the disclosure of the categories and specific pieces of information *collected* under Cal. Civ. Code § 1798.110(a) with those for the right to the disclosure of the categories and specific pieces of information sold or *disclosed for a business purpose* under Cal. Civ. Code § 1798.115(a), this subsection should be read in conjunction with section 26.13A[3][B].

26.13A[3][D] Responding to Requests to Know

In responding to a request to know,[1] a business is not required to search for personal information if all of the fol-

---

(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.

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

[Section 26.13A[3][D]]

[1]*Request to know* means "a consumer request that a business disclose personal information that it has collected about the consumer pursuant to Civil Code sections 1798.100, 1798.110, or 1798.115." Cal. Code Regs. § 999.301(r). It includes a request for any or all of the following:

(1) Specific pieces of personal information that a business has collected about the consumer;

(2) Categories of personal information it has collected about the consumer;

(3) Categories of sources from which the personal information is collected;

(4) Categories of personal information that the business sold or disclosed for a business purpose about the consumer;

(5) Categories of third parties to whom the personal information was sold or disclosed for a business purpose; and

(6) The business or commercial purpose for collecting or selling personal information.

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

lowing conditions are met:

a. The business does not maintain the personal information in a searchable or reasonably accessible format;
b. The business maintains the personal information solely for legal or compliance purposes;
c. The business does not sell the personal information and does not use it for any commercial purpose; and
d. The business describes to the consumer the categories of records that may contain personal information that it did not search because it meets the conditions stated above.[2]

If a business denies a consumer's verified request to know specific pieces of personal information, in whole or in part, because of a conflict with federal or state law, or an exception to the CCPA, the business shall inform the requestor and explain the basis for the denial, unless prohibited from doing so by law. If the request is denied only in part, the business shall disclose the other information sought by the consumer.[3]

In transmitting personal information to a consumer, a business must use reasonable security measures.[4] If a business maintains a password-protected account with the consumer, it may comply with a request to know by using a secure self-service portal for consumers to access, view, and receive a portable copy of their personal information if the portal fully discloses the personal information that the consumer is entitled to under the CCPA and implementing regulations, uses reasonable data security controls, and complies with the verification requirements set forth in Article 4 of the regulations (sections 999.323 to 999.326).[5]

As noted above in section 26.13A[3][B], the CCPA generally provides consumers with a right to request information on the preceding twelve months, but the CPRA will extend that beyond twelve months, effective January 1, 2023, for information collected on or after January 1, 2022, if providing information over a longer period would not be "impossible" or involve a "disproportionate effort," and if requested by a

---

Id.

[2]Cal. Code Regs. § 999.313(c)(3).

[3]Cal. Code Regs. § 999.313(c)(5).

[4]Cal. Code Regs. § 999.313(c)(6).

[5]Cal. Code Regs. § 999.313(c)(7); *see generally infra* § 16.13A[5].

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

consumer.[6] The CPRA, however, does not require a business to keep personal information for any specific period of time.[7]

26.13A[4] Right to the deletion of personal information

The CCPA affords a consumer "the right to request that a business delete any personal information about the consumer which the business has collected from the consumer."[1]

A business generally must provide two or more designated methods for submitting requests to delete, one of which must be a toll-free phone number.[2] Other acceptable methods for submitting these requests include, but are not limited to, a link or form available online through a business's website, a designated email address, a form submitted in person, and a form submitted through the mail.[3]

A business that operates exclusively online and has a direct relationship with a consumer from whom it collects personal information, however, need only provide an email address for submitting requests to know.[4]

In evaluating which methods to provide for submitting requests to know and requests to delete, a business must

---

[6]Cal. Civ. Code § 1798.130(a)(2)(B) (effective Jan. 1, 2023) (providing in part that "[t]he disclosure of the required information shall cover the 12 month period preceding the business's receipt of the verifiable consumer request, provided that, upon the adoption of a regulation pursuant to paragraph (9) of subdivision (a) of Section 1798.185, a consumer may request that the business disclose the required information beyond the 12 month period and the business shall be required to provide such information unless doing so proves impossible or would involve a disproportionate effort. A consumer's right to request required information beyond the 12?month period, and a business's obligation to provide such information, shall only apply to personal information collected on or after January 1, 2022.").

[7]Cal. Civ. Code § 1798.130(a)(2)(B) (effective Jan. 1, 2023) ("Nothing in this subparagraph shall require a business to keep personal information for any length of time.").

[Section 26.13A[4]]

[1]Cal. Civ. Code § 1798.105(a).

[2]Cal. Code Regs. §§ 999.312(a), 999.312(b). *Request to delete* means "a consumer request that a business delete personal information about the consumer that the business has collected from the consumer, pursuant to Civil Code section 1798.105." Cal. Code Regs. § 999.301(q).

[3]Cal. Code Regs. §§ 999.312(a), 999.312(b).

[4]Cal. Code Regs. § 999.312(a).

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

"consider the methods by which it primarily interacts with consumers . . . ."[5]

For online deletion requests, a business may use a two-step process where a consumer must first submit the request and then separately confirm that they want their personal information deleted.[6]

If a consumer submits a request in a manner that is not one of the designated methods of

submission, or is deficient in some manner unrelated to the verification process, the business must either: (1) Treat the request as if it had been submitted in accordance with the business's designated manner, or (2) Provide the consumer with information on how to submit the request or remedy any deficiencies with the request, if applicable.[7]

In responding to a request to delete, a business may present the consumer with the choice to delete select portions of their personal information only if a global option to delete all personal information is also offered and more prominently presented than the other choices.[8]

When a business receives a "verifiable consumer request[9] 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.[10]

---

[5]Cal. Code Regs. § 999.312(c). The regulations further provide that if a business "interacts with consumers in person, the business shall consider providing an in-person method such as a printed form the consumer can directly submit or send by mail, a tablet or computer portal that allows the consumer to complete and submit an online form, or a telephone with which the consumer can call the business's toll-free number." *Id.*

[6]Cal. Code Regs. § 999.312(d).

[7]Cal. Code Regs. § 999.312(e).

[8]Cal. Code Regs. § 999.313(d)(8).

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

[10]Cal. Civ. Code § 1798.105(c). A *service provider,* as discussed earlier in this section 26.13A, 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). Likewise, a business that provides services to a person or organization that is not a business, and that would otherwise

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

To comply with a consumer's verified request to delete their personal information, a business must:

a. Permanently and completely erase the personal information on its existing systems with the exception of archived or back-up systems;
b. Deidentify the personal information; or
c. Aggregate the consumer information.[11]

If a business stores any personal information on archived or backup systems, it may delay compliance with a consumer's request to delete, with respect to data stored on the archived or backup system, until the archived or backup system relating to that data is restored to an active system or next accessed or used for a sale, disclosure, or commercial purpose.[12]

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

---

meet the requirements and obligations of a "service provider" under the CCPA and these regulations, shall be deemed a service provider for purposes of the CCPA and these regulations. Cal. Code Regs. § 999.314(a). To the extent that a business directs a second entity to collect personal information directly from a consumer, or about a consumer, on the first business's behalf, and the second entity would otherwise meet the requirements and obligations of a "service provider" under the CCPA and these regulations, the second entity shall be deemed a service provider of the first business for purposes of the CCPA and these regulations. *Id.* § 999.314(b).

The definition of *service provider* includes the requirement that a business subject to the CCPA specify in a written contract that the service 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).

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

[11]*See* Cal. Code Regs. § 999.313(d)(2).

[12]Cal. Code Regs. § 999.313(d)(3).

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

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.[13] 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."[14] A business may also retain consumer information for the purpose of detecting "security incidents," protecting against or prosecuting malicious and fraudulent activity,[15] debugging,[16] and to comply with the California Electronic Communications Privacy Act, Cal. Penal Code § 1546 or another "legal obligation."[17] 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."[18] Presumably, this is intended to allow an interactive computer service provider discretion to decline takedown requests directed at consumer review sites or other online

---

[13]Cal. Civ. Code § 1798.105(d)(1).

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

[15]Cal. Civ. Code § 1798.105(d)(2).

[16]Cal. Civ. Code § 1798.105(d)(3).

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

[18]Cal. Civ. Code §§ 1798.105(d)(4), 1798.105(d)(6). *Research* is 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). Specifically, *research* is defined under the CCPA to mean

> scientific, systematic study and observation, including basic research or applied research that is in the public interest and that adheres to all other applicable ethics and privacy laws or studies conducted in the public interest in the area of public health. Research with personal information that may have been collected from a consumer in the course of the consumer's interactions with a business's service or device for other purposes shall be:
>
> (1) Compatible with the business purpose for which the personal information was collected.
>
> (2) Subsequently pseudonymized and deidentified, or deidentified and in the aggregate, such that the information cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer.
>
> (3) Made subject to technical safeguards that prohibit reidentification of the consumer to whom the information may pertain.

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

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.

Ultimately, a business must inform the consumer whether or not it has complied with the consumer's deletion request.[19]

If the business complies with the consumer's request, it must inform the consumer that it will maintain a record of the request as required by section 999.317(b),[20] which provides that a business must maintain records of consumer requests made pursuant to the CCPA and how it responded to the requests for at least 24 months (and must implement and maintain reasonable security procedures and practices in maintaining these records).[21] A business may retain a record of the request for the purpose of ensuring that the consumer's personal information remains deleted from the business's records.[22]

Where a business denies a consumer's deletion request, it must:

a. Inform the consumer that it will not comply with the consumer's request and describe the basis for the denial, including any conflict with federal or state law, or exception to the CCPA, unless prohibited from doing so by law;
b. Delete the consumer's personal information that is not subject to the exception; and

---

(4) Subject to business processes that specifically prohibit reidentification of the information.
(5) Made subject to business processes to prevent inadvertent release of deidentified information.
(6) Protected from any reidentification attempts.
(7) Used solely for research purposes that are compatible with the context in which the personal information was collected.
(8) Not be used for any commercial purpose.
(9) Subjected by the business conducting the research to additional security controls that limit access to the research data to only those individuals in a business as are necessary to carry out the research purpose.

Id. The restriction on research for commercial purposes is removed, and other aspects of the definition modified in a limited number of respected under the CPRA. *See id.* § 1798.140(ab) (effective Jan. 1, 2023).

[19]Cal. Code Regs. § 999.313(d)(4).

[20]Cal. Code Regs. § 999.313(d)(5).

[21]Cal. Code Regs. § 999.317(b).

[22]Cal. Code Regs. § 999.313(d)(5).

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

c. Not use the consumer's personal information retained for any other purpose than provided for by that exception.[23]

If a business that denies a consumer's deletion request sells personal information and the consumer has not already made a request to opt-out, the business must ask the consumer if they would like to opt-out of the sale of their personal information (and include either the contents of, or a link to, the notice of right to opt-out in accordance with section 999.306).[24]

26.13A[5] Verification and Confirmation of Informational and Deletion Requests

26.13A[5][A] Verification—In General

A business is required to verify the identity of a person making a consumer request for information, or a deletion request, to ensure that personal information is not improperly provided to those who are not entitled to receive it or that account records are improperly deleted. Rules governing verification of requests—to prevent third parties from gaining access to personal information by impersonating others –are set forth in Article 4 of the Attorney General's final regulations.[1]

The statute provides that a business may only provide informational disclosures "upon receipt of a verifiable consumer request."[1] 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 (and, effective January 1, 2023, by a person who has power of attorney or acting as a conservator for the consumer[2]), "that the business can reasonably verify" pursuant

---

[23]Cal. Code Regs. § 999.313(d)(6).

[24]Cal. Code Regs. § 999.313(d)(7).

[Section 26.13A[5][A]]

[1]*See* Cal. Code Regs. §§ 999.323 to 999.326.

[1]Cal. Civ. Code §§ 1798.100(c), 1798.130(a)(2). Under the regulations, *verify* means "to determine that the consumer making a request to know or request to delete is the consumer about whom the business has collected information, or if that consumer is less than 13 years of age, the consumer's parent or legal guardian." Cal. Code Regs. § 999.301(x).

