

AN A.S. PRATT PUBLICATION

OCTOBER 2025

VOL. 11 NO. 8

PRATT'S

PRIVACY & CYBERSECURITY LAW REPORT



LexisNexis

EDITOR'S NOTE: TERRITORIAL SCOPE

Victoria Prussen Spears

**NIS 2 DIRECTIVE: WHAT TERRITORIAL SCOPE
FOR ADDRESSING THE CYBER THREAT?**

Romain Perray

**CALIFORNIA PRIVACY PROTECTION AGENCY
APPROVES REGULATIONS ON AUTOMATED
DECISIONMAKING TECHNOLOGY, RISK
ASSESSMENTS, CYBERSECURITY
AUDITS AND MORE**

Peter A. Blenkinsop, Doriann H. Cain,
Reed Abrahamson, Simonne Brousseau
and Aliyah N. Price

**NEURAL DATA PRIVACY REGULATION: WHAT
LAWS EXIST AND WHAT IS ANTICIPATED?**

Kristina Iliopoulos and Nancy Perkins

**OHIO ENACTS LAW REGULATING RANSOMWARE
PAYMENTS AND CYBERSECURITY**

Steven G. Stransky, Thomas F. Zych,
Thora Knight and Kimberly Pack

**DEPARTMENT OF JUSTICE DATA SECURITY
PROGRAM: INSIGHTS ON THE GOVERNMENT-
RELATED LOCATION DATA LIST**

Adam S. Hickey and Aaron Futerman

**THE EMPEROR UNCLOTHED: THE ABOLITION
OF THE SHAREHOLDER RULE**

James Brady-Banzet and Emma Williams

Pratt's Privacy & Cybersecurity Law Report

VOLUME 11

NUMBER 8

October 2025

Editor's Note: Territorial Scope

237

Victoria Prussen Spears

NIS 2 Directive: What Territorial Scope for Addressing the Cyber Threat?

239

Romain Perray

California Privacy Protection Agency Approves Regulations on Automated Decisionmaking Technology, Risk Assessments, Cybersecurity Audits and More

248

Peter A. Blenkinsop, Doriann H. Cain, Reed Abrahamson, Simonne Brousseau and Aliyah N. Price

Neural Data Privacy Regulation: What Laws Exist and What Is Anticipated?

253

Kristina Iliopoulos and Nancy Perkins

Ohio Enacts Law Regulating Ransomware Payments and Cybersecurity

258

Steven G. Stransky, Thomas F. Zych, Thora Knight and Kimberly Pack

Department of Justice Data Security Program: Insights on the Government-Related Location Data List

262

Adam S. Hickey and Aaron Futerman

The Emperor Unclothed: The Abolition of the Shareholder Rule

265

James Brady-Banzet and Emma Williams

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)

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.

Copyright © 2025 Reed Elsevier Properties SA, used under license by Matthew Bender & Company, Inc. All Rights Reserved.

No copyright is claimed by LexisNexis, Matthew Bender & Company, Inc., or Reed Elsevier Properties SA, in the text of statutes, regulations, and excerpts from court opinions quoted within this work. Permission to copy material may be licensed for a fee from the Copyright Clearance Center, 222 Rosewood Drive, Danvers, Mass. 01923, telephone (978) 750-8400.

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

(2025–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

EDITOR-IN-CHIEF

STEVEN A. MEYEROWITZ

President, Meyerowitz Communications Inc.

EDITOR

VICTORIA PRUSSEN SPEARS

Senior Vice President, Meyerowitz Communications Inc.

BOARD OF EDITORS

EMILIO W. CIVIDANES

Partner, Venable LLP

CHRISTOPHER G. CWALINA

Partner, Holland & Knight LLP

RICHARD D. HARRIS

Partner, Day Pitney LLP

JAY D. KENISBERG

Senior Counsel, Rivkin Radler LLP

DAVID C. LASHWAY

Partner, Sidley Austin LLP

CRAIG A. NEWMAN

Partner, Patterson Belknap Webb & Tyler LLP

ALAN CHARLES RAUL

Partner, Sidley Austin LLP

RANDI SINGER

Partner, Weil, Gotshal & Manges LLP

JOHN P. TOMASZEWSKI

Senior Counsel, Seyfarth Shaw LLP

TODD G. VARE

Partner, Barnes & Thornburg LLP

THOMAS F. ZYCH

Partner, Thompson Hine

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. Copyright 2025 Reed Elsevier Properties SA, used under license by Matthew Bender & Company, Inc. No part of this journal may be reproduced in any form—by microfilm, xerography, or otherwise—or incorporated into any information retrieval system without the written permission of the copyright owner. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquiries 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.

