AN A.S. PRATT PUBLICATION
FEBRUARY/MARCH 2021
VOL. 7 • NO. 2

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 7 **NUMBER 2** **February/March 2021**

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at 908-673-3380
Email: ..... Deneil.C.Targowski@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3385
Fax Number ..... (800) 828-8341
Customer Service Web site ..... http://www.lexisnexis.com/custserv/
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (937) 247-0293

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY &CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [5] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [245] (LexisNexis A.S. Pratt)

An A.S. Pratt Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2021–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 646.539.8300. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report*, LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

The California Privacy Rights Act of 2020: CCPA Redux

By Lisa J. Sotto and Danielle Dobrusin*

The California Privacy Rights Act of 2020 ballot initiative was approved by voters. The authors of this article discuss the Act, which significantly amends and expands upon the California Consumer Privacy Act of 2018, creating new compliance obligations for businesses subject to the law.

California voters approved Proposition 24, the California Privacy Rights Act of 2020 (the "CPRA"), on this past Election Day.[1] The CPRA ballot initiative was championed by Californians for Consumer Privacy, the group behind the proposed 2018 ballot initiative that coerced the California legislature into passing the groundbreaking California Consumer Privacy Act of 2018 (the "CCPA").[2] The CPRA significantly amends and expands upon the CCPA, creating new compliance obligations for businesses subject to the law.

Most of the CPRA's substantive provisions will become operative on January 1, 2023, and will apply to personal information collected after January 1, 2022.[3] A few of the CPRA's provisions become operative upon the law's effective date,[4] including:

- *An Extension of the HR and B2B Exemptions*: The CPRA extends, until January 1, 2023, existing exemptions for certain personal information obtained in the HR[5] and business-to-business contexts.[6]
- *Establishment of the California Privacy Protection Agency*: The CPRA establishes the California Privacy Protection Agency ("CPPA"), which will be responsible for enforcing and implementing the CCPA/CPRA and imposing administrative fines.[7]

---

* Lisa J. Sotto chairs Hunton Andrews Kurth LLP's Global Privacy and Cybersecurity practice and is a partner in the firm. She can be reached at lsotto@huntonak.com. Danielle Dobrusin is an associate in the firm's New York office, and can be reached at ddobrusin@huntonak.com.

[1] Prop. 24: 19-0021A1, The California Privacy Rights Act of 2020, Version 3 (2020), https://oag.ca.gov/system/files/initiatives/pdfs/19-0021A1%20%28Consumer%20Privacy%20-%20Version%203%29_1.pdf (last visited Dec. 3, 2020).

[2] Alastair Mactaggart, *A Letter from Alastair Mactaggart, Board Chair and Founder of Californians for Consumer Privacy*, Californians for Consumer Privacy, https://www.caprivacy.org/a-letter-from-alastair-mactaggart-board-chair-and-founder-of-californians-for-consumer-privacy/ (last visited Dec. 3, 2020).

[3] Prop. 24: The California Privacy Rights Act of 2020, Sec. 31(a).

[4] Prop. 24: The California Privacy Rights Act of 2020, Sec. 31(b). In accordance with subdivision (a) of section 10 of article II of the California Constitution, the CPRA will take effect on the fifth day after the Secretary of State files the statement of the vote for the November 3, 2020 election.

[5] Prop. 24: The California Privacy Rights Act of 2020, Sec. 15, 1798.145(m)(4).

[6] Prop. 24: The California Privacy Rights Act of 2020, Sec. 15, 1798.145(n)(3).

[7] Prop. 24: The California Privacy Rights Act of 2020, Sec. 24, 1798.199.

- *Authority for Expanded Regulations*: The CPRA requires new regulations to be issued on a variety of topics (e.g., cybersecurity audits and risk assessments and automated decision-making and profiling).[8] While the California Attorney General may begin the rulemaking process, the CPRA's rulemaking authority transfers to the CPPA beginning the later of July 1, 2021 or six months after the CPPA notifies the Attorney General that it is prepared to begin rulemaking.[9]

KEY CHANGES UNDER THE CPRA

Key provisions and changes under the CPRA include:

1. **Applicability:** Most of the law's obligations apply to a "business," which is defined to mean any for-profit organization that (1) does business in the state of California; (2) collects consumers' (i.e., California residents') personal information, or on whose behalf the information is collected, and that alone, or jointly with others, "determines the purposes and means" of the processing of consumers' personal information; and (3) satisfies one or more of the following thresholds: (a) as of January 1 of each calendar year, had annual gross revenues in excess of $25 million in the preceding calendar year, (b) alone or in combination, annually buys, sells, or shares (as the term "shared" is defined below), the personal information of 100,000[10] or more consumers or devices, or (c) derives 50 percent or more of its annual revenues from selling or sharing California consumers' personal information.[11]

   The law also applies to any entity that controls or is controlled by and shares common branding with a business that meets the thresholds described above.[12] While this type of structure existed under the CCPA,[13] the CPRA provides one additional criterion: the primary business also must "share" consumers' personal information with the secondary business. The CPRA narrowly defines the term "share" to mean only the sharing of personal information for "cross-context behavioral advertising" purposes.[14] This change may be problematic for companies that previously relied on the CCPA's provisions to classify intra-company transfers of personal information between entities that share common branding as disclosures within the same "business."