[2]Cal. Civ. Code § 1798.140(ak) (effective Jan. 1, 2023).

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

to the Attorney General's regulations.[2] A business is not required to produce personal information if it cannot verify the identity of the requesting party.[3]

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."[4] Regulations implementing the CCPA further 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.[5]

A business cannot require a consumer to create an account

---

[2]Cal. Civ. Code § 1798.140(y). Under the CPRA, "reasonably verify" will be changed to "verify, using commercially reasonable methods, . . ." and will be further subject to regulations promulgated by the Attorney General. *See* Cal. Civ. Code § 1798.140(ak) (effective Jan. 1, 2023).

[3]Cal. Civ. Code § 1798.140(y).

[4]Cal. Civ. Code § 1798.130(a)(2).

[5]Cal. Code Regs. § 999.308(c)(1)(c). The regulations allow a business to require the consumer to provide signed permission, verify their own identity directly with the business, or directly confirm with the business that they provided the authorized agent permission to submit the request, before acting pursuant to a request submitted by an authorized agent, unless the agent has power of attorney pursuant to the Probate Code. *Id.* §§ 999.326(a), 999.326(b). A business may deny a request for deletion from an authorized agent if the agent cannot provide to the business the consumer's signed permission demonstrating that they have been authorized by the consumer to act on the consumer's behalf. *Id.* § 999.315(f).

The regulations provide that an authorized agent may be a natural person or a business entity registered with the Secretary of State to conduct business in California that a consumer has authorized to act on their behalf subject to the requirements of section 999.326. *See id.* Proposed text of Cal. Code Regs. § 999.301(c).

The regulations also address how to handle a consumer request submitted ostensibly on behalf of a *household*, which are addressed later in this section.

If the household includes a consumer under the age of 13, a business must obtain verifiable parental consent before complying with a request to know about or delete the minor's personal information pursuant to the regulations. *Id.* § 999.318(c); *see generally infra* § 26.13A[8] (minors).

The Attorney General's March 15, 2021 amendments modified section 999.326 to allow a business to require an authorized agent to provide proof that a consumer gave the agent signed permission to submit a request to know or request to delete on the consumer's behalf, and/or require the consumer to either verify their own identity directly with the business or directly confirm with the business that they provided the au-

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

(or, under the CPRA, effective January 1, 2023, provide additional information beyond what is necessary[3]) in order to submit a verifiable consumer request, but if a consumer has an account with the business, "the business may require the consumer to submit the request through that account."[6] In the case of non-account holders (who nonetheless have rights under the CCPA), the regulations allow a business to verify a consumer request by matching data points provided by the consumer with data points maintained by the business.[7]

The regulations require a business to establish, document, and comply with a reasonable method for verifying that the person making a request to know or a request to delete is the consumer about whom the business has collected information[4] (or is acting through an authorized agent[5] or someone with power of attorney[6]). In determining the method by which the business will verify the consumer's identity, a business shall, (1) whenever feasible, match the identifying

---

thorized agent permission to submit the request. *See* Cal. Code Regs. § 999.326(a).

[3]*See* Cal. Civ. Code § 1798.135(c) (effective Jan. 1, 2023). This provision implements the concept of data minimization addressed throughout chapters 26 (data privacy) and 27 (cybersecurity).

[6]Cal. Civ. Code § 1798.130(a)(2); *see also* Cal. Code Regs. § 999.313(c)(7) (portal).

[7]Cal. Code Regs. §§ 999.325(b), 999.325(c), 999.325(d). As discussed at greater length later in this subsection 26.13[A][5], the regulations 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).

[4]Cal. Code Regs. § 999.323(a).

[5]*See* Cal. Code Regs. § 999.326. An *authorized agent* is "a natural person or a business entity registered with the Secretary of State to conduct business in California that a consumer has authorized to act on their behalf subject to the requirements set forth in section 999.326." *Id.* § 999.301(c). When a consumer uses an authorized agent to submit a request to know or a request to delete, a business may require the authorized agent to provide proof that the consumer gave the agent signed permission to submit the request. *Id.* § 999.326(a). The business may also require the consumer to either: (1) Verify their own identity directly with the business; or (2) Directly confirm with the business that they provided the authorized agent permission to submit the request. *Id*. An authorized agent shall not use a consumer's personal information, or any information collected from or about the consumer, for any purposes other than to fulfill the consumer's requests, verification, or fraud prevention. *Id.* § 999.326(d).

[6]Cal. Code Regs. § 999.326(b).

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

information provided by the consumer to the personal information of the consumer already maintained by the business, or use a third-party identity verification service;[7] (2) avoid collecting the types of personal information identified in Cal. Civil Code § 1798.81.5(d),[8] "unless necessary for the purpose of verifying the consumer"; and (3) consider the following factors:

a. The type, sensitivity, and value of the personal information collected and maintained about the consumer;[9]

---

[7]*Third-party identity verification service* means "a security process offered by an independent third party that verifies the identity of the consumer making a request to the business." Cal. Code Regs. § 999.301(v). Third-party identity verification services are subject to the requirements set forth in Article 4 of the regulations (sections 999.323 to 999.326) regarding requests to know and requests to delete. *See id.*

[8]That section identifies *personal information* as:

(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.
  (vii) Genetic data.

(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. Civil Code § 1798.81.5(d).

[9]The regulations state that "[s]ensitive or valuable personal information" warrants a more stringent verification process and clarify that the types of personal information identified in Cal. Civil Code § 1798.81.5(d) are considered "presumptively sensitive." Cal. Code Regs. § 999.323(b)(3)(a).

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

b. The risk of harm to the consumer posed by any unauthorized access or deletion;[10]
c. The likelihood that fraudulent or malicious actors would seek the personal information;[11]
d. Whether the personal information to be provided by the consumer to verify their identity is sufficiently robust to protect against fraudulent requests or being spoofed or fabricated;
e. The manner in which the business interacts with the consumer; and
f. Available technology for verification.[12]

A business must confirm receipt of a request to know or request to delete within 10 business days of receiving the request.[13] The information provided must describe in general the business's verification process and when the consumer should expect a response, except in instances where the business has already granted or denied the request.[14] The confirmation may be given in the same manner in which the request was received. For example, if the request is made over the phone, the confirmation may be given orally during the phone call.[15]

In general, businesses are directed to avoid requesting additional information. If, however, the business cannot verify the identity of a consumer from the information already maintained by the business, the business may request additional information used for the purposes of verifying the identity of the consumer seeking to exercise their rights under the CCPA, security, or fraud-prevention.[16]

A business may not cause consumers to incur fees to

---

[10]The regulations provide that a more stringent verification process is required where there is a greater risk of harm to the consumer by unauthorized access or deletion. *See* Cal. Code Regs. § 999.323(b)(3)(b).

[11]The regulations state that a more stringent the verification process is required where there is a higher likelihood that fraudulent or malicious actors would seek the personal information. *See* Cal. Code Regs. § 999.323(b)(3)(c).

[12]Cal. Code Regs. § 999.323(b).

[13]Cal. Code Regs. § 999.313(a).

[14]Cal. Code Regs. § 999.313(a).

[15]Cal. Code Regs. § 999.313(a).

[16]Cal. Code Regs. § 999.323(c). The regulation further provides that in such case, the business must "delete any new personal information collected for the purposes of verification as soon as practical after processing

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

provide verification. They cannot charge or require a consumer to pay a fee. And if they require consumers to incur fees to verify their identity—such as by providing a notarized affidavit—they must compensate consumers for those costs.[17]

A business also must implement reasonable security measures to detect fraudulent identity-verification activity and prevent the unauthorized access to or deletion of a consumer's personal information.[18]

Importantly, a business is not obligated to provide or delete information about deidentified information in response to a consumer request or to re-identify individual data to verify a consumer request.[19]

26.13A[5][B] Verification—for Password-Protected Accounts

Provided it follows the general requirements (as set forth in section 999.323), a business that maintains a password-protected account with a consumer may verify the consumer's identity through its existing authentication practices for the account (as long as it also requires the consumer to re-authenticate themselves before disclosing or deleting the consumer's data).[1] A business may not comply with a consumer's request to know or request to delete, however, if it suspects "fraudulent or malicious activity on or from the password-protected account," until further verification procedures determine that the consumer request is authentic and the consumer making the request is the person about whom the business has collected information.[2]

---

the consumer's request, except as required to comply with section 999.317." *Id.* Section 999.317 addresses training and record-keeping.

[17]*See* Cal. Code Regs. § 999.323(d).

[18]Cal. Code Regs. § 999.323(e).

[19]*See* Cal. Code Regs. § 999.323(f).

[Section 26.13A[5][B]]

[1]*See* Cal. Code Regs. § 999.324(a).

[2]Cal. Code Regs. § 999.324(b). To do so, the regulations provide that a business "may"—but presumably is not required to—"use the procedures set forth in section 999.325 to further verify the identity of the consumer." *Id.* Section 999.325 addresses verification for non-accountholders.

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

26.13A[5][C] Verification Where There Is No Password-Protected Account or it Can't Be Accessed

Where a business receives a verification request from someone who does not have or cannot access a password-protected account with the business, the business must further verify the identity of the consumer making the request to a reasonable degree of certainty (for a request to know *categories* of personal information)[1] and a reasonably high degree of certainty (for a request to know specific pieces of personal information).[2] A *reasonable degree of certainty* may include matching at least two data points provided by the consumer with data points maintained by the business that it has determined to be reliable for the purpose of verifying the consumer."[3] A *reasonably high degree of certainty* may include matching at least three pieces of personal information provided by the consumer with personal information maintained by the business that it has determined to be reliable for the purpose of verifying the consumer together with a signed[4] declaration under penalty of perjury that the requestor is the consumer whose personal information is the

---

[Section 26.13A[5][C]]

[1]Cal. Code Regs. § 999.325(b).

[2]Cal. Code Regs. § 999.325(c).

[3]Cal. Code Regs. § 999.325(b). As an illustration, if a business maintains personal information in a manner associated with a named actual person, the business may verify the consumer by requiring the consumer to provide evidence that matches the personal information maintained by the business. For example, if a retailer maintains a record of purchases made by a consumer, the business may require the consumer to identify items that they recently purchased from the store or the dollar amount of their most recent purchase to verify their identity to a reasonable degree of certainty. *Id.* § 999.325(e)(1).

By contrast, if a business maintains personal information in a manner that is not associated with a named actual person, the business may verify the consumer by requiring the consumer to demonstrate that they are the sole consumer associated with the personal information. For example, a business that offers a mobile app that collects personal information about the consumer, but does not require an account, may determine "whether, based on the facts and considering the factors set forth in" section 999.323(b)(3), it may reasonably verify a consumer by asking them to provide information that only the person who used the mobile app would know or by requiring the consumer to respond to a notification sent to their device. *Id.* § 999.325(e)(2).

[4]*Signed* means "that the written attestation, declaration, or permission has either been physically signed or provided electronically in accor-

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

subject of the request.[5]

For deletion requests, in contrast to requests for information, whether verification is required to a reasonable degree of certainty or reasonably high degree of certainty for someone who does not have or cannot access a password-protected account with the business depends on the sensitivity of the personal information and the risk of harm to the consumer posed by unauthorized deletion.[6] A business is required to act in good faith when determining the appropriate standard to apply.[7]

26.13A[5][D] If A Business is Unable to Verify a Request

Where a business cannot verify the identity of the requester pursuant to CCPA regulations, it must deny a request to know specific pieces of personal information.[1] If the request is denied in whole or part, the business must treat the request as one seeking the disclosure of categories of personal information about the consumer pursuant to section 999.313(c)(2), and further evaluate it on that basis.[2]

For requests that seek the disclosure of categories of personal information about the consumer, if a business cannot verify the identity of the person making the request, the business *may* deny the request to disclose the categories and other information requested, but is not required to do so. If the request is denied in whole or in part, however, the business must provide or direct the consumer to its general business practices regarding the collection, maintenance, and

---

dance with the Uniform Electronic Transactions Act, Civil Code section 1633.1 *et seq.*" Cal. Code Regs. § 999.301(u).

