AN A.S. PRATT PUBLICATION
JULY-AUGUST 2026
VOL. 12 NO. 6

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 12 **NUMBER 6** **July-August 2026**

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
LexisNexis® Support Center ..... https://supportcenter.lexisnexis.com/app/home
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (518) 487-3385

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*, [7] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [179] (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

(2026–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 opinions expressed are those of the author(s) and do not necessarily reflect the views of their employer, its clients, the editor(s), RELX, LexisNexis, Matthew Bender & Co., Inc, or any of its or their respective affiliates.

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

What Businesses Need to Know About Automated Decision-Making, Cybersecurity Audits and Risk Assessments Under the Amended CCPA Regulations

By Lei Shen, Stephen Lilley, Arsen Kourinian, Amber C. Thomson and Megan P. Von Klein*

In this article, the authors discuss three major new components introduced by amended regulations under the California Consumer Privacy Act.

The amended regulations from the California Privacy Protection Agency (CalPrivacy), which are now in effect, introduce three major new components:

(1) requirements for automated decision-making technology (ADMT);

(2) cybersecurity audits; and

(3) risk assessments for high-risk processing.

Together, these changes represent one of the most consequential expansions of the California Consumer Privacy Act (CCPA) to date, and for many businesses, compliance may require substantial new operational, technical, and governance work.

Businesses may need to consider taking the following actions, all on compressed timelines:

- Inventory and assess automated tools;
- Update consumer notices;
- Prepare for thorough and independent cybersecurity audits with subsequent executive-level certification of completion; and
- Prepare formal risk assessments.

This article offers a practical guide to these new requirements, their implications, and some potential steps businesses can consider taking now to help mitigate regulatory and enforcement risk.

---

* The authors, attorneys with Mayer Brown, may be contacted at lshen@mayerbrown.com, slilley@mayerbrown.com, akourinian@mayerbrown.com, athomson@mayerbrown.com and mvonklein@mayerbrown.com, respectively.

AUTOMATED DECISION-MAKING: EXPANDED TRANSPARENCY, CHOICE AND GOVERNANCE

The amended regulations add requirements for businesses that use ADMT to make "significant decisions." ADMT, which includes profiling, is defined as any technology that processes personal information and uses computation to replace human decision-making or substantially replace human decision-making. To avoid the ADMT decision substantially replacing human decision-making, the human reviewer must:

- Know how to interpret and use the technology's output to make the decision;
- Review and analyze the output of the technology, and any other information that is relevant to make or change the decision; and
- Have authority to make or change the decision based on their analysis.

These requirements apply if a business uses ADMT to make a "significant decision," which includes the provision or denial of any of the following:

- Financial or lending services, which means the extension of credit or a loan, transmitting or exchanging funds, the provision of deposit or checking accounts, check cashing, or installment payment plans.
- Housing, which includes any building, structure, or portion thereof that is used or occupied as, or designed, arranged, or intended to be used or occupied as, a home, residence, or sleeping place by one or more California residents, including for permanent or temporary occupancy.
- Education enrollment or opportunities, which means (a) admission or acceptance into academic or vocational programs; (b) educational credentials (e.g., a degree, diploma, or certification); and (c) suspension and expulsion.
- Employment or independent contractor opportunities or compensation, which means (a) hiring; (b) allocation or assignment of work for employees; or salary, hourly or per assignment compensation, incentive compensation such as a bonus, or another benefit; (c) promotion; and (d) demotion, suspension, and termination.
- Healthcare services, which means services related to the diagnosis, prevention, or treatment of human disease or impairment, or the assessment or care of an individual's health.

What's New and Why It Matters

Businesses that use ADMT to make significant decisions must provide California residents: (1) a notice before using ADMT; (2) an opportunity to opt-out of ADMT

decisions (subject to exceptions); and (3) a right to access information about the ADMT use. A business that uses ADMT for a significant decision prior to January 1, 2027, must be in compliance with these requirements by January 1, 2027. A business that uses ADMT on or after January 1, 2027, must be in compliance with these requirements any time it is using ADMT for a significant decision.

Potential Steps to Mitigate Risk

- *Map ADMT uses*. Inventory how the business uses ADMT, the decisions made using such technology, and the level of human involvement in such decisions to determine if the ADMT substantially replaced human decision-making.
- *Build consumer-facing content*. If the CCPA's ADMT requirements are triggered, prepare ADMT pre-use notices, intake mechanisms for receiving opt-out and access requests, a step-by-step playbook for processing such rights requests, and template responses to the requests.
- *Update contracting*. Draft ADMT-specific requirements in vendor agreements, such as a requirement for service providers to assist the business with its ADMT compliance obligations, as required under the new CCPA contractual provisions for service providers.

CYBERSECURITY AUDITS: FORMALIZING TECHNICAL SECURITY CONTROLS AND DOCUMENTATION

The amended regulations require businesses that process a sufficient volume of personal information of Californians to complete thorough and independent audits of their cybersecurity program. Specifically, the audit requirements apply if a business meets one of the following below:

- Derives 50% or more of its annual revenues from "selling" or "sharing" California residents' personal information (as such terms are defined in the CCPA);
- Processes the personal information of 250,000 or more California residents or households in a calendar year and has annual gross revenues in excess of $25 million (as adjusted over time); or
- Processes the sensitive personal information of 50,000 or more California residents in a calendar year and has annual gross revenues in excess of $25 million (as adjusted over time).