---

[8] Prop. 24: The California Privacy Rights Act of 2020, Sec. 21, 1798.185.

[9] Prop. 24: The California Privacy Rights Act of 2020, Sec. 21, 1798.185(d).

[10] This threshold increased from 50,000 under the CCPA. Prop. 24: The California Privacy Rights Act of 2020, Sec. 14, 1798.140(d)(1)(B).

[11] Prop. 24: The California Privacy Rights Act of 2020, Sec. 14, 1798.140(d)(1).

[12] Prop. 24: The California Privacy Rights Act of 2020, Sec. 14, 1798.140(d)(2).

[13] Cal. Civ. Code §1798.140(c)(2).

[14] Prop. 24: The California Privacy Rights Act of 2020, Sec. 14, 1798.140(ah)(1).

In addition, the CPRA also applies to (1) a joint venture or partnership in which each business has at least a 40 percent interest, and (2) any person that does business in California and that voluntarily certifies to the CPPA that it is in compliance with and agrees to be bound by the CPRA.

2. **Sensitive Personal Information:** The CPRA establishes a new category of "sensitive personal information," which means:

   - A Social Security, driver's license, state identification card, or passport number;
   - A consumer's account log-in or 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;
   - Precise geolocation;
   - Racial or ethnic origin, religious or philosophical beliefs, or union membership;
   - The contents of a consumer's mail, email or text messages, unless the business is the intended recipient of the communication;
   - Genetic data;
   - The processing of biometric information for the purpose of uniquely identifying a consumer; and
   - Personal information collected and analyzed concerning a consumer's health, sex life or sexual orientation.[15]

Notably, the CPRA grants consumers the right to limit a business's use and disclosure of sensitive personal information to the extent the information is used to infer characteristics about the consumer.[16] In that case, a consumer can direct the business to limit its use of the consumer's personal information to (1) that which is necessary to perform the services or provide the goods reasonably expected by an average consumer who requests such goods or services; (2) to provide certain specified services; or (3) as otherwise authorized by forthcoming implementing regulations.[17]

3. **Right to Correction:** The CPRA grants California consumers the right to request the correction of their personal information if the information is inaccurate.[18]

[15] Prop. 24: The California Privacy Rights Act of 2020, Sec. 14, 1798.140(ae).
[16] Prop. 24: The California Privacy Rights Act of 2020, Sec. 10, 1798.121.
[17] *Id.*
[18] Prop. 24: The California Privacy Rights Act of 2020, Sec. 6, 1798.106(a).

Upon a verifiable consumer request, a business must use "commercially reasonable efforts to correct the inaccurate personal information."[19]

4. **Opt Out of Sharing:** The CPRA adds "sharing" as a defined term, which specifically addresses sharing personal information with a third party "for cross-context behavioral advertising."[20] Consumers will have the right to opt out of sharing. In essence, the "right to opt out of selling" under the CCPA becomes the "right to opt out of selling and sharing."[21]

   The CPRA also expands the CCPA's requirement that a business obtain opt-in consent to sell a consumer's personal information if the business has actual knowledge that the consumer is under the age of 16.[22] Under the CPRA, the opt-in requirement also will apply to instances where a business has actual knowledge that it "shares" personal information of a minor under 16.[23]

5. **Privacy Notices:** The CPRA will require businesses to provide certain disclosures in addition to the highly prescriptive language currently required by the CCPA. For example, a business will need to provide notice, at or before the point of collection, of the length of time it intends to retain each category of personal information, including sensitive personal information, or if that is not possible, the criteria used to determine the retention period.[24] A business also will need to provide notice regarding its processing of sensitive personal information, including the categories of sensitive personal information to be collected, the purposes for which the information is collected or used, and whether such information is sold or shared.[25]

   In addition, a business's privacy policy must include a description of all consumer rights under the law, including the new rights granted by the CPRA (i.e., the right of correction, the right to opt-out of sharing, and the right to limit use of sensitive personal information).[26]

---

[19] Prop. 24: The California Privacy Rights Act of 2020, Sec. 6, 1798.106(c).

[20] Prop. 24: The California Privacy Rights Act of 2020, Sec. 14, 1798.140(ah)(1). "Cross-context behavioral advertising" is defined as "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." Prop. 24: The California Privacy Rights Act of 2020, Sec. 14, 1798.140(k).

[21] Prop. 24: The California Privacy Rights Act of 2020, Sec. 9, 1798.120.

[22] Cal. Civ. Code §1798.120(c).

[23] Prop. 24: The California Privacy Rights Act of 2020, Sec. 9, 1798.120(c).

[24] Prop. 24: The California Privacy Rights Act of 2020, Sec. 4, 1798.100(a)(3).

[25] Prop. 24: The California Privacy Rights Act of 2020, Sec. 4, 1798.100(a)(2).