[5]Cal. Code Regs. § 999.325(c). If a business uses this method for verification, the business shall maintain all signed declarations as part of its record-keeping obligations. *Id.*

[6]Cal. Code Regs. § 999.325(d). For example, the deletion of family photographs may require a reasonably high degree of certainty, while the deletion of browsing history may require only a reasonable degree of certainty. *Id.*

[7]*See* Cal. Code Regs. § 999.325(d).

[Section 26.13A[5][D]]

[1]Cal. Code Regs. §§ 999.313(c)(1), 999.325(f).

[2]Cal. Code Regs. § 999.313(c)(1).

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

sale of personal information set forth in its privacy policy.[3]

If there is no reasonable method by which a business can verify the identity of a consumer to the required degree of certainty, it must state so in response to any request and explain why it has no reasonable method by which it can verify the identity of the requestor.[4]

If a business has no reasonable method by which it can verify a consumer, the business must explain why it has no reasonable verification method in its privacy policy.[5] It must also evaluate and document whether a reasonable method can be established at least once every 12 months, in connection with the requirement to update its privacy policy (as set forth in Cal. Civil Code § 1798.130(a)(5)).[6]

26.13A[6] Requests to Know or Delete Household Information

Where a household does not have a password-protected account with a business, a business may not comply with a request to know specific pieces of personal information about the household or a request to delete household personal information unless all of the following conditions are satisfied:

(1) All consumers of the household jointly request to know specific pieces of information for the household or the deletion of household personal information;
(2) The business individually verifies all the members of the household subject to the verification requirements set forth in section 999.325; and
(3) The business verifies that each member making the request is currently a member of the household.[1]

Where a consumer has a password-protected account with a business that collects personal information about a household, the business may process requests to know and requests to delete relating to household information through the business's existing business practices and in compliance

---

[3]Cal. Code Regs. § 999.313(c)(2).

[4]Cal. Code Regs. § 999.325(g).

[5]Cal. Code Regs. § 999.325(g).

[6]Cal. Code Regs. § 999.325(g).

[Section 26.13A[6]]

[1]*See* Cal. Code Regs. § 999.318(a).

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

with these regulations.[2]

If a member of a household is a consumer under the age of 13, a business must obtain verifiable parental consent before complying with a request to know specific pieces of information for the household or the deletion of household personal information pursuant to the parental consent provisions set forth in section 999.330.[3]

26.13A[7] The Timing for Responding to Requests to Know or Delete Information, and the Format and Permissible Charges for Disclosures

The CCPA's implementing regulations require a business to confirm requests to know and requests to delete within ten (10) business days of receipt and provide information on how the business will process the request, describing in general the businesses' verification process and when the consumer should expect a response (except in instances where the business has already granted or denied the request).[1] The confirmation may be given in the same manner in which the request was received.[2]

A business is required to disclose the information requested (or otherwise respond to the information or deletion request) within 45 days of the day the business receives a verifiable consumer request from a consumer.[3] If the business cannot verify the identity of the consumer within the 45 day time period, it may deny the request.[4] If necessary, the business may extend the 45 day time period to respond once, by an additional 45 days (for a total of 90 days from the date of receipt), provided the business gives notice to the requester with an explanation for the delay.[5] The statute actually provides that a business may take up to "90 ad-

---

[2]*See* Cal. Code Regs. § 999.318(b).

[3]*See* Cal. Code Regs. § 999.318(c); *see generally infra* § 26.13A[8] (addressing verifiable parental consent).

[Section 26.13A[7]]

[1]Cal. Code Regs. § 999.313(a).

[2]Cal. Code Regs. § 999.313(a).

[3]Cal. Civ. Code § 1798.130(a)(2); Cal. Code Regs. § 999.313(b). Under the CPRA, this timeline will also apply to requests for correction. *See* Cal. Civ. Code § 1798.130(2)(A) (effective Jan. 1, 2023).

[4]Cal. Code Regs. § 999.313(b).

[5]Cal. Civ. Code §§ 1798.130(a)(2), 1798.145(i)(1); Cal. Code Regs.

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

ditional days where necessary, taking into account the complexity and number of the requests" to respond,[6] but the regulations only allow 45 additional days (or 90 in total). Given that the regulations were promulgated by the Office of the Attorney General, which also has responsibility for enforcing violations of this part of the CCPA, the more prudent approach would be to adhere to the terms of the regulations, not the statute.

A business is not required, however, to provide personal information requested to a consumer more than twice in a 12-month period.[7]

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.[8] The disclosure "shall cover the 12-month period preceding the business's receipt of the verifiable consumer request."[9] 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.[10] 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.[11]

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

---

§ 999.313(b)..

[6]Cal. Civ. Code § 1798.145(i)(1).

[7]Cal. Civ. Code § 1798.100(d).

[8]Cal. Civ. Code § 1798.100(d); Cal. Civ. Code § 1798.145(i)(3).

[9]Cal. Civ. Code § 1798.130(a)(2). Unless otherwise specified by the business to cover a longer period of time, the 12- month period covered by a consumer's verifiable request to know referenced in section 1798.130(a)(2) runs from the date the business receives the request, regardless of the time required to verify the request. *See* Cal. Code Regs. § 999.313(c)(8).

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

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

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

business."[12]

The timing of opt-out requests, as analyzed in section 26.13A[8], is subject to an outside timeline of fifteen business days.[13]

26.13A[8] Business obligations in implementing consumers' right to opt-out of the sale of personal information and minors' right to opt-in

The CCPA gives California residents a right to *opt-out* of having their information sold, and requires affirmative *opt-in* consent from consumers who are younger than 16 years old. Procedures for obtaining consent on behalf of minors younger than 16 years old are addressed in section 26.13A[9].

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."[1] The regulations further require that a business provide two or more designated methods for submitting requests to opt-out,[2] including an interactive form accessible via a clear and conspicuous link titled "Do Not Sell My Personal Information," on the business's website or mobile application.[3] Other acceptable methods for submitting these requests include, but are not limited to, a toll-free phone number, a designated email address, a form submitted in person, a form submitted through the mail, and user-enabled global privacy controls, such as a browser plug-in or privacy setting, device setting, or other mechanism, that communicate or signal the consumer's choice to opt-out of the sale of their personal information.[4]

A business is required, by regulation, to consider the

---

[12]Cal. Civ. Code § 1798.145(i)(2).

[13]*See* Cal. Code Regs. § 999.315(e); *see generally supra* § 26.13A[8].

[Section 26.13A[8]]

[1]Cal. Civ. Code § 1798.120(a).

[2]*Request to opt-out* means "a consumer request that a business not sell the consumer's personal information to third parties, pursuant to Civil Code section 1798.120, subdivision (a)." Cal. Code Regs. § 999.301(t).

[3]Cal. Code Regs. § 999.315(a).

[4]Cal. Code Regs. § 999.315(a). In January 2021, California's Attorney General tweeted about the use of a new Global Privacy Control (GPC) standard, informing California consumers that on certain browsers they

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

methods by which it interacts with consumers, the manner in which the business sells personal information to third parties, available technology, and ease of use by the consumer when determining which methods consumers may use to submit requests to opt-out.[5] At least one method offered must reflect the manner in which the business primarily interacts with the consumer.[6]

The Attorney General's March 15, 2021 amended final regulations added new section 999.315(h), requiring that a business's methods for submitting opt-out requests be "easy for consumers to execute and shall require minimal steps to allow a consumer to opt-out."[7]

---

could use GPC as a "stop selling my data switch" to exercise their right to opt out of the sale of their personal information in one step—rather than on a site-by-site basis. *See* Tweet, Xavier Becerra, Jan. 28, 2021, *available at* https://twitter.com/agbecerra/status/1354850758236102656?lang=en; Global Privacy Control, https://globalprivacycontrol.org/; *see also* Gretchen A. Ramos & Darren J. Abernethy, "Global Privacy Control Endorsed by California AG—Next Steps," Greenberg Traurig LLP Alert (Feb. 22, 2021), *available at* https://www.gtlaw.com/en/insights/2021/2/global-privacy-control-endorsed-by-california-ag-next-steps.

[5]Cal. Code Regs. § 999.315(b).

[6]Cal. Code Regs. § 999.315(b).

[7]Cal. Code Regs. § 999.315(h). That section provides that:

> (h) A business's methods for submitting requests to opt-out shall be easy for consumers to execute and shall require minimal steps to allow the consumer to opt-out. A business shall not use a method that is designed with the purpose or has the substantial effect of subverting or impairing a consumer's choice to opt-out. Illustrative examples follow:
>
> (1) The business's process for submitting a request to opt-out shall not require more steps than that business's process for a consumer to opt-in to the sale of personal information after having previously opted out. The number of steps for submitting a request to opt-out is measured from when the consumer clicks on the "Do Not Sell My Personal Information" link to completion of the request. The number of steps for submitting a request to opt-in to the sale of personal information is measured from the first indication by the consumer to the business of their interest to opt-in to completion of the request.
>
> (2) A business shall not use confusing language, such as double-negatives (e.g., "Don't Not Sell My Personal Information"), when providing consumers the choice to opt-out.
>
> (3) Except as permitted by these regulations, a business shall not require consumers to click through or listen to reasons why they should not submit a request to opt-out before confirming their request.

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

A consumer may make a request directly, or through an authorized agent.[8] Requests need not be a verifiable consumer request, but if a business has a "good-faith, reasonable, and documented belief that a request to opt-out is fraudulent," it may—but is not required to—deny the request, provided it informs the requester that it will not comply with the request and provides an explanation of why it believes the request is fraudulent.[9]

A business is required to notify California residents of their right to opt-out if it sells consumers' personal information. 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."[10] A business, however, may avoid placing the required text and link on "the homepage that the business makes available to the public generally, . . ." if it maintains a "separate and additional" homepage for California consumers that includes the required text and link and if the business "takes reasonable steps to ensure that California consumers are directed" to that homepage and "not the

---

(4) The business's process for submitting a request to opt-out shall not require the consumer to provide personal information that is not necessary to implement the request.

(4) Upon clicking the "Do Not Sell My Personal Information" link, the business shall not require the consumer to search or scroll through the text of a privacy policy or similar document or webpage to locate the mechanism for submitting a request to opt-out.

Id.

[8]A consumer may use an authorized agent to submit a request to opt-out on the consumer's behalf if the consumer provides the authorized agent written permission signed by the consumer. Cal. Code Regs. § 999.315(f). A business may deny a request from an authorized agent if the agent cannot provide to the business the consumer's signed permission demonstrating that they have been authorized by the consumer to act on the consumer's behalf. *Id.*

The regulations provide that "[u]ser-enabled global privacy controls, such as a browser plug-in or privacy setting, device setting, or other mechanism, that communicate or signal the consumer's choice to opt-out of the sale of their personal information shall be considered a request directly from the consumer, not through an authorized agent." *Id.*

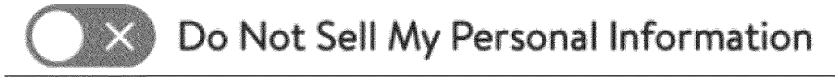
[9]Cal. Code Regs. § 999.315(g).

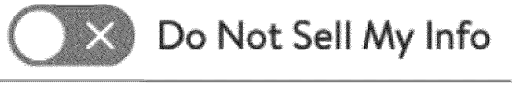
[10]Cal. Civ. Code § 1798.135(a)(1).

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

homepage made available to the public generally."[11]

The Attorney General's February 2020 draft regulations would have required 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 appeared as follows:





[11]Cal. Civ. Code § 1798.135(b).

