AN A.S. PRATT PUBLICATION
OCTOBER 2026
VOL. 12 NO. 8

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

EDITOR'S NOTE: PRIVACY IN THE STATES
Victoria Prussen Spears

DELAWARE'S PRIVACY LAW IS ABOUT TO EXPAND: 6 STEPS EMPLOYERS AND BUSINESSES SHOULD TAKE TO PREPARE
Vivian Isaboke

OKLAHOMA ENACTS NATION'S TWENTIETH STATE COMPREHENSIVE PRIVACY LAW
Kirk J. Nahra, Ali A. Jessani and Blythe Riggan

ALABAMA ENACTS NATION'S TWENTY-FIRST STATE COMPREHENSIVE PRIVACY LAW
Kirk J. Nahra, Samuel Kane and Blythe Riggan

NEW YORK STATE DEPARTMENT OF FINANCIAL SERVICES RAMPS UP HEALTH CARE CYBERSECURITY ENFORCEMENT WITH $2.25 MILLION SETTLEMENT
Jason Johnson and Linda Malek

THE GOOD, THE BAD, AND THE UGLY: WHAT 7 RECENT COURT DECISIONS TELL YOU ABOUT TODAY'S WEBSITE PRIVACY LIABILITY
Usama Kahf

CHARTING NEW WATERS: ENGLISH HIGH COURT CONFINES EFFECT OF *THREE RIVERS (NO 5)*, CONFIRMING PRIVILEGE CAN APPLY TO INTRA-CLIENT COMMUNICATIONS
James Norris-Jones and Tim Vogel

COURT OF JUSTICE OF THE EUROPEAN UNION RULES THAT A FIRST DATA SUBJECT ACCESS REQUEST CAN BE REFUSED AS EXCESSIVE
Huw Beverley-Smith, Charlotte H N Perowne and James Ford

Pratt's Privacy & Cybersecurity Law Report

VOLUME 12 **NUMBER 8** **October 2026**

Editor's Note: Privacy in the States 255
Victoria Prussen Spears

Delaware's Privacy Law Is About to Expand: 6 Steps Employers and Businesses Should Take to Prepare 257
Vivian Isaboke

Oklahoma Enacts Nation's Twentieth State Comprehensive Privacy Law 264
Kirk J. Nahra, Ali A. Jessani and Blythe Riggan

Alabama Enacts Nation's Twenty-First State Comprehensive Privacy Law 268
Kirk J. Nahra, Samuel Kane and Blythe Riggan

New York State Department of Financial Services Ramps Up Health Care Cybersecurity Enforcement With $2.25 Million Settlement 273
Jason Johnson and Linda Malek

The Good, the Bad, and the Ugly: What 7 Recent Court Decisions Tell You About Today's Website Privacy Liability 277
Usama Kahf

Charting New Waters: English High Court Confines Effect of *Three Rivers (No 5)*, Confirming Privilege Can Apply to Intra-Client Communications 283
James Norris-Jones and Tim Vogel

Court of Justice of the European Union Rules That a First Data Subject Access Request Can Be Refused as Excessive 288
Huw Beverley-Smith, Charlotte H N Perowne and James Ford

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)

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 © 2026 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

(2026–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 2026 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 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.

The Good, the Bad, and the Ugly: What 7 Recent Court Decisions Tell You About Today's Website Privacy Liability

By Usama Kahf*

In this article, the author compiles seven recent court decisions involving website tracking claims and organizes them by identifying the good, the bad, and the ugly. In connection with website tracking litigation, the author also discusses what's working in court, what's failing, and, most importantly, what businesses need to do to protect themselves.

California's website tracking litigation wave shows no signs of slowing down. Plaintiffs' attorneys continue to file cookie and pixel tracking lawsuits by the hundreds, alleging that routine third-party analytics and advertising tools on business websites constitute illegal wiretapping under the California Invasion of Privacy Act (CIPA) and the federal Electronic Communications Privacy Act (ECPA). Courts have been grappling with these claims for years, and their answers have been anything but consistent. To help you make sense of where things stand today, this article compiles seven recent decisions and organizes them by identifying the good, the bad, and the ugly. This article discusses what is working in court, what is failing, and, most importantly, what businesses need to do to protect themselves.

THE GOOD: DECISIONS THAT HELP BUSINESSES

Sisti v. Bosley, Inc.: Complete Dismissal with Prejudice

Bosley stands as the cleanest defense win in the current batch of decisions, and the reasons it succeeded offer a blueprint for other businesses. The court's April 27 decision dismissed all claims with prejudice (meaning plaintiffs cannot amend their complaint and refile the case) on two grounds that each would have been independently dispositive.

- First, the court found the plaintiff lacked Article III standing. The data allegedly collected through third-party tracking pixels (browsing behavior, device identifiers, and general usage patterns) wasn't sufficiently sensitive to constitute a concrete privacy injury.
- Second, and equally important, Bosley had a properly structured sign-in agreement that required users to affirmatively accept the company's terms of service before using the site. Because those terms included consent to the tracking at issue, the plaintiff's claims failed on the merits as well.

