AN A.S. PRATT PUBLICATION
SEPTEMBER 2026
VOL. 12 NO. 7

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 12 **NUMBER 7** **September 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.

U.S. State Privacy Enforcement: Key Priorities and Practical Guidance From State Regulators

By Jason Johnson and Linda Malek*

In this article, the authors summarize the key themes from the recent International Association of Privacy Professionals annual conference and offer practical guidance for companies navigating the evolving enforcement landscape.

At the International Association of Privacy Professionals' (IAPP) annual conference held earlier this year, enforcement officials from California, Connecticut, Indiana, and Delaware shared their current and upcoming enforcement priorities under U.S. state consumer privacy laws. This article summarizes the key themes from the panel and offers practical guidance for companies navigating the evolving enforcement landscape.

State regulators and enforcement authorities are working collaboratively, both publicly and behind the scenes, on enforcement and enforcement priorities, often sharing information on potential targets. The enforcement themes outlined below, although focused on certain jurisdictions, reflect an enforcement posture of coordination across multiple state enforcement agencies.

KEY ENFORCEMENT PRIORITIES BY STATE

California

California's enforcement approach has matured significantly. Regulators have moved beyond reviewing privacy policies for simple alignment violations and are now focused on operational issues — specifically, how data is being processed and what companies are doing with that data beyond what is stated in their notices. Areas of particular interest include connected TVs and other nontraditional devices that collect data.

The opt-out right has been a major enforcement focus. Regulators are walking through opt-out processes to test how these function in practice — including the symmetry between opt-outs and cookie mechanisms. Critically, intent is not a defense: regulators care about the real-world effect on consumers, and companies must be able to demonstrate how opt-outs are implemented behind the scenes.

Looking ahead, the California Privacy Protection Agency (CPPA) has indicated that calibrating fines to function as a genuine deterrent — rather than simply a cost of doing

* The authors, partners in Crowell & Moring LLP, may be contacted at jjohnson@crowell.com and lmalek@crowell.com, respectively.

business — is a priority. Data minimization and purpose limitation are also identified enforcement priorities.

On children's privacy, California is focused on age assurance for addictive features and has announced investigations into AI platforms in connection with children's safety, including a public investigation into Grok involving child sexual assault material. California is also conducting a "surveillance pricing" sweep, scrutinizing whether companies are using consumer data to set or modify prices — a practice that implicates purpose limitation obligations.

Connecticut

Connecticut is focused on similar issues to California. Connecticut has identified consumer rights and universal opt-out mechanisms, sensitive data (where express consent is required), children's privacy (including gaming and messaging apps), and data breaches and security as enforcement priorities. The Illuminate case, involving Connecticut, California, and New York, is illustrative of the state's approach as well as its collaboration with other states on enforcement.

Connecticut's enforcement report is a reliable preview of its ongoing priorities. Connecticut is also highly responsive to complaints, media coverage, and consumer advocacy activity. It has a particular focus on chatbots and serious harms — especially involving children — and has joined 42 other attorneys general in writing to AI companies around strengthening safeguards for chatbot products. Recent legislative amendments are also shaping enforcement priorities: companies that use or sell data for large language models (LLM) must disclose this in their privacy notices, and consumers must have the ability to challenge profiling decisions. Sensitive data and protections for minors, including addressing addictive design features, remain prominent focus areas.

Indiana

Indiana is ramping up its privacy enforcement efforts given that its Consumer Data Protection Act only became effective on January 1, but the state has also worked quickly on certain enforcement actions. A recent $1 million settlement with Apreia focused on delayed breach notification and reflects Indiana's ongoing focus on health data.

Indiana's additional priorities include the protection of sensitive data — specifically, genetic data and children's data that falls outside of HIPAA — as well as age verification laws in the context of adult websites. Transparency is also a theme: Indiana regulators emphasized that privacy notices must be understandable to everyday consumers, not just legal professionals, applying what one regulator described as the "give it to your mom" test.

Delaware

Delaware's enforcement focus has also moved beyond reviewing privacy notices to examining how businesses are operationalizing their data flows. Inquiry letters are

asking structural questions, including when the board of directors reviews the company's privacy practices. Regulators are signaling that senior executive and board-level buy-in — and a demonstrated compliance governance structure — will be expected going forward.

KEY TAKEAWAYS

1. *Opt-out mechanisms must work in practice.* Across states, and particularly in California, regulators are not accepting "intent to comply" as a defense. Opt-out flows must function symmetrically, propagate correctly through systems, and be tested from a consumer's perspective.

2. *Sensitive data requires heightened attention.* Express consent obligations for sensitive data are being actively enforced by multiple states. Companies should audit what sensitive data they collect, how it is disclosed, and whether consent and access controls are in place and documented.

3. *Data minimization and purpose limitation are operational obligations.* Regulators are scrutinizing whether companies are collecting only what they need, using data consistently with disclosed purposes, and able to document and justify this. The "surveillance pricing" sweep signals that using data to modify prices without adequate disclosure is a specific risk area.

4. *Children's privacy is a cross-state enforcement priority.* California and Connecticut are both actively investigating harms to minors, including AI platforms, addictive design features, and age assurance practices.

5. *AI-related transparency obligations are growing*. In Connecticut, using or selling data to train LLMs must be disclosed in privacy notices. The ability for consumers to challenge profiling decisions is also required. These requirements are likely to expand to other states.

6. *Operational compliance and board-level governance are under scrutiny.* Delaware and California both reflect a broader trend: regulators want to see not just compliant policies, but a functioning compliance program — including demonstrated governance, documented data flows, and senior leadership accountability.

7. *Data protection assessments are expected.* Regulators are routinely requesting these. Companies that have them documented and current are significantly better positioned when an inquiry is received.

8. *Security and breach notification remain core enforcement areas.* Delayed notification, inconsistent information provided to regulators, and inadequate security practices can be significant aggravating factors.

GUIDANCE ON RESPONDING TO REGULATORY INQUIRIES

Regulators offered candid guidance on how outside counsel and companies can approach enforcement interactions more effectively:

- *Cooperate efficiently*. Regulators are busy value cooperation during an inquiry in order to proceed efficiently. Treating a regulatory inquiry like private litigation — including making objections to production requests — is counterproductive. The goal of the inquiry process is to close the file, and regulators need detailed information to do that. Vague or bare-bones answers are a red flag.

- *Have your documentation ready*. Data protection assessments are regularly requested. Companies that already have documented privacy practices and can quickly produce responsive information are in a much better position than those that appear unprepared. Appearing unprepared can itself be a negative signal.

- *Proactively remediate*. If there is a problem, regulators are open to hearing that the company identified it and fixed it. Proactive remediation can reduce penalties and streamline settlement. Many matters are closed after a single round of information exchange when companies provide what is needed and demonstrate good-faith cooperation. Conversely, doubling down on problematic practices after notice will increase penalty exposure significantly.

- *Do not over-assert privilege*. Regulators are skeptical of privilege assertions, particularly around breach response. Copying counsel on a document does not make it privileged. The factual circumstances of a breach are not privileged in the regulators' view, and if companies withhold information, regulators will conduct their own investigation — at the company's expense.

- *Save legal arguments for later*. At the outset of a regulatory investigation, regulators are gathering facts. Legal arguments are appropriate at a later stage. Experienced counsel who have worked with the relevant regulators — and who understand the scope of pre-investigative authority — can be particularly valuable in calibrating the engagement strategy.