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

Ultimately, however, use of this graphic was not required and the final regulations removed reference to the shorthand "Do Not Sell My Info."

A business cannot require a consumer to create an account in order to opt-out.[12] It may, however, present consumers with the choice to opt-out of sales for certain uses of personal information, but not others, in response to an opt-out request, as long as a global option to opt-out of the sale of all personal information is more prominently presented than the other choices.[13]

When an opt-out request is received, a business must comply with a request to opt-out "as soon as feasibly possible, but no later than 15 business days from the date the business receives the request."[14] If a business sells a consumer's personal information to any third parties after the consumer submits their request but before the business complies with that request, it must notify those third parties that the consumer has exercised their right to opt-out and direct them not to sell that consumer's information.[15]

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.[16] The regulations more broadly require that all individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance with the CCPA "be informed of all of the requirements in the CCPA and these regulations and how to direct consumers to exercise their rights under the CCPA and these regulations."[17]

A business must also maintain records of consumer requests made pursuant to the CCPA, and how it responded to those requests, for at least 24 months.[18] Maintaining these records will not be deemed a violation of the CCPA where

---

[12]Cal. Civ. Code § 1798.135(a)(1).

[13]Cal. Code Regs. § 999.315(d).

[14]Cal. Code Regs. § 999.315(e).

[15]Cal. Code Regs. § 999.315(e).

[16]Cal. Civ. Code § 1798.135(a)(3).

[17]Cal. Code Regs. § 999.317(a).

[18]Cal. Code Regs. § 999.317(b). The records may be maintained "in a ticket or log format provided that the ticket or log includes the date of request, nature of request, manner in which the request was made, the

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

the information is not used for any other purpose.[19] Conversely, information maintained for record-keeping purposes may not be used for any other purpose "except as reasonably necessary for the business to review and modify its processes for compliance with the CCPA" and the CCPA's implementing regulations, and may not be shared with any third party "except as necessary to comply with a legal obligation."[20]

Additional recordkeeping requirements are imposed on businesses that process large volumes of consumer information. Specifically, a business "that knows or reasonably should know that it, alone or in combination, 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" must compile metrics on the number of requests for information, requests to delete information, and requests to opt-out of sales, for the prior calendar year, and disclosure these metrics in its Privacy Policy or on its website, by July 1 of every calendar year.[21] It must also "[e]stablish, document, and comply with a training policy to ensure that all individu-

---

date of the business's response, the nature of the response, and the basis for the denial of the request if the request is denied in whole or in part." *Id.* § 999.317(c).

[19]Cal. Code Regs. § 999.317(d).

[20]Cal. Code Regs. § 999.317(e).

[21]*See* Cal. Code Regs. § 999.317(g). Section 999.317(g) provides that a business that knows or reasonably should know that it, alone or in combination, 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 must:

(1) Compile the following metrics for the previous calendar year:
   a. The number of requests to know that the business received, complied with in whole or in part, and denied;
   b. The number of requests to delete that the business received, complied with in whole or in part, and denied;
   c. The number of requests to opt-out that the business received, complied with in whole or in part, and denied; and d. The median or mean number of days within which the business substantively responded to requests to know, requests to delete, and requests to opt-out.

(2) Disclose, by July 1 of every calendar year, the information compiled in subsection (g)(1) within their privacy policy or posted on their website and accessible from a link included in their privacy policy
   a. In its disclosure pursuant to subsection (g)(2), a business may choose to disclose the number of requests that it denied in whole or in part because the request was not verifiable,

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

als responsible for handling consumer requests made under the CCPA or the business's compliance with the CCPA are informed of all the requirements in these regulations and the CCPA."[22]

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."[23] Even after that time, requests to opt-in to the sale of personal information must involve "a two-step opt-in process whereby the consumer shall first, clearly request to opt-in and then second, separately confirm their choice to opt-in."[24] If a consumer who has opted-out of the sale of their personal information initiates a transaction or attempts to use a product or service that requires the sale of their personal information, a business may inform the consumer that the transaction, product, or service requires the sale of their personal information and provide instructions on how the consumer can opt-in.[25] If the consumer then chooses to opt-in, it must follow the two-step process outlined in this paragraph.[26]

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 Cali-

---

was not made by a consumer, called for information exempt from disclosure, or was denied on other grounds.

Id. A business may choose to compile and disclose the information required by subsection (g)(1) for requests received "from all individuals, rather than requests received from consumers." *Id.* § 999.317(h).

A business required to comply with section 999.317(g) because it meets the ten million consumer threshold must state whether it its disclosure is based on individuals or consumers (as specified in section 999.317(h)) and must, upon request, compile and provide to the Attorney General the information required by subsection (g)(1) for requests received from consumers. *See id.* § 999.317(h).

[22]Cal. Code Regs. § 999.317(g)(3).

[23]Cal. Civ. Code § 1798.135(a)(5). This prohibition is extended, under the CPRA effective January 1, 2023, to requests to opt out of selling *or sharing* personal information and requests to limit the use or disclosure of sensitive personal information, subject to regulations to be promulgated by July 1, 2022. *See* Cal. Civ. Code § 1798.135(c)(4) (effective Jan. 1, 2023).

[24]Cal. Code Regs. § 999.316(a).

[25]Cal. Code Regs. § 999.316(b).

[26]*See* Cal. Code Regs. § 999.316(a).

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

fornia residents.

26.13A[9] Minors

26.13A[9][A] In General

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 the sale.[1] 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."[2] The CCPA refers to the prohibition on the sale of minors' personal information without consent as the "right to opt-in."[3]

Provisions governing consumers who are minors are set forth in sections 999.330, 999.331 and 999.332 of the implementing regulations. Section 999.330 addresses consumers younger than 13 years of age. Section 999.331 sets forth rules for consumers who are at least 13 years old but younger than 16. A business subject to either or both provision must include in its privacy policy a description of the processes it follows, to comply with those regulatory provisions.[4]

The requirement for parental consent for children under age 13 is consistent with the federal Children's Online Privacy Protection Act (COPPA).[5] 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.[6]

In addition to deletion requests under the CCPA (for businesses subject to the CCPA), California's "Online Eraser"

[Section 26.13A[9][A]]

[1]Cal. Civ. Code § 1798.120(c).

[2]Cal. Civ. Code § 1798.120(c).

[3]Cal. Civ. Code § 1798.120(c).

[4]Cal. Code Regs. § 999.332(a).

[5]15 U.S.C.A. §§ 6501 to 6506; 16 C.F.R. §§ 312.1 to 312.13; *see generally supra* § 26.13[2].

[6]*See supra* § 26.13[2][H].

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

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 complete erasure of content posted by the minor.[7] The Constitutionality of this provision, and whether it is preempted in certain cases by COPPA,[8] has yet to be fully tested.

Other state privacy laws governing information from minors (including Colorado and Virginia laws) are noted in section 26.13[2][I].

26.13A[9][B] Consumers 13-15 Years Old

The CCPA's implementing regulations require that a business that has actual knowledge that it sells the personal information of consumers at least 13 years of age and less than 16 years of age "establish, document, and comply with a reasonable process for allowing such consumers to opt-in to the sale of their personal information, pursuant to section 999.316."[1]

When a business receives a request to opt-in to the sale of personal information from a consumer at least 13 years of age and less than 16 years of age, it must "inform the consumer of the right to opt-out at a later date and of the process for doing so pursuant to section 999.315."[2] However, a business that exclusively targets offers of goods or services directly to consumers under 16 years of age and does not sell the personal information without the affirmative authorization of consumers at least 13 years of age and less than 16 years of age, or the affirmative authorization of their parent or guardian for consumers under 13 years of age, is not required to provide the notice of right to opt-out.[3]

26.13A[9][C] Consumers Younger than 13 Years Old

Section 999.330(a) of the regulations implementing the

---

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

[8] *See* 15 U.S.C.A. § 6502(d); *supra* § 26.13[2][F] (analyzing COPPA preemption).

[Section 26.13A[9][B]]

[1] Cal. Code Regs. § 999.331(a).

[2] Cal. Code Regs. § 999.331(b).

[3] Cal. Code Regs. § 999.332(b).

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

CCPA require a business that has actual knowledge that it sells the personal information of a consumer under the age of 13 to "establish, document, and comply with a reasonable method for determining that the person affirmatively authorizing the sale of the personal information about the child is the parent or guardian of that child."[1] This affirmative authorization is in addition to any verifiable parental consent required under COPPA.[2]

The regulations provide that "[m]ethods that are reasonably calculated to ensure that the person providing consent is the child's parent or guardian" include, but are not limited to:

a. Providing a consent form to be signed by the parent or guardian under penalty of perjury and returned to the business by postal mail, facsimile, or electronic scan;
b. Requiring a parent or guardian, in connection with a monetary transaction, to use a credit card, debit card, or other online payment system that provides notification of each discrete transaction to the primary account holder;
c. Having a parent or guardian call a toll-free telephone number staffed by trained personnel;
d. Having a parent or guardian connect to trained personnel via video-conference;
e. Having a parent or guardian communicate in person with trained personnel; and
f. Verifying a parent or guardian's identity by checking a form of government-issued identification against databases of such information, as long as the parent or guardian's identification is deleted by the business from its records promptly after such verification is complete.[3]

A business must establish, document, and comply with a reasonable method, in accordance with the methods set forth above, for determining that a person submitting a request to know or a request to delete the personal information of a child under the age of 13 is the parent or guardian of that

---

[Section 26.13A[9][C]]

[1]Cal. Code Regs. § 999.330(a)(1).

[2]Cal. Code Regs. § 999.330(a)(1); *see generally supra* § 26.13[2] (analyzing COPPA).

[3]Cal. Code Regs. § 999.330(a)(2).

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

child.[4]

When a business receives an affirmative authorization that complies with section 999.330, it is required to inform the parent or guardian of the right to opt-out and of the process for doing so on behalf of their child pursuant to section 999.315(a) through 999.315(f).[5] By contrast, a business that exclusively targets offers of goods or services directly to consumers under 16 years of age and does not sell the personal information without the affirmative authorization of consumers at least 13 years of age and less than 16 years of age, or the affirmative authorization of their parent or guardian for consumers under 13 years of age, is not required to provide the notice of right to opt-out.[6]

26.13A[10] Nondiscrimination and Financial incentives

The CCPA generally prohibits businesses from discriminating against consumers based on their exercise of any rights provided in the statute[1] or its implementing regulations.[2] 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.[3] However, the CCPA provides that businesses are not prohibited from "charging a consumer a

---

[4]Cal. Code Regs. § 999.330(c); *see generally infra* §§ 26.13A[8] (opt-in consent required from children), 26.13A[9] (children's privacy).

[5]Cal. Code Regs. § 999.330(b).

[6]Cal. Code Regs. § 999.332(b).

[Section 26.13A[10]]

[1]Cal. Civ. Code § 1798.125(a).

[2]Cal. Code Regs. § 999.336(a). A financial incentive or a price or service difference is discriminatory, and therefore prohibited by Civil Code § 1798.125, if the business treats a consumer differently because the consumer exercised a right conferred by the CCPA or its implementing regulations. *Id.*

A business's denial of a consumer's request to know, request to delete, or request to opt-out for reasons permitted by the CCPA or its implementing regulations is not deemed discriminatory. *See id.* § 999.336(c).

Similarly, a price or service difference that is the direct result of compliance with a state or federal law shall not be considered discriminatory. *Id.* § 999.336(g).

[3]Cal. Civ. Code § 1798.125(a)(1).

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

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."[4]

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."[5] 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. If a business is unable to calculate a good-faith estimate of the value of the consumer's data or cannot show that the financial incentive or price or service difference is reasonably related to the value of the consumer's data, the regulations provide that the business may not offer the financial incentive or price or service difference.[6]

The regulations include examples that further illustrate that arbitrarily assigned values will not suffice.[7]

The Attorney General's regulations require businesses to

---

[4]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.

