AN A.S. PRATT PUBLICATION
NOVEMBER-DECEMBER 2020
VOL. 6 • NO. 9

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 6 NUMBER 9 NOVEMBER - DECEMBER 2020

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)

This publication is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If legal advice or other expert assistance is required, the services of a competent professional should be sought.
LexisNexis and the Knowledge Burst logo are registered trademarks of Reed Elsevier Properties Inc., used under license.A.S. Pratt is a trademark of Reed Elsevier Properties SA, used under license.

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

(2020–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 Has Passed: What's In It?

By Brandon P. Reilly and Scott T. Lashway [*]

The California Privacy Rights Act ("CPRA") expands the recently operative California Consumer Privacy Act and moves California's privacy regime toward that of the EU General Data Protection Regulation. This article highlights certain immediate considerations following the CPRA's approval.

On Election Day, Californians voted to approve Proposition 24, a ballot measure that creates the California Privacy Rights Act ("CPRA"). The CPRA amends and expands the California Consumer Privacy Act ("CCPA") – California's current privacy law that itself is nearly brand new. If you are left wondering what it all means for privacy regulation in California and beyond, you are not alone. This article highlights certain immediate considerations following the CPRA's approval.

1. HOW DID THE CPRA BECOME LAW?

Because Proposition 24 was passed by Californians in the General Election, the CPRA becomes state law. While we address below when action is needed (answer = now), let us note how California got here again. California is notorious for its ballot proposition system, which is unique for its breadth and the costs involved in supporting an initiative in the nation's most populous state. The system allows advocates to bypass traditional legislative mechanisms as well as stakeholders in government and industry and, if they are successful, it can result in laws more insulated from legislative revision without subsequent voter approval.

This is not the first time the group behind the CPRA successfully pursued a privacy measure for the California ballot. In June 2018, Californians for Consumer Privacy had initially gathered enough signatures to qualify the Consumer Right to Privacy Act of 2018 for the November 2018 ballot. In response, the California Legislature negotiated the withdrawal of the initiative from the ballot in exchange for passage of the CCPA, which is a slightly less restrictive version of its predecessor initiative.

The group spearheading the original initiative, however, was not satisfied with the CCPA, which was already the nation's most robust consumer-focused privacy law. The

[*] Brandon P. Reilly is a privacy and data security partner and civil litigator in the Orange County office of Manatt, Phelps & Phillips, LLP, counseling clients on a wide array of consumer protection and privacy matters, including data privacy and security compliance and procedure and data breach response. Based in the firm's Boston office, Scott Lashway, co-leader of the firm's privacy and data security group, focuses his practice on matters involving the intersection of law and technology. The authors may be contacted at breilly@manatt.com and slashway@manatt.com, respectively.

group's founder, Alastair Mactaggart, has expressed frustration over what he perceived were industry efforts to weaken the CCPA through amendments and has pursued a second ballot measure to address his concerns.

2. WHAT ARE THE EFFECTS OF THE CPRA'S PASSAGE?

The CPRA becomes a baseline for California consumer privacy law absent a subsequent ballot measure to repeal it, because it requires that any amendments be "consistent with and further the purpose and intent of this Act."

In other words, if Sacramento lawmakers ever passed a CPRA amendment that is even arguably privacy restrictive, privacy advocates and other Californians may sue to attempt to repeal that amendment. Other ways to modify the CPRA include through a subsequent ballot measure or if the federal government or a federal court invalidates the law via a pre-emptive federal privacy law or a ruling of unconstitutionality.

3. WHEN WOULD THE CPRA BECOME EFFECTIVE?

Most of the CPRA's substantive provisions will not take effect until January 1, 2023, providing covered businesses with two years of valuable ramp-up time. The CPRA authorizes the rulemaking process to begin during that same period. Notably, however, the CPRA's expansion of the "Right to Know" impacts personal information ("PI") collected during the ramp-up period, on or after January 1, 2022. Businesses must still comply with the CCPA and any regulations in the meantime.

The CPRA immediately extends the current limited CCPA exemption for employment and business-to-business data until January 1, 2023.

4. HOW DOES THE CPRA COMPARE WITH THE CCPA?

The CPRA augments and expands the CCPA in many ways. We break down notable changes by topic below.

New Criteria for Which Businesses are Regulated

The CPRA modifies the definition of a covered "business" in notable ways that both increase and decrease the number of businesses currently subject to the CCPA:

- Doubles the CCPA's threshold number of consumers or households from 50,000 to 100,000, resulting in reduced applicability of the law to small and midsize businesses.
- Expands applicability to businesses that generate most of their revenue from sharing PI, not just selling it, which is defined as "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." "Making available" is noteworthy, particularly for its vagueness and breadth.

- Extends the definition to joint ventures or partnerships composed of businesses that each have at least a 40 percent interest.

