AN A.S. PRATT PUBLICATION
FEBRUARY-MARCH 2023
VOL. 9 NO. 2

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 9 **NUMBER 2** **February-March 2023**

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Alexandra Jefferies at ..... (937) 560-3067
Email: ..... alexandra.jefferies@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*, [1] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [82] (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

(2023–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, 631.291.5541. 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.

Preparing for Today, and for the Future, in California

By Devika Kornbacher*

The author provides insights into new privacy developments in California and strategies for compliance, including Frequently Asked Questions.

A flurry of activity in California means big changes this year for data privacy. New obligations, an expanded scope of covered data, increasing enforcement, and scant regulations all mean it is a good time for companies processing the personal information of California residents to make sure they are prepared for the new year. Read ahead for insights into new privacy developments and strategies for compliance, including Frequently Asked Questions.

KEY CCPA EXEMPTIONS THAT EXPIRED IN JANUARY 2023

Upon becoming effective in 2020, the California Consumer Privacy Act (CCPA)[1] temporarily exempted covered entities from complying with most of the CCPA's requirements with respect to personal information related to workforce members and B2B communications. These exemptions lasted until January 1, 2023. Many expected the exemptions to be renewed, but despite many attempts, legislators were unsuccessful, and the legislative session ended in August without any action. This means companies should already have expanded (or created) their compliance program to cover employee and B2B data.

What Types of Personal Information Fall Under the Employee and B2B Exemptions?

The employee exemption covers the personal information of California job applicants, employees, owners, directors, officers, and medical staff members, as defined in the statute, collected and used by businesses in the context of an individual's role, for emergency contact information, or to provide benefits. Until 2023, the law exempted this data from most CCPA obligations, but at collection employers are still required to provide a notice to their employees explaining what information is being collected and its intended use.

The B2B exemption covers personal information reflecting a written or verbal communication or transaction between a covered business and an employee, owner, director, officer, or independent contractor, of another business, which occurs within the

* Devika Kornbacher, a partner in the New York office of Clifford Chance and co-head of the firm's Tech Group, represents clients in fields such as software, hardware, sports, aviation, and retail.

[1] https://oag.ca.gov/privacy/ccpa.

context of conducting due diligence or providing or receiving a product or service. Until 2023, the law only required B2B data to be subject to the statute's personal information sales opt-out and opt-in rights, non-discrimination obligations, and private right of action for data breaches.

These exemptions expired on January 1, 2023; now, this data is subject to all aspects of the CCPA, as amended by the California Privacy Rights Act (CPRA), just like any other personal information of California residents.

FAQ 1: How Can Companies Prepare to Comply with the Expanded Scope of the CCPA and CPRA?

Companies that already are compliant with the CCPA should have many of their processes and policies in place; their main tasks will be to update their notices, policies, and processes to include employee and B2B personal information (in addition to refreshing the policies to comply with the expanded requirements of the CPRA – see below). In particular, companies should consider how to handle employee data requests in light of employment laws and existing HR policies. Many companies are configuring their HR portal to permit employees to exercise their rights without requiring a separate request.

Meanwhile, global companies that must comply with the European Union's General Data Protection Regulation (GDPR) – which has none of these exemptions – can draw upon their experience handling this data under their GDPR policies and procedures.

Some steps to comply include:

- Conducting a thorough assessment of how employee (including applicants') and B2B personal information is currently collected, used, and disclosed, including what categories of personal information are involved and to what extent data minimization protocols should be put in place;
- Supplementing privacy notices to ensure they include information regarding data subject's rights with respect to this previously exempted information;
- Expanding existing policies and procedures regarding the retention of personal information and handling CPRA rights requests (right to know, delete, etc.) to incorporate employee and B2B-related requests; and
- Assessing contracts with relevant service providers and businesses which have access to employee and B2B data to ensure downstream compliance and, if applicable, the inclusion of clauses required for those businesses to remain service providers.

AGE-APPROPRIATE DESIGN LEGISLATION

Following in the footsteps of Europe's Age-Appropriate Design Code enacted in 2020, California enacted the California Age-Appropriate Design Code Act (CAADCA)[2] on September 15, 2022. Under the CAADCA, online platforms must "consider the best interests of children when designing, developing, and providing that online service, product, or feature." Businesses also must prioritize children's safety and well-being wherever there is a conflict between their commercial interests and the interests of children who access these platforms. The CAADCA is scheduled to come into force on July 1, 2024, although some obligations kick in earlier.

Who Is Covered by the Statute?

The CAADCA applies to any business that "provides an online service, product, or feature likely to be accessed by children" under the age of 18. Terms not defined in the legislation follow the CCPA's definitions, as amended by the CPRA. Therefore, "business" under the CAADCA has the same meaning as under the CCPA/CPRA, which includes any for-profit entity doing business in California that collects personal information of California residents and meets one or more specific thresholds defined by the statute.