[5]Cal. Civ. Code §§ 1798.125(b)(1), (3). Stated differently, "a business may offer a financial incentive or price or service difference if it is reasonably related to the value of the consumer's data." Cal. Code Regs. § 999.336(b). Charging a fee pursuant to Cal. Civil Code § 1798.145(i)(3), for complying with manifestly unfounded or excessive requests, is not deemed a financial incentive subject to these regulations. *See id.* § 999.336(f).

[6]Cal. Code Regs. § 999.336(b).

[7]The regulations include the following four examples:

Example 1: A music streaming business offers a free service as well as a premium service that costs $5 per month. If only the consumers who pay for the music streaming service are allowed to opt-out of the sale of their personal information, then the practice is discriminatory, unless the $5-per-month payment is reasonably related to the value of the consumer's data to the business.

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

provide extremely robust disclosures regarding any financial incentives offered in exchange for personal information in the form of a notice of financial incentive. The regulations require businesses to disclose (1) a succinct summary of the financial incentive or price or service difference offered, (2) "a description of the material terms of the financial incentive or price or service difference, including the categories of personal information that are implicated by the financial incentive or price or service difference" and the categories of personal information that are implicated, (3) how the consumer can opt-in to the financial incentive or price or service difference; (4) a statement of the consumer's right to withdraw from the financial incentive at any time and how the consumer may exercise that right; and (5) an explanation of how the financial incentive or price or service difference is reasonably related to the value of the consumer's data," including 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 "de-

---

Example 2: A clothing business offers a loyalty program whereby customers receive a $5-off coupon by email after spending $100 with the business. A consumer submits a request to delete all personal information the business has collected about them but also informs the business that they want to continue to participate in the loyalty program. The business may deny their request to delete with regard to their email address and the amount the consumer has spent with the business because that information is necessary for the business to provide the loyalty program requested by the consumer and is reasonably anticipated within the context of the business's ongoing relationship with them pursuant to Civil Code section 1798.105, subdivision (d)(1).

Example 3: A grocery store offers a loyalty program whereby consumers receive coupons and special discounts when they provide their phone numbers. A consumer submits a request to opt-out of the sale of their personal information. The retailer complies with their request but no longer allows the consumer to participate in the loyalty program. This practice is discriminatory unless the grocery store can demonstrate that the value of the coupons and special discounts are reasonably related to the value of the consumer's data to the business.

Example 4: An online bookseller collects information about consumers, including their email addresses. It offers coupons to consumers through browser pop-up windows while the consumer uses the bookseller's website. A consumer submits a request to delete all personal information that the bookseller has collected about them, including their email address and their browsing and purchasing history. The bookseller complies with the request but stops providing the periodic coupons to the consumer. The bookseller's failure to provide coupons is discriminatory unless the value of the coupons is reasonably related to the value provided to the business by the consumer's data. The bookseller may not deny the consumer's request to delete with regard to the email address because the email address is not necessary to provide the coupons or reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business.

Cal. Code Regs. § 999.336(d).

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

scription of the method the business used to calculate the value of the consumer's data."[8] The form used for this notice is discussed earlier in this section 26.13A and is set forth in section 999.307(a).

The Attorney General has set forth 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;
(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.[9]

A business offering a financial incentive or price or service difference subject to Cal. Civil Code § 1798.125 must "use and document a reasonable and good faith method for calculating the value of the consumer's data" considering one or more of these eight methods.[10] For the purpose of calculating the value of consumer data, a business may consider the value to the business of the data of all natural persons in the United States and not just consumers.[11]

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. Calculations

---

[8]Cal. Code Regs. §§ 999.307(b); 999.336(e).

[9]Cal. Code Regs. § 999.337(a).

[10]Cal. Code Regs. § 999.337(a). *Value of the consumer's data* means "the value provided to the business by the consumer's data as calculated under section 999.337." *Id.* § 999.301(w).

[11]Cal. Code Regs. § 999.337(b).

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

made pursuant to section 999.337 also potentially could be used against a business in litigation or administrative enforcement actions.

26.13A[11] 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 collect and sell consumers' personal information, but do not have direct relationships with consumers.[1] 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."[2] 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.[3]

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.[4]

The Attorney General also is required to publicly list all registered data brokers on its website.[5] The registry may be accessed at https://oag.ca.gov/data-brokers

Data brokers generally are not subject to the CCPA's requirement for notice at the time of collection (because they do not collect data directly from consumers). The Attorney General's CCPA regulations clarify that a business that does not collect personal information directly from consumers does not need to provide notice to consumers at the time of collection.[6] They clarify, however, that, to avoid having to provide notice to consumers at the time of collection, data brokers registered with the California Attorney General pur-

---

[Section 26.13A[11]]

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

[2] Cal. Civ. Code § 1798.99.82.

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

[4] Cal. Civ. Code § 1798.99.82(c).

[5] Cal. Civ. Code § 1798.99.84.

[6] Cal. Code Regs. § 999.305(d).

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

suant 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."[7]

26.13A[12] Scope and exclusions

The California legislature mandated that the CCPA "be liberally construed to effectuate its purposes."[1] 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.[2] 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.[3]

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.[4] 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[5]

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

---

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

[Section 26.13A[12]]

[1]Cal. Civ. Code § 1798.194.

[2]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.

[3]Cal. Civ. Code § 1798.196.

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

[5]Cal. Civ. Code § 1798.145(b).

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

what is authorized under the Act.[6]

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 covered by a vehicle warranty or a recall pursuant to federal law.[7] 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[8] (although it may apply to certain deidentified

---

[6]Cal. Civ. Code §§ 1798.145(d)(1), 1798.145(d)(2). Effective January 1, 2023, the CPRA will exclude any activity otherwise subject to the CPRA (such as sales or sharing of personal information) to the extent it constitutes an "activity involving the collection, maintenance, disclosure, sale, communication, or use of any personal information bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by a consumer reporting agency," as defined in 15 U.S.C.A. § 1681a(f), by a furnisher of information, as set forth in 15 U.S.C.A. § 1681s-2, "who provides information for use in a consumer report, as defined in" 15 U.S.C.A. § 1681a(d), and by a user of a consumer report as set forth in 15 U.S.C.A. § 1681b, to the extent this activity involves "the collection, maintenance, disclosure, sale, communication or use of such information by that agency, furnisher, or user is subject to regulation under the Fair Credit Reporting Act," 15 U.S.C.A. §§ 1681 *et seq.*, "and the information is not collected, maintained, used, communicated, disclosed or sold except as authorized by the Fair Credit Reporting Act." *See* Cal. Civil Code § 1798.145(d) (effective Jan. 1, 2023). This exclusion, however, does not apply to the private cause of action for certain security breaches created by section 1798.150. *See id.* § 1798.145(d)(3) (effective Jan. 1, 2023); *see generally infra* § 26.13A[14] (analyzing the private right of action under 1798.150).

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

[8]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

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

data derived from these records[9]).

The CCPA temporarily excludes from its scope certain B2B businesses and personal information collected from job applicants or employees, including information necessary for a business to administer benefits, until the CPRA takes effect on January 1, 2022.[10] Even before then, a business is still required to disclose the categories of personal information that it collects from employees and job applicants pursuant to the CCPA.[11] Effective January 1, 2023, under the CPRA, the exemptions for certain B2B transactions and job applicant and employee data will expire absent further

---

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).

[9]*See* Cal. Civ. Code § 1798.135(a)(5)(D); *see generally supra* § 26.13A[2][B].

[10]*See* Cal. Civ. Code §§ 1798.145(h)(1), 1798.145(m), 1798.145(n). California A.B. 1281, which was signed into law on September 29, 2020, extended the effective date of Cal. Civ. Code § 1798.145 applicable to employee data to January 1, 2022, rather than January 1, 2021, but "only if the voters do not approve any ballot proposition that amends Section 1798.145 of the Civil Code at the November 3, 2020, statewide general election." Proposition 24—the California Privacy Rights Act (CPRA)—was adopted, and by its terms extended the partial exemption created by subsection 1798.145(n) for B2B businesses and 1798.145(m) for job applicant and employee data through December 31, 2022 (the day before the CPRA takes effect). *See* Cal. Civ. Code §§ 1798.145(m)(4), 1798.145(n)(3) (effective Jan. 1, 2023).

Section 1798.145(n)(1) currently provides that:

> The obligations imposed on businesses by Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.130, and 1798.135 shall not apply to personal information reflecting a written or verbal communication or a transaction between the business and the consumer, where the consumer is a natural person who is acting as an employee, owner, director, officer, or contractor of a company, partnership, sole proprietorship, nonprofit, or government agency and whose communications or transaction with the business occur solely within the context of the business conducting due diligence regarding, or providing or receiving a product or service to or from such company, partnership, sole proprietorship, nonprofit, or government agency.

[11]*See* Cal. Civ. Code §§ 1798.145(h)(3), 1798.145(n)(3).

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

amendment or regulatory relief (or federal preemption). The CPRA also will extend the consumer right against retaliation to employees.[12]

The CPRA also creates an exception for a commercial credit reporting agency's collection, processing, sale, or disclosure of business controller information used to identify the relationship of a consumer to a business which the consumer owns or contact the consumer only in the consumer's role as the owner, director, officer, or management employee of the business.[13]

In construing the CCPA, it may not be applied to infringe upon the noncommercial free speech rights protected by the California Constitution.[14]

---

[12]*See* Cal. Civ. Code § 1798.125(a)(1)(E) (effective Jan. 1, 2023).

[13]*See* Cal. Civ. Code § 1798.145(o) (effective Jan. 1, 2023) (creating an exception for the obligations otherwise imposed by sections 1798.105 and 1798.120).

[14]Cal. Civ. Code § 1798.145(m) ("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.") (repealed 2021). Article I section 2(b) of the California Constitution provides that:

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

Cal. Const. Art. I § 2(b). Although this version of section 1798.145(m) was repealed effective January 1, 2022, the protections afforded by the

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

26.13A[13] Regulatory enforcement

The CCPA 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),[1] Health Insurance Portability and Accountability Act (HIPAA)[2] and the Gramm-Leach-Bliley Act (GLB).[3] The Attorney General is authorized to adopt regulations,[4] provide opinions, and file suit to enforce the law (subject to affording businesses notices and an opportunity to cure within 30 days).[5] Given the limited nature of the private right of action (which, as discussed in subsection 26.13A[14], only relates to security breaches), the Attorney General has been given primary responsibility for interpreting and shaping enforcement priorities under the CCPA. Significantly, the 30 day opportunity to cure following notice will disappear for regulatory enforcement actions (but not the limited private cause of action for a security breach[6]) when the CPRA takes effect on January 1, 2023 (unless offered voluntarily by the California Privacy Protection Agency, in specific enforcement notices).

The CCPA also allows any business or third party may seek the opinion of the Attorney General for guidance on how to comply with the CCPA[7] (although this right is eliminated, effective January 1, 2023, by the CPRA, unless the right to an advisory opinion is created by a CPRA implementing regulation).

The CCPA empowered the Attorney General to begin

California Constitution should nonetheless trump the CCPA, to the extent there is a conflict.

[Section 26.13A[13]]

[1]*See supra* § 26.13[2][F].

[2]*See supra* § 26.11.

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

[4]*See* Cal. Civ. Code § 1798.185.

[5]*See* Cal. Civ. Code § 1798.155. The regulations promulgated by the Attorney General extend enforcement power to violations of the regulations themselves. *See* Cal. Code Regs. § 999.300(b).

[6]*See* Cal. Civ. Code § 1798.150(b) (effective Jan. 1, 2023); *infra* § 26.13A[14] (analyzing the private right of action).

[7]Cal. Civ. Code § 1798.155(a).

