

AN A.S. PRATT PUBLICATION

MARCH-APRIL 2025

VOL. 11 NO. 3

PRATT'S
**PRIVACY &
CYBERSECURITY
LAW**
REPORT



LexisNexis

EDITOR'S NOTE: BEST PRACTICES

Victoria Prussen Spears

**7 BEST PRIVACY PRACTICES FOR COMPANIES
WHEN USING GEOLOCATION TOOLS
TO TRACK WORKERS**

Kate Dedenbach and Usama Kahf

**DOES YOUR AI CHATBOT COLLECT
BIOMETRIC DATA?**

Shani Rivaux, Catherine Perez,
Jeewon K. Serrato and
Shruti Bhutani Arora

**DIGITAL WIRETAPPING LITIGATION: TOP 5
SURPRISING TAKEAWAYS**

Kate Dedenbach and Usama Kahf

**FEDERAL TRADE COMMISSION CRACKS DOWN
ON SELLING SENSITIVE LOCATION INFO;
RESTRICTS USE OF CONSUMER DATA
FOR THE FIRST TIME**

Bess Hinson-Greenspan, Haylie D. Treas and
Brandon L. Lewis

**SECURITIES AND EXCHANGE COMMISSION
SETTLES WITH COMPANIES OVER CHARGES
RELATING TO CYBERSECURITY DISCLOSURES**

Eric S. Wu, Pavel (Pasha) A. Sternberg and
Mary Ann H. Quinn

**U.S. DEPARTMENT OF JUSTICE AND U.S.
DEPARTMENT OF HOMELAND SECURITY'S
CYBERSECURITY AND INFRASTRUCTURE
SECURITY AGENCY ISSUE NEW NATIONAL
SECURITY PROGRAM TO REGULATE FOREIGN
ACCESS TO SENSITIVE DATA**

Megan L. Brown, Duane C. Pozza, Kathleen E. Scott,
Jacqueline F. "Lyn" Brown and
Sydney M. White

Pratt's Privacy & Cybersecurity Law Report

VOLUME 11

NUMBER 3

March-April 2025

Editor's Note: Best Practices Victoria Prussen Spears	75
7 Best Privacy Practices for Companies When Using Geolocation Tools to Track Workers Kate Dedenbach and Usama Kahf	77
Does Your AI Chatbot Collect Biometric Data? Shani Rivaux, Catherine Perez, Jeewon K. Serrato and Shruti Bhutani Arora	81
Digital Wiretapping Litigation: Top 5 Surprising Takeaways Kate Dedenbach and Usama Kahf	85
Federal Trade Commission Cracks Down on Selling Sensitive Location Info; Restricts Use of Consumer Data for the First Time Bess Hinson-Greenspan, Haylie D. Treas and Brandon L. Lewis	88
Securities and Exchange Commission Settles With Companies Over Charges Relating to Cybersecurity Disclosures Eric S. Wu, Pavel (Pasha) A. Sternberg and Mary Ann H. Quinn	92
U.S. Department of Justice and U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency Issue New National Security Program to Regulate Foreign Access to Sensitive Data Megan L. Brown, Duane C. Pozza, Kathleen E. Scott, Jacqueline F. "Lyn" Brown and Sydney M. White	95

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 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.

Digital Wiretapping Litigation: Top 5 Surprising Takeaways

*By Kate Dedenbach and Usama Kahf**

In this article, the authors examine the new trend of digital wiretapping litigation claims – one of the fastest-growing compliance risks.

Some businesses might be surprised to learn that digital wiretapping litigation claims are one of today's fastest-growing compliance risks, with over 1,560 lawsuits filed in 28 states since a groundbreaking 2022 decision opened a new set of floodgates. And while businesses in any industry are susceptible to such a lawsuit, those in the retail, tech, and healthcare sectors need to be especially cautious. Here are the five biggest takeaways for employers.

QUICK BACKGROUND

Any business that utilizes websites, apps, or email marketing to reach their intended audience can fall victim of a digital wiretapping lawsuit. Plaintiffs' attorneys are identifying those businesses that utilize tracking technology to collect and disclose information that could identify an individual user without the user's consent to determine if a lawsuit could be worthwhile. The tracking technology at issue includes cookies, pixels, tags, and web beacons installed on websites and apps – as well as digital tracking code embedded in marketing emails.

TOP 5 TAKEAWAYS

Top States for Litigation Include the Expected – and Some Surprises

It comes as no surprise that we see traditionally privacy-minded California as the state where businesses are facing the most litigation matters. In fact, close to 83% of all digital wiretapping claims to date have been filed in California.

But the litigation trend is taking off outside of California as well, with some states you might not have expected listed among those with the most. Here are the top states for claims since these lawsuits first started surfacing:

- California: 1,284;
- Illinois: 64;
- Pennsylvania: 34;

* The authors, attorneys with Fisher Phillips, may be contacted at kdedenbach@fisherphillips.com and ukahf@fisherphillips.com, respectively.

- New York: 28;
- Massachusetts: 27;
- Arizona: 18; and
- Washington: 16.

No Industry Is Immune

The retail industry has faced the lion's share of claims, with 522 lawsuits – about one out of every three – filed against retail businesses. The other two industries that stand out are the tech sector (231) and healthcare (161). The common thread among these high-target industries is that marketing is a significant business driver with them all, meaning they have website practices that expose them to additional risk.

But the data demonstrates that every industry is at risk. The good news is that there are steps that companies can take to mitigate risk. Making small changes to a website or app can reduce the potential for a claim and can significantly reduce the costs of resolving any claims.

A State Consumer Privacy Act Is Irrelevant

It might be easy to assume that this litigation trend is not something a company needs to worry about if its business does not operate in one of the 31 states that have not enacted a generally applicable consumer privacy law – but that would be wrong. Plaintiffs' attorneys are filing these claims utilizing a variety of statutory and non-statutory claims.

- Some of the claims are based upon decades-old statutes that were written to prevent wiretapping on phone lines, and some local courts are interpreting them in new ways to apply to new technology.
- Claims also allege violations of federal laws, such as HIPAA in the healthcare industry, rendering the status of state law as irrelevant.
- Finally, many claims allege non-statutory theories, such as invasion of privacy under a state's constitution or common law.

In other words: The absence of a consumer privacy statute in the state is not a factor in whether companies are at risk of falling victim to one of these claims. And even if businesses are subject to state consumer privacy laws like the California Consumer Privacy Act (CCPA), compliance with those laws will not immunize companies from lawsuits under wiretapping laws.

Even One Unknown Issue On a Website or App Can Lead to a Claim

If a business operates a website or app, there are a variety of common website features that are frequently the subject of wiretapping claims. While cookies are the most frequent culprit in digital wiretapping claims, some of the claims have alleged that a website's search bar and chat features are disclosing the contents of electronic communications to third parties. There are numerous ways to continue using cookies, search bars, and chat functionality with changes in how they are disclosed and the timing of their usage that can reduce the risks of becoming the subject of a wiretapping litigation claim. Businesses may want to look at ways to reduce risk that balance the business' need for continued use of certain features.

The Public Data Only Shows Part of the Picture

Thus far, this article has discussed only the publicly available data. However, businesses usually receive pre-litigation demands and many of these are resolved well before they show up in publicly available litigation data. Not to mention the fact that many might end up in private arbitration and are never revealed to the public. Indeed, many, many more businesses are finding themselves caught up in this new trend than the numbers reveal.