[26] Prop. 24: The California Privacy Rights Act of 2020, Sec. 12, 1798.130(a)(5)(A).

6. **Necessity/Proportionality Concept:** Under the CPRA, a business's collection, use, retention and sharing of a consumer's personal information must be reasonably necessary and proportionate to achieve the purposes for which the information was collected or processed, or for another disclosed purpose that is compatible with the context in which the information was collected.[27]

7. **Service Provider, Contractor and Third-Party Contracts:** The CPRA clarifies that a service provider or contractor is not a third party, a point which, due to muddled language, caused confusion under the CCPA.[28] Notably, the CPRA requires that businesses enter into written contracts with service providers, contractors and third parties (collectively, "Recipients"), and those contracts must contain required provisions.[29] Specifically, all contracts with Recipients must:

   - Specify that the personal information is sold or disclosed by the business only for limited and specified purposes;
   - Obligate the Recipient to comply with applicable obligations under the CPRA and provide the same level of privacy protection required by the CPRA;
   - Grant the business rights to take reasonable and appropriate steps to help to ensure that the Recipient uses the personal information transferred in a manner consistent with the business's obligations under the CPRA;
   - Require the Recipient to notify the business if it determines that it can no longer meet its obligations under the CPRA; and
   - Grant the business the right, upon notice, to take reasonable and appropriate steps to stop and remediate unauthorized use of personal information.[30]

   Additional provisions are required for agreements with service providers and contractors.[31]

8. **Audits and Risk Assessments:** Pursuant to forthcoming regulations, businesses whose processing of personal information presents a significant risk to consumers' privacy or security will be required to (1) perform a cybersecurity

[27] Prop. 24: The California Privacy Rights Act of 2020, Sec. 4, 1798.100(c).

[28] Prop. 24: The California Privacy Rights Act of 2020, Sec. 14, 1798.140(ai).

[29] Prop. 24: The California Privacy Rights Act of 2020, Sec. 4, 1798.100(d); Sec. 14, 1798.140(j) and (ag).

[30] Prop. 24: The California Privacy Rights Act of 2020, Sec. 4, 1798.100(d).

[31] Prop. 24: The California Privacy Rights Act of 2020, Sec. 14, 1798.140(j) and (ag).

audit on an annual basis, and (2) submit to the CPPA on a regular basis a risk assessment with respect to their processing of personal information.[32]

9. **Automated Decision-Making and Profiling:** Forthcoming regulations will be issued to govern access and opt-out rights with respect to businesses' use of automated decision-making technology, including profiling.[33] The regulations will require a business's response to a consumer's access request to provide meaningful information about the logic involved in automated decision-making processes, as well as a description of the likely outcome of the process with respect to the consumer.[34]

10. **Data Breach Liability:** The CPRA extends the CCPA's limited private right of action to certain data breaches involving a consumer's email address in combination with a password or security question and answer that would permit access to the consumer's account.[35] The CPRA also retains the 30-day cure period for actions brought against a business for statutory damages and clarifies that "[t]he implementation and maintenance of reasonable security procedures and practices . . . following a breach does not constitute a cure with respect to that breach."[36]

11. **Enforcement:** As previously discussed, the CPRA establishes the CPPA, which will be responsible for enforcing and implementing the CCPA/CPRA and imposing administrative fines.[37] Establishment of a dedicated privacy agency could result in more enforcement resources than are currently available to the California Attorney General, who presently is tasked with enforcing the CCPA.

    Importantly, the CPRA removes the mandatory 30-day cure period that currently exists under the CCPA with respect to enforcement actions.[38] The cure period provided some peace of mind to companies struggling to understand the confusing and untested language of the CCPA. Under the CPRA, the CPPA will have discretion in determining whether to investigate a complaint or provide a business with a specified period of time in which to cure an alleged violation.[39] In making such a determination, the CPPA may consider (1) the alleged offender's

[32] Prop. 24: The California Privacy Rights Act of 2020, Sec. 21, 1798.185(a)(15).
[33] Prop. 24: The California Privacy Rights Act of 2020, Sec. 21, 1798.185(a)(16).
[34] *Id.*
[35] Prop. 24: The California Privacy Rights Act of 2020, Sec. 16, 1798.150(a)(1).
[36] Prop. 24: The California Privacy Rights Act of 2020, Sec. 16, 1798.150(b).
[37] Prop. 24: The California Privacy Rights Act of 2020, Sec. 24, 1798.199.
[38] Cal. Civ. Code §1798.15(b).
[39] Prop. 24: The California Privacy Rights Act of 2020, Sec. 24, 1798.199.45.

lack of intent to violate the CPRA, and (2) voluntary efforts to cure the alleged violation prior to being notified by the CPPA of the complaint.[40]

CONCLUSION

The CPRA significantly changes and expands the obligations imposed on businesses subject to the law. Moreover, forthcoming regulations undoubtedly will bring new developments and clarifications.

Businesses would be well advised to closely examine their CCPA compliance programs to identify the actions needed to comply with the CPRA prior to January 1, 2023.

[40] *Id.*