The regulations require the business to allow the auditor to determine which portions of a business's cybersecurity program—ranging from access controls to secure coding practices—will be subject to the audit and to provide access to all of the information

that the auditor requests as relevant to the cybersecurity audit. The audit must be independent and thorough, covering 18 separate cyber components that are detailed in the regulations. Relevant companies must complete the required audits annually and submit a certification of compliance to CalPrivacy that is signed, under penalty of perjury, by a member of the business's executive management team who is directly responsible for the business's cyber-audit compliance, has sufficient knowledge to provide accurate information, and has authority to submit the certification. This certification must, among other statements, represent that "the business has not made any attempt to influence the auditor's decisions or assessments regarding the cybersecurity audit." Businesses required to complete cybersecurity audits must submit certifications to CalPrivacy by: (1) April 1, 2028, if the business makes over $100 million; (2) April 1, 2029, if the business makes between $50 million and $100 million; or (3) April 1, 2030, if the business makes less than $50 million.

What's New and Why It Matters

The cybersecurity audit regulations establish a new obligation to conduct thorough and independent audits of the business's cybersecurity program for protecting personal information. These new requirements may create significant questions for businesses, including to the extent that they require:

- The business to allow an auditor independence in the design and implementation of the audit;
- The performance of a comprehensive cybersecurity audit that may be substantially broader in scope than prior audits the company has performed on its cybersecurity program;
- Creation of a detailed record of the state of the business's cybersecurity program; and
- Executive certification under penalty of perjury.

Potential Steps to Mitigate Risk

- Confirm applicability and scope. Determine if the regulations apply to the business (including considering relevant exceptions (e.g., for data subject to the Gramm–Leach–Bliley Act)), evaluate which systems should be subject to the audit, and assess when reporting requirements will start to apply.
- Define approach. The amended regulations leave the business discretion on key points including whether to perform the audit internally or rely upon an external auditor, whether to rely on prior audits, and which executive should sign the required certification. Determine how the business will answer these key questions in order to define the approach that will work best for the business.

- Take appropriate steps to prepare for audit. The first auditable period, for the largest companies, begins in January 2027, allowing companies limited time to prepare for the audits including by strengthening portions of their cybersecurity programs. Consider how your business can best prepare for a required audit, including whether it would be appropriate to strengthen portions of the business' cybersecurity program or to perform preliminary assessments under privilege to determine readiness.

RISK ASSESSMENTS: DOCUMENTING HIGH-RISK PROCESSING DECISIONS

The amended regulations require businesses to conduct a risk assessment that evaluates whether the risks to California residents' privacy from high-risk processing of personal information outweigh the benefits to the individuals, the business, other stakeholders, and the public. A business must conduct a risk assessment if it engages in certain high-risk processing, including "selling" or "sharing" personal information, processing sensitive personal information, using automated processing to make a significant decision or to infer or extrapolate about a California resident, or processing personal information that the business intends to use to train an ADMT for a significant decision concerning an individual or a facial-recognition, emotion-recognition, or other technology that verifies an individual's identity, or conducts physical or biological identification or profiling of an individual.

A business must review and update the risk assessment at least once every three years or within 45 calendar days of a material change to the processing activity. The business must retain its risk assessments, including originals and updated versions, for as long as the processing continues or for five years after completing the risk assessment, whichever is later.

What's New and Why It Matters

Businesses subject to the risk assessment requirements were required to begin compliance by January 1, 2026. For risk assessments conducted in 2026 and 2027, the business must submit the information and attestation to CalPrivacy no later than April 1, 2028.

For risk assessments conducted after 2027, the business must submit the information to CalPrivacy no later than April 1 following any year during which the business conducted the risk assessment. For example, if the risk assessment was conducted in 2028, the business must submit the information to CalPrivacy no later than April 1, 2029.

Potential Steps to Mitigate Risk

- Standardize a risk assessment template. Create a modular risk assessment template with clear criteria for likelihood and severity of harm, tied to mitigating controls and measures.

- Integrate with product and procurement. Coordinate with your product development and procurement teams to ensure risk assessments occur for all high-risk use cases.
- Decision logging. Document approvals, required safeguards, and risk acceptance by appropriate stakeholders to create a defensible compliance record.[1]

[1] A redlined version reflecting the amendments to the CCPA regulations can be found at https://cppa.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_appr_text.pdf. As reflected therein, CalPrivacy made additional textual edits to pre-existing requirements under the CCPA, including to some of the definitions, consumer rights, and requirements regarding children's data. CalPrivacy's publication, 7 Things to Know Before 2026 CCPA Updates Take Effect, available at https://cppa.ca.gov/pdf/things_to_know_before_2026_updates.pdf, provides a helpful overview of other changes under the CCPA that went into effect on January 1, 2026, along with the new major additions discussed in this article.