California Privacy Protection Agency Approves Regulations on Automated Decisionmaking Technology, Risk Assessments, Cybersecurity Audits and More

*By Peter A. Blenkinsop, Doriann H. Cain, Reed Abrahamson, Simonne Brousseau, and Aliyah N. Price**

The California Privacy Protection Agency (CPPA) Board voted to approve its proposed California Consumer Privacy Act (CCPA) regulations addressing cybersecurity audits, risk assessments, automated decisionmaking technology and applicability of the CCPA to insurance companies. This article explores some of the key aspects of these updates.

The California Privacy Protection Agency (CPPA) Board has voted 5-0 to approve its long-awaited proposed California Consumer Privacy Act (CCPA) regulations addressing cybersecurity audits, risk assessments, automated decisionmaking technology (ADMT) and applicability of the CCPA to insurance companies. The regulatory package also includes some updates to the main body of the pre-existing CCPA regulations. First formally proposed in November 2024, these regulations underwent a robust public comment period through the winter and faced substantial revisions in spring 2025. The Board will now submit the regulations to the California Office of Administrative Law for final review.

This article explores some of the key aspects of these updates, in particular, the regulations.

RELATIVELY NARROWLY DEFINE “ADMT”

Article 11 of the CCPA regulations now regulates businesses’ use of “ADMT to make a significant decision concerning a consumer.”¹ In 11 C.C.R. § 7001(e), “ADMT” is defined as “any technology that processes personal information and uses computation to replace human decisionmaking or substantially replace human decisionmaking.”

“Substantially replace human decisionmaking” is defined, in turn, to mean that a business “uses the technology’s output to make a decision without human involvement,”

* The authors, attorneys at Faegre Drinker Biddle & Reath LLP, may be contacted at peter.blenkinsop@faegredrinker.com, doriann.cain@faegredrinker.com, reed.abrahamson@faegredrinker.com, simonne.brousseau@faegredrinker.com and aliyah.price@faegredrinker.com, respectively.

¹ See 11 C.C.R. § 7200(a).

where “[h]uman involvement requires the human reviewer to: (A) Know how to interpret and use the technology’s output to make the decision; (B) Review and analyze the output of the technology, and any other information that is relevant to make or change the decision; and (C) Have the authority to make or change the decision based on [that] analysis. . . .”

Overall, the definition of ADMT was substantially simplified in the CPPA’s revisions to its proposed regulations in May 2025, following broad criticism of the previous draft, and will now cover a narrower range of activities than initially proposed.

CREATE OBLIGATIONS FOR BUSINESSES USING ADMT FOR SIGNIFICANT CONSUMER DECISIONS

Any company that uses ADMT to make a “significant decision” concerning a consumer will need to:

- Conduct a risk assessment prior to engaging in the activity;
- Provide an ADMT pre-use notice to the consumer;
- Grant the consumer the ability to opt-out of such use of ADMT; and
- Grant the consumer the ability to access ADMT, including by providing information, in response to a consumer request, regarding the purpose for use of ADMT, the logic of the ADMT, the outcome of the decisionmaking process for the consumer, and information about nondiscrimination and exercise of additional CCPA rights.

A “significant decision” in this context means any decision resulting in the provision or denial of financial/lending services; housing; education enrollment or opportunities; employment/independent contracting opportunities or compensation; or health care services.² Businesses that use ADMT for significant decisions must comply with the ADMT regulations by January 1, 2027.³

MANDATE ANNUAL CYBERSECURITY AUDITS FOR CERTAIN BUSINESSES

Article 9 of the CCPA regulations now requires businesses to conduct annual, independent cybersecurity audits if their processing of consumer personal information presents “significant risk” to consumers’ security. Under the regulations, “[a] business’s processing of consumers’ personal information presents significant risk to consumers’ security if”: (1) the business derived, in the preceding calendar year, 50% or more of its annual revenue from selling/sharing personal information; or (2) the business had

² See 11 C.C.R. 7001(ddd).