* The author, a partner in Fisher Phillips, may be contacted at ukahf@fisherphillips.com.

The lesson from *Bosley* is that two independent lines of defense – standing and consent – are far better than one. A company that can argue both "you weren't really injured" and "you agreed to this" is in a much stronger position than one relying on a single theory.

This is also an example where a plaintiff tried to allege disclosure of something more than just IP addresses and the court found no concrete harm could possibly result from a website's (even a health-related website like Bosley's) disclosure to social media platforms of plaintiff's browsing behavior, device identifiers, general usage patterns, and the fact plaintiff scheduled a hair transplantation consultation on the website's "scheduler page." The court also found that the plaintiff did not suffer monetary loss to establish standing because he never attempted to sell the information that was allegedly disclosed.

Importantly, the court found that plaintiff could not proceed with his ECPA claim because the tortious conduct was the alleged interception itself. The crime-tort exception to the ECPA's party exception did not apply because plaintiff could not plausibly establish that health data was disclosed in violation of HIPAA.

Diaz v. Paramount Skydance: Standing Analysis Gives Businesses a Roadmap

The *Paramount* ruling, involving the free streaming platform Pluto TV, is significant less for its outcome than for its reasoning on standing. The court dismissed the complaint on April 20 after conducting a rigorous analysis of what kind of privacy injury is actually sufficient to support a lawsuit, and its conclusions are very business-friendly.

The court drew a sharp distinction between tracking data that is genuinely "sensitive," such as medical information, financial data, and highly personal communications, and the kind of routine behavioral metadata that ad-targeting pixels typically collect. Vague allegations that tracking pixels collected "personal information" didn't cut it, the court said. Plaintiffs have to identify specific, sensitive data that was actually disclosed to sustain a concrete injury. For streaming platform visitors browsing free content, the court found that bar wasn't met.

This standing framework has become increasingly influential. Multiple courts have cited similar reasoning to dismiss tracking claims at the threshold before ever reaching the merits of whether CIPA was violated. For businesses whose websites handle ordinary consumer browsing rather than financial applications or healthcare data, this line of cases provides meaningful protection.

THE BAD: DECISIONS THAT WENT THE WRONG WAY — WITH CAVEATS

Garcia v Anschutz Entertainment Group: Mixed Result, But the Warning Is Clear

The AEG case produced a split result that illustrates how a company can win on one claim while losing on another, and how the gap between a consent banner and actual consent can be fatal.

- On the positive side, the court's May 5 ruling dismissed the federal wiretapping claim under the ECPA, finding the party exception applied. And because the plaintiff admitted she would never return to the website, her request for injunctive relief was also dismissed.

- But the CIPA pen register claim survived, and that's because the tracking started before the plaintiff had a chance to reject it. This should serve as a warning for every business with a cookie consent mechanism. AEG had a cookie consent banner, but the problem was that its third-party cookies activated the moment a user landed on the site – before the banner rendered, before the user could make a choice. A consent tool deployed after the data is already flowing is problematic, according to this decision.

- Note, however, that whether the CIPA pen register prohibition applies in this manner to require opt-in consent before cookies or pixels can start collecting data on a website is an issue currently before the California Court of Appeal in an appeal brought by Variety Media. Opt-in consent is not necessarily required by CIPA or any other law, as courts are split on this issue, and this is one more trial court decision in the plaintiffs' column.

***Ortiz v. Foris Dax, Inc. (Crypto.com)*: CIPA Wiretapping Dismissed, Pen Register Survives**

The May 21 *Crypto.com* ruling produced the same split outcome that is becoming a recurring pattern: the CIPA § 631 wiretapping claim was dismissed because plaintiffs failed to allege with any specificity what communications of theirs were actually intercepted, but the § 638.51 pen register claim survived.

- On the wiretapping side, this case reinforces what courts have been saying consistently: claiming you "browsed" a website and that the site's cookies were capable of collecting certain categories of information is not the same as alleging that your personal communications were actually intercepted. Plaintiffs who don't describe their actual on-site activities (search terms entered, forms submitted, clicks made, etc.) are giving courts nothing to work with on the contents element of § 631.

- On the pen register side, the court delivered the most thorough federal analysis yet of whether CIPA's pen register provision applies to internet tracking. The answer was yes, grounded in both plain text and legislative history. The court found that CIPA borrowed its pen register definition from a federal statute that Congress had already broadened in 2001 to cover internet-based tracking, and nothing in the California statute limits it to telephonic devices.

- Note, however, that several California state courts have applied statutory interpretation principles to reach the opposite conclusion, finding that the text of the CIPA pen register sections itself shows that it only applies to telephone lines, not to website tracking technology. For example, one state court recently reached this conclusion because the CIPA section outlining the process for obtaining a court order to install a pen register speaks only of telephone lines and leaves no room for any other technology. The court reasoned that this section must be read in context with the section prohibiting pen registers without a court order.