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

enforcement on July 1, 2020.[8] The Office of the Attorney General in fact sent out its first enforcement letters shortly thereafter. While the Attorney General may pursue individual companies deemed not to be in compliance, it also has targeted particular industries or practices. For example, in early 2022, Attorney General Bonta announced that his office had sent concompliance and 30-day request to cure notices to operators of loyalty programs.[9]

The CCPA further authorizes the Attorney General to bring a civil action against businesses, service providers, or any other person that violates the CCPA.[10] A business "shall be in violation" if it "fails to cure any alleged violation within 30 days after being notified of noncompliance."[11] 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.[12] While the penalties *per violation* are small, it remains to be seen how the Attorney General will construe the term *violation* in administrative 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.[13] 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.

---

[8] *See* Cal. Civ. Code § 1798.185(c) (permitting enforcement to begin on the earlier of six months after publication of final regulations or July 1, 2020).

[9] *See* Press Release, Office of the California Attorney General, *On Data Privacy Day, Attorney General Bonta Puts Businesses Operating Loyalty Programs on Notice for Violations of California Consumer Privacy Act* (Jan. 28, 2022).

[10] Cal. Civ. Code § 1798.155(b).

[11] Cal. Civ. Code § 1798.155(a).

[12] Cal. Civ. Code § 1798.155(b).

[13] Cal. Civ. Code § 1798.160.

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

Under the CPRA this authority will be transitioned to the California Privacy Protection Agency, a new agency created by the CPRA.[14] The CPRA authorized five million dollars to the Agency for the fiscal year 2020-2021 plus an additional ten million dollars each year thereafter, adjusted for cost of living changes.[15] After the CPRA takes effect on January 1, 2023, the Agency will be empowered to investigate possible violations relating to any business, service provider, contractor, or person, on its own initiative, or in response to a sworn complaint from any person.[16] Under the CPRA, administrative actions must be brought within five years of the time the alleged violation occurred.[17] No finding of probable cause to believe that the CPRA has been violated may be made unless the Agency provides at least 30 days' notice of the alleged violation, with a summary of the evidence, and their right to appear with counsel.[18] Among other things, the Agency will have the power to subpoena witnesses.[19] The Agency also will be able to bring a civil action to enforce any unpaid administrative fines (within four years of the date on which the fine was imposed).[20]

Agency decisions under the CPRA will be subject to judicial review, subject to an abuse of discretion standard.[21]

The Attorney General will also be authorized to seek in court 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 (as well as for each violation involving the personal information of minor consumers).[22] No civil action may be filed by the Attorney General, however, where the California Privacy Protection Agency (sometimes referred to as the CPPA, as opposed to the CCPA or CPRA) has issued an administrative decision pursuant to section

---

[14]*See* Cal. Civ. Code §§ 1798.199.10 to 1798.199.100.

[15]*See* Cal. Civ. Code § 1798.199.90.

[16]*See* Cal. Civ. Code § 1798.199.45.

[17]*See* Cal. Civ. Code § 1798.199.70.

[18]*See* Cal. Civ. Code § 1798.199.50.

[19]*See* Cal. Civ. Code § 1798.199.65.

[20]*See* Cal. Civ. Code § 1798.199.75; *see also id.* § 1798.199.80 (addressing clerk- issued orders where the time for judicial review of a final agency order or decision has lapsed).

[21]*See* Cal. Civ. Code § 1798.199.85.

[22]*See* Cal. Civ. Code § 1798.199.90.

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

1798.199.85 or an order pursuant to section 1798.99.55 against the same person for the same violation.[23]

The Agency (or a court) must consider the good faith cooperation of a business, service provider, contractor, or other person, in determining the amount of any administrative fine or civil penalty for a violation of the CPRA (and may not award both an administrative fine and civil penalty).[24]

26.13A[14] Private right of action for data breaches

The CCPA (and, as of January 1, 2023, the CPRA) affords 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 . . . ."[1] The private right of action created by the CCPA may be brought *only* for data breaches arising from a business's failure to maintain reasonable security measures, and not

---

[23]*See* Cal. Civ. Code § 1798.199.90(d).

[24]*See* Cal. Civ. Code § 1798.199.100.

[Section 26.13A[14]]

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

(A) An individual's first name or first initial and 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

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

any other failures to comply with the CCPA.[2] Nevertheless, the potential availability of statutory damages has created a strong incentive for plaintiffs' class action lawyers to assert CCPA claims whenever a data security incident affects California residents. Whether a plaintiff in fact may assert a CCPA claim in state or federal court (and potentially seek class certification) generally depends on whether (1) the plaintiff is a resident of California, (2) the defendant is a *business* (as defined in the statute) subject to the CCPA,[3] (3)

---

a physical or digital photograph, unless used or stored for facial recognition purposes.

(vii) Genetic data.

(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).

Genetic data means any data, regardless of its format, that results from the analysis of a biological sample of an individual, or from another source enabling equivalent information to be obtained, and concerns genetic material. Genetic material includes, but is not limited to, deoxyribonucleic acids (DNA), ribonucleic acids (RNA), genes, chromosomes, alleles, genomes, alterations or modifications to DNA or RNA, single nucleotide polymorphisms (SNPs), uninterpreted data that results from analysis of the biological sample or other source, and any information extrapolated, derived, or inferred therefrom. *Id.* § 1798.81.5(d)(5).

Under the CPRA, the definition of *personal information* applicable to lawsuits brought pursuant to section 1798.150(a)(1) will be expanded to also include an "email address in combination with a password or security question and answer that would permit access to the account . . . ." *Id.* § 1798.150(a)(1) (effective Jan. 1, 2023).

[2]Cal. Civ. Code § 1798.150(c).

[3]*See, e.g.*, *In re Blackbaud, Inc., Customer Data Breach Litig.*, Case No. 3:20-mn-02972-JMC, 2021 WL 3568394, at *4-6 (D.S.C. Aug. 12, 2021) (denying defendant's motion to dismiss where the plaintiffs adequately alleged that Blackbaud was a *business* under the CCPA in a case arising out of a ransomware attack).

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

the incident occurred on or after January 1, 2020[4] and (4) resulted in the unauthorized[5] access and exfiltration, theft, or disclosure of specific *personal information* (defined more narrowly than under the CCPA generally),[6] (5) the personal information was unencrypted or unredacted at the time when exfiltrated, stolen, or disclosed,[7] (6) the exfiltration, theft, or disclosure resulted from a business's failure to implement reasonable security measures, and (7) the plaintiff is not subject to a binding and enforceable arbitration agreement.[8] To recover statutory damages, a plaintiff must further show that it provided notice and an opportunity to cure, and that the business did not do so (as discussed

---

[4]*See, e.g.*, *Gardiner v. Walmart Inc.,* Case No. 20-cv-04618-JSW, 2021 WL 2520103, at *2-3 (N.D. Cal. Mar. 5, 2021) (dismissing plaintiff's CCPA claim for failing to allege that the breach occurred after January 1, 2020, when the CCPA took effect, and failing to adequately allege the disclosure of personal information as defined by the statute); *see also Gardiner v. Walmart Inc.,* Case No. 20-cv-04618-JSW, 2021 WL 4992539, at *2 (N.D. Cal. July 28, 2021) (dismissing plaintiff's CCPA claim with prejudice).

[5]*See, e.g.*, *Gershfeld v. Teamviewer US, Inc.,* Case No. SACV 21-00058-CJC(ADSx), 2021 WL 3046775, at *2 (C.D. Cal. June 24, 2021) (dismissing plaintiff's CCPA claim, in a putative class action suit, where the disclosure alleged did not result from defendant's alleged storage of information "in a nonencrypted and nonredacted fashion," and was authorized, not unauthorized);

[6]*See* Cal. Civ. Code §§ 1798.150(a)(1), 1798.81.5; *see also, e.g., Gardiner v. Walmart Inc.,* Case No. 20-cv-04618-JSW, 2021 WL 2520103, at *2-3 (N.D. Cal. Mar. 5, 2021) (dismissing plaintiff's CCPA claim for, among other things, failing to adequately allege the disclosure of personal information as defined by the statute).

As noted earlier in this section, the definition of *personal information* applicable to lawsuits brought pursuant to section 1798.150(a)(1) will be expanded under the CPRA to also include an "email address in combination with a password or security question and answer that would permit access to the account . . . ." Cal. Civ. Code § 1798.150(a)(1) (effective Jan. 1, 2023).

[7]*See, e.g.*, *Gershfeld v. Teamviewer US, Inc.,* Case No. SACV 21-00058-CJC(ADSx), 2021 WL 3046775, at *2 (C.D. Cal. June 24, 2021) (dismissing plaintiff's CCPA claim, in a putative class action suit, where the disclosure alleged did not result from defendant's alleged storage of information "in a nonencrypted and nonredacted fashion," and was authorized, not unauthorized);

[8]*See generally supra* § 22.05[2][M] (analyzing the enforceability of consumer arbitration claims, which under the Federal Arbitration Act and Supremacy Clause of the U.S. Constitution, will preempt inconsistent state laws or judge made rules favoring litigation of disputes). The CCPA does not purport to bar arbitration and, if it did, it would conflict with, and be preempted by, the Federal Arbitration Act. *See supra* § 22.05[2][M].

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

later in this section).

CCPA claims frequently are brought as putative class action suits because of the potential availability of statutory damages. Whether a case proceeds as a class action depends on whether plaintiffs can meet their burden of showing entitlement to class certification.[9] Where claims are subject to binding and enforceable arbitration agreements, however, a class typically may not be certified either in court or in arbitration.[10]

Many purported CCPA claims in fact are not viable because the information at issue was accessed and exfiltrated, stolen, or disclosed in encrypted or redacted form (even if it may have been subsequently decrypted or recompiled); the exfiltration, theft, or disclosure was authorized; the data elements exfiltrated, stolen, or disclosed do not qualify as *personal information* for purposes of Cal. Civ. Code §§ 1798.150(a)(1) and 1798.81.5; the defendant is not a *business* subject to the CCPA based on its size, revenue or use of personal information; the breach occurred prior to January 1, 2020; or the dispute is subject to binding arbitration. Some of these issues may be addressed through preliminary motion practice,[11] while some require affirmative evidence and therefore would have to be addressed on

---

[9]Class certification is analyzed in section 25.07[2] in chapter 25 and is also addressed in connection with data privacy putative class action suits in section 26.15, and in connection the data breach putative class action suits in section 27.07 (in chapter 27).

[10]*See generally supra* § 22.05[2][M] (analyzing the enforceability of arbitration provisions in consumer cases, class action waivers, and class arbitration).

[11]*See, e.g.*, *Gershfeld v. Teamviewer US, Inc.,* Case No. SACV 21-00058-CJC(ADSx), 2021 WL 3046775, at *2 (C.D. Cal. June 24, 2021) (dismissing plaintiff's CCPA claim, in a putative class action suit, where the disclosure alleged did not result from defendant's alleged storage of information "in a nonencrypted and nonredacted fashion," and was authorized, not unauthorized); *Gardiner v. Walmart Inc.,* Case No. 20-cv-04618-JSW, 2021 WL 2520103, at *2-3 (N.D. Cal. Mar. 5, 2021) (dismissing plaintiff's CCPA claim for failing to allege that the breach occurred after January 1, 2020, when the CCPA took effect, and failing to adequately allege the disclosure of personal information as defined by the statute).

In a number of cases, plaintiffs have voluntarily dismissed CCPA claims in response to motions to dismiss. *See, e.g.*, *McCoy v. Alphabet, Inc.,* Case No. 20-cv-05427-SVK, 2021 WL 405816, at *8 (N.D. Cal. Feb. 2, 2021); *Flores-Mendez v. Zoosk, Inc.*, No. C 20-04929 WHA, 2021 WL 308543, at *4 (N.D. Cal. Jan. 30, 2021); *Shay v. Apple Inc.,* 512 F. Supp. 3d 1066, 1070 (S.D. Cal. 2021).

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

motion for summary judgment or at trial.