³ For further details, please see 11 C.C.R. §§ 7150, 7200-22.

annual gross revenues, in the preceding calendar year, in excess of \$26.625 million and either (a) processed, in the preceding calendar year, personal information of 250,000+ California consumers'/households' or (b) processed, in the preceding calendar year, 50,000+ California consumers' sensitive personal information.

This broad definition of "significant risk" will require many companies to comply with the regulations' new annual cybersecurity audit requirement. Audits must be completed by April 1 of each year, with staggered effective dates ranging from 2028 through 2030 depending on companies' annual gross revenues. For example, companies with annual gross revenues of more than \$100 million in 2026 will be required to conduct cybersecurity audits under the regulations by April 1, 2028, covering the period from January 1, 2027, to January 1, 2028.

Moreover, by April 1 of each year, businesses that are required to complete cybersecurity audits must submit to the CPPA a certification of completion of their cybersecurity audit, which must be completed by a member of the business's executive management team and contain the details required by 11 C.C.R. § 7124(d).

REQUIRE RISK ASSESSMENTS PRIOR TO ENGAGING IN ACTIVITIES POSING SIGNIFICANT RISK TO CONSUMER PRIVACY

The regulations also now require businesses to conduct risk assessments prior to engaging in processing activities that present a "significant risk to consumers' privacy."⁴ Activities that present a "significant risk to consumers' privacy" include:

- Selling/sharing personal information;
- Processing sensitive personal information (except for narrow employee exemptions);
- Using ADMT for a significant decision concerning a consumer;
- Using automated processing to infer/extrapolate certain characteristics about a consumer from systemic observation of that consumer when the consumer is acting in an educational, applicant or employment-related context;
- Using automated processing to infer/extrapolate certain characteristics about a consumer from systemic observation of that consumer based on the consumer's presence in a sensitive location; or
- Processing personal information that the business intends to use to train ADMT for significant decisionmaking.

Although these categories are more limited than they were in the CPPA's initial draft of the risk assessment regulations, they do still cover a broad range of personal information processing activities. The regulations:

⁴ See generally 11 C.C.R. §§ 7150-57.

- Articulate various content requirements for risk assessments;⁵
- Require that businesses review and update their risk assessments at least once every three years;⁶
- Permit use of a single risk assessment for a comparable set of processing activities;⁷ and
- Require businesses to submit certain high-level information about their preparation of risk assessments by April 1 of each year.

For risk assessments conducted in 2026 and 2027, that information must be submitted to the CCPA by April 1, 2028. For risk assessments conducted after 2027, that information must be submitted to the CCPA by no later than April 1 following any year during which the business conducted the risk assessments.

CLARIFY THE CCPA'S APPLICABILITY TO INSURANCE COMPANIES

The regulations now specifically clarify that insurance companies:

that meet the definition of “business” under the CCPA shall comply with the CCPA with regard to any personal information not subject to the Insurance Code and its regulations. For example, those insurance companies shall comply with the CCPA for personal information that is collected for purposes not in connection with an insurance transaction, as that term is defined in Insurance Code, section 791.02.⁸

Article 12 of the regulations also includes three illustrative examples that further explain how the CCPA applies to insurance companies.

OTHER AMENDMENTS

The amended regulations also make some edits to the main body of the existing regulations, including provisions regarding dark patterns; some tailored updates to privacy policy, notice at collection and notice of right to limit requirements; clarifications regarding data subject rights and opt-out preference signals; updates to service provider contract requirements; and more.⁹

⁵ See generally 11 C.C.R. § 7152.

⁶ Id. § 7155(a)(2).

⁷ Id. § 7156(a).

⁸ See 11 C.C.R. § 7271(a).

⁹ https://cppa.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_mod_txt_pro_reg.pdf.

TAKEAWAYS

- Overall, the definition of ADMT was substantially simplified in the CPPA's revisions to its proposed regulations in May 2025, following broad criticism of the previous draft, and will now cover a narrower range of activities than initially proposed.
- Any company that uses ADMT to make a "significant decision" concerning a consumer will need to conduct a risk assessment prior to engaging in the activity. The regulations also now require businesses to conduct risk assessments prior to engaging in processing activities that present a "significant risk to consumers' privacy."
- The regulations now specifically clarify that insurance companies "that meet the definition of 'business' under the CCPA shall comply with the CCPA with regard to any personal information not subject to the Insurance Code and its regulations."