What's Changed?	
CCPA	**CPRA**
(1) Has $25+ million in annual revenue; (2) Buys or sells, or receives or shares for business's *commercial purpose*, PI of *50,000+ consumers, households or devices*; or (3) Derives at least 50 percent of annual revenue from selling consumer PI.	(1) Has $25+ million in annual revenue; (2) Buys, sells, or shares PI of *100,000+ consumers or households*; or (3) Derives at least 50 percent of annual revenue from selling *or sharing* consumer PI.

New Category of "Sensitive Personal Information"

The CPRA introduces "sensitive personal information" as a new regulated dataset in California. The category is subject to new disclosure and purpose limitation requirements, and consumers have new rights designed to limit businesses' use of their sensitive PI. Sensitive PI includes:

- Government identifiers (such as Social Security numbers and driver's licenses);
- Financial account and login information (such as credit or debit card number together with login credentials);
- Precise geolocation;
- Race, ethnicity, religious or philosophical beliefs, or union membership;
- Content of nonpublic communications (mail, email, and text messages);
- Genetic data;
- Biometric or health information; and
- Sex life or sexual orientation information.

What's Changed?	
CCPA	**CPRA**
Implicitly includes sensitive PI in broader regulated dataset, but does not impose separate requirements and prohibitions for sensitive PI (other than increased verification requirements).	Imposes separate requirements and restrictions on sensitive PI: • Disclosure requirements • Opt-out requirements for use and disclosure • Opt-in consent standard for use and disclosure • Purpose limitation requirements

New and Expanded Consumer Privacy Rights

The CPRA provides for new rights and amends existing rights.

Brand-New Rights

- *Right to Correction*. Consumers may request any correction of their PI held by a business if that information is inaccurate.
- *Right to Opt Out of Automated Decision Making Technology*. The CPRA authorizes regulations allowing consumers to opt out of the use of automated decision making technology, including "profiling," in connection with decisions related to a consumer's work performance, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.
- *Right to Access Information About Automated Decision Making*. The CPRA authorizes regulations allowing consumers to make access requests seeking meaningful information about the logic involved in the decision making processes and a description of the likely outcome based on that process.
- *Right to Restrict Sensitive PI*. Consumers may limit the use and disclosure of sensitive PI for certain secondary purposes, including prohibiting businesses from disclosing sensitive PI to third parties, subject to certain exemptions.
- *Audit Obligations*. The CPRA authorizes regulations that will require mandatory risk assessments and cybersecurity audits for high-risk activities. The risk assessments must be submitted to the newly established California Privacy Protection Agency (see below) on a "regular basis."

Modified Rights

- *Modified Right to Delete*. Businesses are now required to notify third parties to delete any consumer PI bought or received, subject to some exceptions.
- *Expanded Right to Know*. The PI that must be reflected in a “Right to Know” response is expanded to include, for valid requests, PI collected beyond the prior 12 months, if collected after January 1, 2022.
- *Expanded Right to Opt Out*. The CCPA already grants consumers the right to opt out of the sale of their PI to third parties, which implicitly includes sensitive PI; however, the opt-out right now covers “sharing” of PI for cross-context behavioral advertising as outlined below.
- *Strengthened Opt-In Rights for Minors*. Extends the opt-in right to explicitly include the sharing of PI for behavioral advertising purposes. As with the opt-out right, businesses must wait 12 months before asking a minor for consent to sell or share his or her PI after the minor has declined to provide it.
- *Expanded Right to Data Portability*. Consumers may request that the business transmit specific pieces of PI to another entity, to the extent it is technically feasible for the business to provide the PI in a structured, commonly used and machine-readable format.

What’s Changed?	
CCPA	**CPRA**
• Right to Know • Right to Delete • Right to Opt Out of Third-Party Sales • Right to Nondiscrimination	• Right to Know • Right to Delete • Right to Opt Out of Third-Party Sales *and Sharing* • *Right to Limit Use and Disclosure of Sensitive PI* • *Right to Correction* • *Right to Access Information About Automated Decision Making* • *Right to Opt Out of Automated Decision Making Technology* • Right to Nondiscrimination

Directly Regulates the Sharing of PI for Cross-Context Behavioral Advertising

In an attempt to explicitly regulate digital advertising, the CPRA distinguishes between two types of advertising: "cross-context behavioral advertising" and "non-personalized advertising." The sharing of PI for cross-context behavioral advertising is subject to the Right to Opt Out, whereas the use of PI (apart from precise geolocation) for non-personalized, first-party advertising is not and is instead designated as internal "business purpose." These newly defined terms solidify a current interpretation of the CCPA that the Right to Opt Out extends to certain behavioral advertising practices. Business that were already operating under this interpretation likely do not need to heavily modify their compliance programs.

What's Changed?	
CCPA	**CPRA**
Opt-out right restricts sharing of PI only for advertising purposes in exchange for money or other valuable consideration.	Opt-out right explicitly extends to PI used for cross-context behavioral advertising, which may or may not involve an exchange for money or other valuable consideration.