Where a CCPA claim is plausibly alleged, a business may defend the claim by arguing, among other things, that the breach did not involve personal information, that the breach was not caused by its violation of the duty to implement and maintain reasonable security procedures and practices (*i.e.,* no causation—the breach resulted for some other reason), that notwithstanding the breach the business took reasonable security measures, or that the plaintiff is not entitled to seek statutory damages because the business cured the action in response to a 30 day CCPA notice letter (or no such letter was sent, or the letter sent was defective in failing to specifically identify the violation to be cured).

What constitutes a *reasonable* security measure is not defined in the statute. Hence, where the issue is legitimately contested, causation may raise factual questions that could be difficult to resolve through motion practice in some cases. The adequacy of any alleged cure may also raise factual questions in some cases.

Where liability and entitlement to statutory damages are established, a defendant may argue that damages should be awarded at the lower end of the statutory damage range, rather than the higher end, based on the nonexclusive list of criteria set forth in the statute (and any others a defendant wishes the trier of fact to consider).[12]

A person harmed by the data breach may who can establish liability under the CCPA may 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.[13] 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."[14] Nevertheless, a data breach impacting 100,000 consumers could

[12]*See* Cal. Civ. Code § 1798.150(a)(2).

[13]Cal. Civ. Code § 1798.150(a)(1).

[14]Cal. Civ. Code § 1798.150(a)(2).

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

invite putative class action suits seeking up to $75,000,000, will almost always be seems disproportionate to the harm caused (if any). 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 a minimum of recovery of *at least* $100,000,000. These calculations are not only wildly disproportionate to the harm experienced in most cases, but 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).[15] Given the potential for large awards in putative class action suits, the private cause of action created by the CCPA has generated substantial litigation since claims could first be asserted in court, on January 1, 2020.

To seek an award of statutory damages under the CCPA, 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, "prior to initiating any action against a business for statutory damages on an individual or class-wide basis. . . ."[16] If within the 30 days the business actually cures the noticed violation (assuming a cure is possible) and provides the consumer an express written statement that the violations have been cured and that no further violations shall occur, then no action for individual statutory damages or class-wide statutory damages may be initiated against the business.[17]

This provision was modeled on the 30 day notice and cure period in the California Consumers Legal Remedies Act,[18] a statute popular with class action counsel. Under that stat-

---

[15]*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).

[16]Cal. Civ. Code § 1798.150(b) (emphasis added).

[17]Cal. Civ. Code § 1798.150(b).

[18]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].

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

ute, 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 . . . ."[19] Nevertheless, it is generally desirable for defense counsel to respond to valid CCPA 30 day notification letters—*i.e.,* those that identify "the specific provisions of this title the consumer alleges have been or are being violated . . . ." While a business should avoid undertaking an obligation in response to a CCPA 30-day notice letter that could itself form the basis of a CCPA claim for noncompliance (as discussed below), any legitimate effort to cure could prevent a claimant (or class of claimants) from recovering statutory damages, create a jury question over whether plaintiffs are even entitled to recover statutory damages, or justify an award at the lower end of the range for statutory damages.

Some class action lawyers, concerned about beating other plaintiffs' counsel to file first following a security incident, have initiated legal action before the expiration of the 30-day period and waited to serve the complaint until the expiration of the period. In such cases, statutory damages would be unavailable because the statute is clear that notice and a full 30 days to cure must occur "*prior* to initiating any action against a business for statutory damages on an individual or class-wide basis . . . ."[20]

The CCPA thus sets up a number of potential substantive and procedural hurdles that a plaintiff must surmount to recover statutory damages. At the outset of the case, a defendant may be able to obtain a ruling through motion practice that the plaintiff is not entitled to recover statutory damages because the plaintiff did not provide notice and an opportunity to cure, is not entitled to maintain a CCPA action at all because the plaintiff is not a California resident or the defendant or information are not subject to the CCPA (based on the definitions of a *business* and *personal information*), or may not proceed in court (either individually, or to seek class certification) because the claim is subject to arbitration, depending on the facts alleged by the plaintiff and evidence that may be subject to judicial notice or otherwise presented to the court. While a defendant may be

[19]Cal. Civ. Code § 1798.150(b).

[20]Cal. Civ. Code § 1798.150(b).

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

able to win or narrow a claim through motion practice, a plaintiff may need to proceed to trial to prove its entitlement to recover under the CCPA, by showing that any security breach was caused by a defendant's failure to maintain reasonable practices, and to recover statutory damages (at least above the minimum $100 level[21]). Plaintiff's counsel also typically must be able to win a motion for class certification to make CCPA statutory damage claims worthwhile litigating in most instances. For all of these reasons, while many purported CCPA claims have been filed since January 1, 2020, few if any thus far have proceeded to judgment for the plaintiff. Most have been won (or moved to individual arbitration) by the defendants, settled, or await trial.

The CPRA largely retains section 1798.150 intact, but, effective January 1, 2023, section 1798.150 will also apply to businesses engaged in consumer credit collection and reporting.[22] It also will authorize legal action when a person's "email address in combination with a password or security question and answer that would permit access to the account"—and not just *personal information* as defined in sec-

---

[21]A plaintiff presumably could move for summary judgment if it could establish liability and sought only the minimum statutory award. Where a jury trial has been demanded, a defendant would be entitled to have the jury determine the amount of the award where any amount above the minimum was sought. *Cf. BMG Music v. Gonzalez,* 430 F.3d 888, 892 (7th Cir. 2005) (holding that the defendant did not have a right to a jury trial in a copyright infringement suit where the plaintiff sought and was awarded statutory damages at the lowest permissible level, on summary judgment), *cert. denied*, 547 U.S. 1130 (2006).

[22]The CPRA generally will not apply to "activity involving the collection, maintenance, disclosure, sale, communication, or use of any personal information bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by a consumer reporting agency," as defined in 15 U.S.C.A. § 1681a(f), by a furnisher of information, as set forth in 15 U.S.C.A. § 1681s-2, "who provides information for use in a consumer report, as defined in" 15 U.S.C.A. § 1681a(d), and by a user of a consumer report as set forth in 15 U.S.C.A. § 1681b, but only to the extent this activity involves "the collection, maintenance, disclosure, sale, communication or use of such information by that agency, furnisher, or user . . . subject to regulation under the Fair Credit Reporting Act," 15 U.S.C.A. §§ 1681 *et seq*., "and the information is not collected, maintained, used, communicated, disclosed or sold except as authorized by the Fair Credit Reporting Act." *See* Cal. Civil Code § 1798.145(d) (effective Jan. 1, 2023). This exclusion, however, does not apply to the private cause of action for certain security breaches created by section 1798.150. *See id*. § 1798.145(d)(3) (effective Jan. 1, 2023).

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

tion 1798.81.5(d)—has been 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 appropriate to the nature of the information.[23]

Effective January 1, 2023, the CPRA also will provide that the implementation and maintenance of reasonable security procedures and practices pursuant to Cal. Civil Code § 1798.81.5 following a breach may not be deemed a cure under the CPRA.[24] It also expands the data elements that could trigger a claim under the CPRA to include an email address in combination with a password or security question and answer that would permit access to the account.[25] Inferentially, prior to January 1, 2023, it may be possible to cure a CCPA 30 day claim by implementing and maintaining reasonable security procedures and practices pursuant to Cal. Civil Code § 1798.81.5.

The CPRA will, as of January 1, 2023, prohibit any waiver of "a representative action" waiver, including "any right to a remedy or means of enforcement . . . ."[26] This would render void any class action waiver in litigation. However, a stipulation for individual, not class-wide arbitration of CCPA claims that is part of a binding and enforceable arbitration provision subject to the Federal Arbitration Act should be enforceable based on binding U.S. Supreme Court precedent construing the Federal Arbitration Act and the Supremacy Clause of the U.S. Constitution[27] (although the issue of the validity of such a provision could be left to the arbitrator,

---

[23]*See* Cal. Civ. Code § 1798.150(a) (effective Jan. 1, 2023).

[24]Cal. Civil Code § 1798.150(b) (effective Jan. 1, 2023).

[25]Cal. Civil Code § 1798.150(a)(1) (effective Jan. 1, 2023).

[26]*See* Cal. Civil Code § 1798.192 (effective Jan. 1, 2023) ("Any provision of a contract or agreement of any kind, including a representative action waiver, that purports to waive or limit in any way rights under this title, including, but not limited to, any right to a remedy or means of enforcement, shall be deemed contrary to public policy and shall be void and unenforceable.").

[27]*See Stolt-Nielsen S.A. v. AnimalFeeds Int'l Corp.*, 559 U.S. 662 (2010); *see also Lamps Plus, Inc. v. Varela*, 139 S. Ct. 1407, 1415-19 (2019) (holding that ambiguity in an arbitration agreement does not provide sufficient grounds for compelling classwide arbitration); *Epic Systems Corp. v. Lewis*, 138 S. Ct. 1612, 1623 (2018) (explaining that "*Concepcion*'s essential insight remains: courts may not allow a contract defense to reshape traditional individualized arbitration by mandating classwide arbitration procedures without the parties' consent."); *see generally supra*

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

and not a court, if the arbitration provision includes a delegation clause and this issue is not carved out from the delegation provision[28]). Arbitration issues in connection with consumer data privacy and cybersecurity claims are analyzed more extensively in section 22.05[2][M] in chapter 22.

It remains to be seen whether the Attorney General will promulgate regulations under the CPRA to provide more detailed guidance on the type of "cure" that would meet the requirement of the statute (such as measures to mitigate the consequences of a breach and minimize the risk of similar future breaches) beyond the new statutory limitation on cure attempts made pursuant to Cal. Civil Code § 1798.81.5, 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.[29]

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.[30]

Significantly, the cause of action established by section 1798.150 applies "only to violations as defined in subdivision (a) and shall not be based on violations of any other section of this title. Nothing in this title shall be interpreted to serve as the basis for a private right of action under any other law."[31] A violation of the CCPA therefore could *not* form the basis for a claim under California's notorious unfair competition law, California Business & Professions Code section

---

§ 22.05[2][M].

[28]*See, e.g.*, *Lamps Plus, Inc. v. Varela*, 139 S. Ct. 1407, 1415-19 (2019) (holding that ambiguity in an arbitration agreement does not provide sufficient grounds for compelling classwide arbitration, which is only permissible when expressly agreed upon); *see generally supra* § 22.05[2][M] (analyzing the issue in depth).

[29]Cal. Civ. Code § 1798.150(b).

[30]Cal. Civ. Code § 1798.150(b).

[31]Cal. Civ. Code § 1798.150(c).

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

17200,[32] which typically affords a cause of action for violation of other statutes, laws or regulations.[33] The private enforcement right created by the CCPA is actually quite narrow (and will remain so even when the CPRA takes effect). Nevertheless, the potential availability of statutory damages means that section 1798.150 will ontinue to 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 should 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 for undertaking, but failing to adhere to, any of the provisions of the CCPA. Although a claim by a resident of another state could not be premised on a violation of the

---

[32]*See, e.g.*, *Silver v. Stripe, Inc.*, Case No. 4:20-cv-08196-YGR, 2021 WL 3191752, at *7 (N.D. Cal. July 28, 2021) (dismissing plaintiffs' California unfair competition claim to the extent based on an alleged violation of the CCPA).

[33]*See, e.g.*, 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].

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

CCPA *per se,* the failure of a business to adhere to its stated practices or procedures potentially could be actionable under theories of express or implied contract or unfair competition.[34]

The CCPA also leaves in place an array of other California privacy laws, which could form the basis for litigation against a business—even if noncompliance with the CCPA (other than a security breach within the terms of section 1798.150) is not be actionable in a private lawsuit.[35] 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.[36] 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.[37] Unlike the CCPA, Cal-OPPA provides a private right of action[38] and potentially could support a claim for a violation of California's unfair competition statute, Cal. Bus. & Prof. Code § 17200.[39]

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

---

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

[35]*See generally supra* § 26.13[6].

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

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

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

[39]*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].

