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

# PRATT'S PRIVACY & CYBERSECURITY LAW REPORT



LexisNexis

EDITOR'S NOTE: THE NEXT FRONTIER
Victoria Prussen Spears

SURVEILLANCE PRICING: THE NEXT FRONTIER OF PRIVACY LITIGATION
Matthew M. Morrissey, Josh Mahoney, Michael William Fires, Kate C. Goldberg and Tyler J. Hoguet

DRIFT PROTOCOL EXPLOIT: WHY "SOCIAL TRUST" IS THE NEWEST CYBERSECURITY GAP
Rajeev Raghavan, Anand Sithian and Sarah Rippy

GENETIC DATA AND ARTIFICIAL INTELLIGENCE TRAINING FOLLOWING ACQUISITIONS: EMERGING LITIGATION RISK AND A RAPIDLY EXPANDING STATE REGULATORY LANDSCAPE
Jason Johnson, Linda Malek and Sarah Rippy

NAVIGATING AI COMPLIANCE WITH HIPAA ESSENTIALS
Jeff Wurzburg, Susana Medeiros, Susan Linda Ross, Abel Chacko and Kathleen Rubinstein

THIRD CIRCUIT OFFERS CLARITY ON DATA PRIVACY AND REPLAY CODE: 3 PROACTIVE STEPS FOR BUSINESSES FOLLOWING DUAL RULINGS
Risa B. Boerner, Logan S. Booth and Catherine M. Contino

U.S. STATE PRIVACY ENFORCEMENT: KEY PRIORITIES AND PRACTICAL GUIDANCE FROM STATE REGULATORS
Jason Johnson and Linda Malek

# Pratt's Privacy & Cybersecurity Law Report

**VOLUME 12** **NUMBER 7** **September 2026**

**Editor's Note: The Next Frontier** 221
Victoria Prussen Spears

**Surveillance Pricing: The Next Frontier of Privacy Litigation** 223
Matthew M. Morrissey, Josh Mahoney, Michael William Fires, Kate C. Goldberg and Tyler J. Hoguet

**Drift Protocol Exploit: Why "Social Trust" Is the Newest Cybersecurity Gap** 236
Rajeev Raghavan, Anand Sithian and Sarah Rippy

**Genetic Data and Artificial Intelligence Training Following Acquisitions: Emerging Litigation Risk and a Rapidly Expanding State Regulatory Landscape** 240
Jason Johnson, Linda Malek and Sarah Rippy

**Navigating AI Compliance With HIPAA Essentials** 243
Jeff Wurzburg, Susana Medeiros, Susan Linda Ross, Abel Chacko and Kathleen Rubinstein

**Third Circuit Offers Clarity on Data Privacy and Replay Code: 3 Proactive Steps for Businesses Following Dual Rulings** 248
Risa B. Boerner, Logan S. Booth and Catherine M. Contino

**U.S. State Privacy Enforcement: Key Priorities and Practical Guidance From State Regulators** 251
Jason Johnson and Linda Malek

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, Norton Rose Fulbright US 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.

# Third Circuit Offers Clarity on Data Privacy and Replay Code: 3 Proactive Steps for Businesses Following Dual Rulings

***By Risa B. Boerner, Logan S. Booth and Catherine M. Contino****

*In this article, the authors review two decisions by the U.S. Court of Appeals for the Third Circuit that provide important guidance to help businesses avoid and defeat website tracking lawsuits.*

Over the last few years, the plaintiffs' bar has frequently cited businesses' use of session replay code (SRC) on websites as one basis for the flood of website tracking litigation against businesses across the country. SRCs allow domain hosts to track nearly every element of a website visitor's activity – from mouse movements to clicks, scrolls, zooms, and keystrokes – allowing the host to effectively recreate the user's visit to their website. Since SRCs typically operate without a visitor's consent, a wave of class action lawsuits has been filed alleging that SRCs effectively constitute digital wiretapping since they intercept and log behavior in real time. Although there have been mixed decisions across the country on motions to dismiss such claims, a pair of recent decisions from the U.S. Court of Appeals for the Third Circuit provides important guidance that can help businesses to avoid and defeat such claims. This article covers everything businesses need to know about the rulings and what they can take away from them.