Creates a New Privacy Enforcement Authority

The General Data Protection Regulation ("GDPR") utilizes a network of Data Protection Authorities for each member state to enforce the law. Similar authorities dedicated to the enforcement of privacy law are absent from the federal and California governments; instead, the CCPA is currently enforced by the California Office of the Attorney General ("OAG"). The CPRA restructures this enforcement apparatus by establishing the California Privacy Protection Agency ("CPPA") and granting it investigative, enforcement and rulemaking powers. Most notably, the CPRA removes the 30-day cure period that businesses currently enjoy under the CCPA after being formally notified by the OAG of an alleged violation. The CPRA also triples the maximum penalties to $7,500 for violations concerning minors.

Adopts Certain GDPR Principles

The CPRA codifies the concepts of data minimization, purpose limitation and storage limitation – all principles currently enforced in Europe through the GDPR.

- *Data minimization*. A business's collection, use, retention and sharing of PI must be minimized to what is reasonably necessary and proportionate to achieve the purpose of collection or processing or for another disclosed purpose that is compatible with the context of collection; the processing must not be subject to processing for incompatible, undisclosed purposes.

- *Purpose limitation*. Businesses must not collect or use PI for a new purpose that is incompatible with previously disclosed purposes without first providing consumer notice.
- *Storage limitation*. Businesses must disclose, at the time of collection, their retention periods for each category of PI (or if that is not possible, the criteria used to determine such period). Businesses are further prohibited from retaining PI for longer than is "reasonably necessary" for each disclosed purpose.

Most consequentially, the CPRA brings data minimization and data retention requirements into the realm of direct liability by appearing to authorize the state regulator to enforce regulations regarding the failure to reasonably minimize data or retain PI for no longer than reasonably necessary, even if such failure does not lead to further CPRA violations. The CPRA's purpose and storage limitations, by contrast, appear to be more indirectly enforceable as a failure to properly disclose such practices in a privacy policy or notice at collection.

Service Providers and Contractors

The CPRA amends the definition of "service provider" and introduces "contractors," a new category of recipients of PI who process PI made available to them by businesses pursuant to a written contract. The CPRA imposes the same contractual and direct obligations on contractors that it otherwise imposes on service providers, and also requires contractors to certify that they understand and will comply with such contractual obligations.

Here are the materially new obligations and prohibitions the CPRA imposes on service providers and contractors:

- Requires service providers and contractors to notify businesses of any engagement with a sub-service provider or subcontractor and to bind those parties to the same written contract that is otherwise arranged between businesses and service providers.
- Directly obligates service providers and contractors to cooperate with and assist businesses in responding to privacy rights requests.
- Clarifies that businesses must contractually prohibit service providers and contractors from combining any PI received from the business with PI from other sources or collected on its own behalf (subject to exceptions).

Employee and B2B Exemptions

The CPRA extends the employee and business-to-business ("B2B") exemption to January 1, 2023, allowing two years for the California Legislature to address employee and B2B privacy questions in a separate bill. It is possible, however, that subsequent attempts by the California Legislature to further extend the exemptions beyond 2023 could be challenged by consumer advocates by arguing that such an amendment is not "consistent with and further[ing] the purpose and intent of [the CPRA]." The success of such a challenge is debatable, particularly in light of the CPRA's stated intent to treat employee and B2B PI differently than consumer PI.

What's Changed?	
CCPA	**CPRA**
Exemptions sunset January 1, 2022, but may be subsequently extended by legislature.	Exemptions permanently sunset January 1, 2023.

New Consent Standard

The CPRA also fleshes out the "consent" standard, bringing it closer to the strict standard utilized in Europe. The consent standard, however, is used only in the following relatively marginal scenarios, some of which already required consent under the CCPA:

- Consenting to the sale or sharing of PI after an opt-out;
- Minor opt-in consent for sale and sharing of PI;
- Consenting to secondary use and disclosure of sensitive PI after an opt-out;
- The research exemptions; and
- Opt-in consent for financial incentive programs.

Data Breaches and Private Right of Action

The CPRA does not explicitly attempt to alter the CCPA's existing private right of action for data breaches; however, the CPRA does add consumer login credentials to the list of data types that can be actionable under the law if breached.

TIMELINE

The CPRA's timeline over the next three years is complex, with several dates fixed on contingent events. Here are the basics:

- *November Certification Date* – Secretary of State certifies election results.
- *November Certification Date + Five Days* – Employment and B2B exemptions extended; certain provisions authorizing the CPPA go into effect.
- *January 1, 2021* – CPRA becomes operative, effectively blocking any subsequent and conflicting privacy legislation.
- *On or About July 1, 2021* – Rulemaking process commences (or later if it has not yet been six months since CPPA formally notified OAG).
- *January 1, 2022* – 12-month lookback period for collected data commences.
- *July 1, 2022* – Deadline for CPPA to adopt final regulations.
- *January 1, 2023* – CPRA becomes fully operative; employment and B2B exemptions expire, and those datasets become fully regulated by the CPRA.
- *July 1, 2023* – CPRA becomes fully enforceable by the CPPA.