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

customers to opt out, pursuant to the "Shine the Light" Law.[40] Disclosures under the Shine the Light Law must be, in at least some ways, more fulsome than pursuant to the 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."[41] Further, a business is afforded less time—only 30 days—to comply with a disclosure request under the Shine the Light Law[42] 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).[43]

Data 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[44] or injunctive relief,[45] in addition to any other remedies that may be available.[46] 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.[47] 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.[48] CCPA and other California law claims, of course, could be brought in California state courts.

---

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

[41]Cal. Civ. Code § 1798.83(b)(3).

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

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

[44]Cal. Civil Code § 1798.84(b).

[45]Cal. Civil Code § 1798.84(e).

[46]Cal. Civil Code § 1798.84(g).

[47]*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).

[48]*See, e.g.*, *Rahman v. Marriott International, Inc.*, Case No. SA CV 20-00654-DOC-KES, 2021 WL 346421 (C.D. Cal. Jan. 12, 2021) (dismissing plaintiff's complaint under the CCPA and for breach of contract, breach of implied contract, unjust enrichment and unfair competition, for lack of Article III standing, in a suit arising out of Russian employees accessing

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

As analyzed more extensively in other sections of this treatise,[49] other claims typically joined in security breach and data 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.[50]

The cause of action created by the CCPA, by providing a remedy of statutory damages, has increased 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,[51] many of these claims have been brought in federal court, although suits by California residents against California companies need to be

---

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

[49]*See supra* § 27.07 (cybersecurity breach putative class action litigation); *infra* § 26.15 (data privacy putative class action litigation).

[50]*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).

[51]*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), *cert. denied*, 139 S. Ct. 1373 (2019); *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).

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

brought in state court, because of the lack of diversity jurisdiction, unless plaintiffs are able to also sue for violations of federal statutes or allege jurisdiction under the Class Action Fairness Act (CAFA),[52] for putative class action suits. Indeed, CCPA claims have been brought in federal court in other states as well.

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.[53] Crafting a binding and enforceable arbitration provision is addressed in section 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, if it is possible to do so.[54] 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 (or contractors, under the CPRA) leaves open the possibility for litigation between or among *businesses*, *service providers* and *third parties*, as those terms

---

[52]28 U.S.C.A. § 1332(d); *see generally infra* § 26.15 (discussing CAFA jurisdiction in connection with data privacy litigation).

[53]*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 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].

[54]*See supra* §§ 22.05[2][P] (analyzing third-party beneficiaries in Terms of Use agreements), 22.05[2][M][vi] (drafting tips for consumer arbitration provisions).

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

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 administrative enforcement actions brought by the California Attorney General or, on or after July 1, 2023, by the California Privacy Protection Agency, pursuant to the CPRA).

It is possible that, at some point, Congress may act to preempt the CCPA prior to the time the CPRA is scheduled to enter into force on January 1, 2023.

The CCPA 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.[55] Dormant Commerce Clause arguments thus far have been rebuffed in lower court challenges to various state privacy laws[56]—albeit ones substantially less burdensome or expensive for out-of-state companies to comply with. The

---

[55]*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).

[56]*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

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

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[57]—suggests there potentially could be merit to an argument that the CCPA burdens interstate commerce. Dormant Commerce Clause case law is analyzed in section 35.04 in chapter 35.

Putative data privacy class action litigation is analyzed in section 26.15. Putative data breach class action litigation is analyzed in section 27.07.

26.13A[15] Non-waiver

The CCPA provides that any provision of a contract or agreement of any kind that purports to waive or limit in any way a consumer's rights under the statute, including, but not limited to any right to a remedy or means of enforcement, "shall be deemed contrary to public policy and shall be void and unenforceable."[1] Effective January 1, 2023, the CPRA will add to this section a prohibition on "a representative action waiver . . . ."[2]

This provision "shall not prevent a consumer from declining to request information from a business, declining to opt out of a business's sale of the consumer's personal information, or authorizing a business to sell or share the consumer's personal information after previously opting out."[3]

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).

[57]*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

[Section 26.13A[15]]

[1]Cal. Civ. Code § 1798.192.

[2]Cal. Civ. Code § 1798.192 (effective Jan. 1, 2023).

[3]Cal. Civ. Code § 1798.192.

PAGE PROOFS - SUBJECT TO REVISION
© 2022 Ian C. Ballon, www.IanBallon.net

E-COMMERCE & INTERNET LAW: TREATISE WITH FORMS 2D 2022

Ian C. Ballon

2022 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

- AI, ML, screen scraping and data portability
- Antitrust in the era of techlash
- The CPRA, Virginia, Colorado and Nevada pricy laws, GDPR, California IoT security statute, state data broker laws, and other privacy and cybersecurity laws
- Software copyrightability and fair use after *Google v. Oracle*
- Mobile and online contract formation, unconscionability and enforcement of arbitration and class action waiver clauses in an era of mass arbitration
- TCPA law and litigation after *Facebook v. Duguid* - 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 (including the CDA and DMCA)
- 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
- Defending cybersecurity breach and data privacy class action suits – case law, trends & strategy
- IP issues including Copyright and Lanham Act fair use, *Rogers v. Grimaldi,* 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, #hashtags, 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

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

Chapter 1. Context for Developing the Law of the Internet
2. A Framework for Developing New Law
3. [Reserved]

Part II. Intellectual Property

4. Copyright Protection in Cyberspace
5. Data Scraping, Database Protection, and the Use of Bots and Artificial Intelligence to Gather Content and Information
6. Trademark, Service Mark, Trade Name and Trade Dress Protection in Cyberspace
7. Rights in Internet Domain Names

Volume 2

Chapter 8. Internet Patents
9. Unique Intellectual Property Issues in Search Engine Marketing, Optimization and Related Indexing, Information Location Tools and Internet and Social Media Advertising Practices
10. Misappropriation of Trade Secrets in Cyberspace
11. Employer Rights in the Creation and Protection of Internet-Related Intellectual Property
12. Privacy and Publicity Rights of Celebrities and Others in Cyberspace
13. Idea Submission, Protection and Misappropriation

Part III. Licenses and Contracts

14. Documenting Internet Transactions: Introduction to Drafting License Agreements and Contracts
15. Drafting Agreements in Light of Model and Uniform Contract Laws: The Federal eSign Statute, Uniform Electronic Transactions Act, UCITA, and the EU Distance Selling Directive
16. Internet Licenses: Rights Subject to License and Limitations Imposed on Content, Access and Development
17. Licensing Pre-Existing Content for Use Online: Music, Literary Works, Video, Software and User Generated Content Licensing Pre-Existing Content
18. Drafting Internet Content and Development Licenses
19. Website Development and Hosting Agreements
20. Website Cross-Promotion and Cooperation: Co-Branding, Widget and Linking Agreements
21. Obtaining Assent in Cyberspace: Contract Formation for Click-Through and Other Unilateral Contracts
22. Structuring and Drafting Website Terms and Conditions
23. ISP Service Agreements

Volume 3

Chapter 24. Software as a Service: On-Demand, Rental and Application Service Provider Agreements

Part IV. Privacy, Security and Internet Advertising

25. Introduction to Consumer Protection in Cyberspace
26. Data Privacy
27. Cybersecurity: Information, Network and Data Security
28. Advertising in Cyberspace

Volume 4

Chapter 29. Email and Text Marketing, Spam and the Law of Unsolicited Commercial Email and Text Messaging
30. Online Gambling

Part V. The Conduct and Regulation of Internet Commerce

31. Online Financial Transactions and Payment Mechanisms
32. Online Securities Law
33. State and Local Sales and Use Taxes on Internet and Mobile Transactions
34. Antitrust Restrictions on Technology Companies and Electronic Commerce
35. Dormant Commerce Clause and Other Federal Law Restrictions on State and Local Regulation of the Internet
36. Best Practices for U.S. Companies in Evaluating Global E-Commerce Regulations and Operating Internationally

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

37. Defamation, Torts and the Good Samaritan Exemption (47 U.S.C.A. § 230)
38. Tort and Related Liability for Hacking, Cracking, Computer Viruses, Disabling Devices and Other Network Disruptions
39. E-Commerce and the Rights of Free Speech, Press and Expression in Cyberspace

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

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

Part VIII. Theft of Digital Information and Related Internet Crimes

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

Volume 5

Chapter 46. Identity Theft
47. Civil Remedies for Unlawful Seizures

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

48. Assessing and Limiting Liability Through Policies, Procedures and Website Audits
49. Content Moderation and Platform Liability: Service Provider and Website, Mobile App, Network and Cloud Provider Exposure for User Generated Content and Misconduct
50. Cloud, Mobile and Internet Service Provider Compliance with Subpoenas and Court Orders
51. Web 2.0 Applications: Social Networks, Blogs, Wiki and UGC Sites

Part X. Civil Jurisdiction and Litigation

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

"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 Los Angeles and Washington, DC offices. He defends data privacy, cybersecurity breach, AdTech, TCPA, and other Internet and mobile class action suits and litigates copyright, trademark, patent, trade secret, right of publicity, database, AI 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 in every year the list has been published (2009-2021), 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 2022, 2021, 2020, 2019, 2018, 2016 and 2013 editions of *The Best Lawyers in America* and is listed in Legal 500 U.S., Law Dragon and Chambers and Partners USA Guide. 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).

Mr. Ballon is also 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.lanBallon.net).

He may be contacted at BALLON@GTLAW.COM and followed on Twitter and LinkedIn (@lanBallon).

Contributing authors: Parry Aftab, Darren Abernethy, Viola Bensinger, Ed Chansky, Francoise Gilbert, Rebekah Guyon, Tucker McCrady, Josh Raskin, & Tom Smedinghoff.

NEW AND IMPORTANT FEATURES FOR 2022

- **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)
- **How *TransUnion v. Ramirez* (2021) changes the law of standing in cybersecurty breach, data privacy, AdTech and TCPA class action suits.**
- **90+ page exhaustive analysis of the CCPA and CPRA, all statutory amendments and final regulations, and how the law will change under the CPRA – the most comprehensive analysis available!** (ch 37)
- **Text and other mobile marketing under the TCPA following the U.S. Supreme Court's ruling in *Facebook, Inc. v. Duguid,* 141 S. Ct. 1163 (2021) – and continuing pitfalls companies should avoid to limit exposure**
- **Software copyrightability and fair use in light of the U.S. Supreme Court's 2021 decision in *Google LLC v. Oracle America, Inc.*, 141 S. Ct. 1183 (2021)** (ch 4)
- **Rethinking 20 years of database and screen scraping case law in light of the U.S. Supreme Court's opinion in *Van Buren v. United States,* 141 S. Ct. 1648 (2021)** (ch5)
- **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)
- **Virginia, Colorado and Nevada privacy laws** (ch 26)
- Applying **the single publication rule** to websites, links and uses on social media (chapter 37)
- **Digital economy litigation strategies**
- **Circuit-by-circuit, claim-by-claim analysis of CDA opinions**
- **How new Copyright Claims Board proceedings will disrupt DMCA compliance for copyright owners, service providers and users** (ch 4)
- **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)
- 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)
- **AdTech law** (chapter 28, Darren Abernethy)
- **The risks of being bound by the CASE Act's ostensibly *voluntary* jurisdiction over small copyright cases**
- **Rethinking approaches to consumer arbitration clauses in light of mass arbitration and case law on representative actions.**
- **Dormant Commerce Clause challenges to state privacy and other laws – explained**
- **First Amendment protections and restrictions on social media posts and the digital economy – important new case law**
- **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)
- **Idea protection & misappropriation** (ch 13)
- Revisiting **links, embedded links, sponsored links, and SEO/SEM practices and liability** (chapter 9)
- **eSIGN case law** (chapter 15)

SAVE 20% NOW!! To order call 1-888-728-7677
or visit lanBallon.net
enter promo code WPD20 at checkout

List Price: $3,337.00
Discounted Price: $2,669.60