- The court also directly addressed SB 690, the pending legislative reform bill, and declined to use it as a guide to statutory interpretation. The court said that the legislature's awareness of the litigation wave says nothing about what the current law means.

Ingraham v. Capital One: Financial Data Changes Everything

The May 22 *Capital One* ruling is in the "bad" column, but it deserves a significant asterisk: this case is genuinely distinguishable from most of what businesses in this space will face, and understanding why could help you develop your own game plan.

The tracking at issue here wasn't routine browsing behavior. Capital One's website allegedly transmitted customers' employment status, citizenship information, bank account type, credit card application status, approval or denial outcomes, FICO score segments, and income bands to third-party services, along with names, email addresses, and phone numbers. Capital One didn't even dispute that one plaintiff's employment status and credit card denial were transmitted to third parties.

The court found those facts sufficient to clear the "highly offensive" threshold that routine metadata cases fail to reach – relying on the 9th Circuit's *Popa v. Microsoft* decision, which specifically distinguished technologies that capture sensitive financial information from those that capture general browsing behavior. The court also rejected Capital One's anonymization argument at the pleading stage, where a genuine factual dispute existed about whether "anonymized" identifiers could be re-linked to individuals.

There was one notable defense win: one of the two named plaintiffs was dismissed entirely because, after filing the lawsuit, he submitted two more credit card applications on Capital One's website. You cannot credibly claim a reasonable expectation of privacy in data you voluntarily continue submitting to the same defendant after alleging in litigation that it misuses that data.

The takeaway for most businesses is that this decision is an outlier. If your website collects general consumer browsing data for marketing analytics, you are not in the same position as a financial institution transmitting credit application outcomes and income data to third-party ad networks.

THE UGLY: DECISIONS THAT WENT BADLY

Podraza v. Nourish, Inc.: Wiretapping and CIPA Claims Both Survive

Nourish is the most straightforwardly bad decision in the set for businesses because the court's April 20 decision allowed both the federal wiretapping claim and the CIPA § 631 claim to survive dismissal without the kind of limiting factors that make other plaintiff wins distinguishable.

The central problem was consent architecture. Unlike *Bosley*, which had a properly structured sign-in clickwrap agreement requiring affirmative acceptance before access, *Nourish* relied on browsewrap: a notice somewhere on the site that users were deemed to have accepted simply by visiting. Courts have grown increasingly hostile to browsewrap agreements, and this case is a direct illustration of why: the court found the consent mechanism inadequate and refused to dismiss on that basis.

The ruling also navigated the HIPAA crime-tort exception in a way that allowed the federal wiretapping claim to proceed, a result that will be of particular concern to any business operating in or adjacent to the healthcare space.

Castro v. SBE Restaurant Group: State Court Proves More Plaintiff-Friendly

The April 16 *SBE Restaurant Group* decision is the ugliest entry on the list, and it carries a warning that federal court outcomes may not tell the full story of your exposure. This was a California state court ruling, and the result was a near-total plaintiff win: four of five causes of action survived the demurrer, including the CIPA pen register theory.

State courts have shown a consistent willingness to let these claims proceed that federal courts (with their standing requirements and pleading standards) have not always matched. *SBE* is a reminder that CIPA litigation isn't only a federal courthouse problem. If you operate in California, your exposure runs across both court systems.

WHAT TO DO RIGHT NOW

The consistent message throughout all of these decisions is that businesses across the country face real legal exposure, and the outcome of any litigation depends heavily on decisions they have already made (or failed to make) about how their website handles tracking and consent.

Here are the steps every business should take:

- First, audit every tracking tool currently running on your website. Know what cookies, pixels, analytics tools, and session replay software you're using, who operates them, and when they start collecting data. If any tool activates before a user has an opportunity to consent or decline, you may be in the same position as the *AEG* decision.

- Second, upgrade your consent mechanism from browsewrap to something that actually works. A notice buried in a footer or a banner that users

scroll past isn't enough to establish consent at the motion to dismiss stage. Affirmative, pre-tracking consent, like a properly structured sign-in clickwrap or a consent banner that genuinely works, is the standard that courts are enforcing.

- Third, scrutinize the data your site collects and transmits to third parties. If your tracking tools are capturing the kind of sensitive financial, health, or personally identifiable information that was at issue in *Capital One*, your risk profile is materially higher than a retail website capturing general browsing behavior.

- Fourth, align your privacy policy with what your tools actually do. Policies that promise users control over their data but don't reflect actual practices compound your exposure by supporting both CIPA and ECPA claims simultaneously.

- And fifth, get ahead of this before a demand letter arrives. The plaintiffs' bar targets businesses based on automated scans of what tracking technology is detectable on your site. Proactive review is far less expensive than reactive litigation, and far more effective.