The CAADCA provides several factors for determining whether a product, service, or feature is one that is "likely to be accessed by children," including:

- Whether it is directed to children as defined by the Children's Online Privacy Protection Act (COPPA, a federal children's privacy law);
- Whether it is determined to be routinely accessed by a significant number of children according to competent, reliable evidence;
- Whether its advertisements are marketed to children; and
- Whether it has design elements that are known to be interesting to children, including games, cartoons, music, and celebrities, that children enjoy.

FAQ 2: What Are Some of the Key Obligations Under The CAADCA?

The law imposes a set of obligations on covered businesses, including:

- *Data Impact Assessments*: Covered businesses must complete a "Data Protection Impact Assessment" before offering any new online service, product, or feature, to the public that is likely to be accessed by children.

[2] https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202120220AB2273.

The assessment should analyze and explore mitigations for any potential risk to children, such as whether algorithms used in a product or advertisements displayed could be harmful to children. These assessments must be made available within three business days of a request from the California Attorney General. Importantly, a Data Impact Assessment must be completed on or before the effective date of the CAADCA – July 1, 2024 – for any online service, product, or feature likely to be accessed by children and offered to the public before July 1, 2024 and after.

- *Default Privacy Settings*: All default privacy settings of online services, products, or features, provided to children must be configured in such a manner as to provide a high level of privacy, unless the business has a compelling reason that a different privacy setting is in the best interests of children.

- *Prominently and Easily Display Privacy Information*: All privacy policies, terms of service, and community standards information must be concise and prominently displayed with language suitable for the age of children likely to access the online program. Companies also must clearly notify children if their activity is being monitored or tracked, even if by a parent or guardian.

- *Various Restrictions to Keep Children Safe*: All covered businesses are prohibited from:

  (i.) Using personal information of children in a way that is detrimental to a child's well-being;

  (ii.) Profiling a child unless necessary to provide the online service or feature, or if the business has a compelling reason that that is in the best interests of the child;

  (iii.) Collecting, selling, or disclosing, precise geolocation data unless strictly necessary; and

  (iv.) Using dark patterns – a deceptive design pattern – to entice children to provide their personal information.

FAQ 3: How Will the CAADCA Be Enforced?

Any business that violates the CAADCA will be subject to an injunction and civil penalty of no more than $2,500 per affected child for each negligent violation and no more than $7,500 for each intentional violation. These enforcement actions may be brought by the California Attorney General.

CPRA OBLIGATIONS FINALLY COME INTO EFFECT

The new year brings other key changes to data protection in California, with many of the substantive provisions of the CPRA coming into effect, including:

- Expanding the definition of business to companies who derive over 50% of their annual revenues from "sharing" personal information;
- A new consumer right to correct inaccurate personal information;
- Definition (and limitations on use) of "sensitive" personal information;
- Expanded rights and obligations, including disclosure of retention limits, data and purpose limitation obligations, and reasonable security measure obligations; and
- Expanded contractual requirements for agreements with service providers and contractors.

Companies should take this opportunity to review their policies and procedures to ensure compliance with these expanded obligations. Because the CPRA regulations[3] have not been finalized, companies should also remain alert to communications from the California Office of the Attorney General and California Privacy Protection Agency (CPPA). For example, on October 17, 2022, the CPPA published proposed modifications[4] to the CPRA regulations that seek to clarify some of the key obligations. To receive notifications on CCPA and CPRA-related developments, sign up at the following url: https://oag.ca.gov/subscribe.

CONCLUSION

There is mounting evidence that enforcement of California privacy laws will increase in 2023. Recently, the California Attorney General issued its first monetary penalty for CCPA violations – a $1.2 million action against Sephora for noncompliance with obligations. Along with the penalty, the AG announced new enforcement sweeps, including against financial institutions and large consumer retailers. Meanwhile the state continues to build out its new privacy regulator, the California Privacy Protection Agency, complete with a $10 million/year operating budget. In addition, the mandatory 30-day cure period for noncompliance becomes discretionary in 2023 – meaning the CPPA or AG can go directly to enforcement if they determine that that is appropriate.

And that's just California! The Virginia CDPA now is in effect, with Colorado and Connecticut following, and with Utah's law taking effect at the end of 2023. With the looming specter of a comprehensive national privacy bill, it will be more important than ever for companies to have thorough data privacy and governance protocols in place.

---

[3] https://cppa.ca.gov/meetings/materials/20220608_item3.pdf.

[4] https://cppa.ca.gov/meetings/materials/20221021_22_item3_modtext.pdf.