## DATA DISCLOSURE DOES NOT ALWAYS AMOUNT TO A TORT

Plaintiffs in both cases before the Third Circuit alleged that businesses using SRC on their websites violated the common-law torts of disclosure of private information and intrusion upon seclusion. But the court tossed the cases, finding that the plaintiffs failed to show any injury from the technology and lacked standing to sue.

In one case against a defunct budget airline, the court ruled that the tort of disclosure of private information was not applicable because the information collected by the SRC was not used to embarrass or humiliate the plaintiffs – a necessary element of such claim. The judges also held that the airline did not commit intrusion upon seclusion because:

(i) the plaintiffs voluntarily provided the information to the SRC;

(ii) their information was anonymized; and

* The authors, attorneys with Fisher Phillips, may be contacted at rboerner@fisherphillips.com, lbooth@fisherphillips.com and ccontino@fisherphillips.com, respectively.

(iii) there is a limited expectation of privacy on the internet.

Similarly, in another case involving outdoor retailers, the court determined that "mouse clicks and movements, keystrokes, and search terms" did not amount to sensitive information and could not be linked to the plaintiffs' identities. Thus, the plaintiffs in this case could not plausibly allege that disclosing this information caused "embarrassment or humiliation."

In this case, however, the Third Circuit went a step further and clarified that the mere collection of sensitive financial information – without subsequent revelation – fails to meet the threshold needed to prove disclosure of private information.

For individuals who merely perused the retailers' websites without inputting any personal information, the court held that their activity on the website generated no greater expectation of privacy than a shopper would have while walking the aisles of a brick-and-mortar store. Nevertheless, once a visitor to the website entered their complete credit or debit card numbers, the recording of that information by the SRC did qualify as an intrusion upon seclusion, since the sensitivity of financial information makes any nonconsensual interception particularly harmful.

## WHAT'S THE IMPACT OF THIS RULING?

It is important to keep in mind that the Third Circuit's decisions are only binding on the states within its jurisdiction, which include Delaware, New Jersey, Pennsylvania, and the U.S. Virgin Islands. But, within this circuit, the Court has shown consistency in ruling against plaintiffs in related wiretapping and privacy disputes. For example, in *Popa v. Harriet Carter Gifts, Inc.*, the Court held that simply browsing an online retailer's website without entering sensitive information failed to rise to the level of an injury-in-fact.

And for those outside the jurisdictional purview of the Third Circuit, these holdings can be used by other courts as persuasive authorities. The Ninth Circuit has already issued a similar ruling in *Popa v. Microsoft Corporation*, in which it held that the routine use of web-analytics and session-replay tools does not run afoul of wiretapping laws or yield "concrete" harm. Whether other courts borrow of these precedents, and how the Supreme Court ultimately rules if it takes up a case addressing these issues, will be important considerations for how website operators should conduct themselves moving forward.

## WHAT THIS MAY MEAN FOR BUSINESSES

The Third Circuit's rulings that the mere recording of a user's activity on a company's website, absent additional factors, does not automatically constitute digital wiretapping is a major win for domain hosts. It provides hosts with the ability to control the liability they may face from employing SRCs based on what type of information they gather and how that information is used. Following this ruling, you should work with legal counsel and consider reviewing:

- *What type of information is your SRC collecting?*

It's important to audit and frequently review the types of information collected by your SRC. Merely recording a user's "movements" on your platform likely will not give rise to a tortious claim. Even if a consumer is accessing your websites from the confines of their home, the Third Circuit is inclined to view their activity on your website like a shopper moving through a physical store. In the same way that the physical shopper has no expectation of privacy vis-à-vis their movements, the website visitor should not, either.

- *Would a reasonable person consider the information gathered by your SRC to be highly sensitive?*

While mere movement within a web domain is not inherently sensitive, the collection of financial information is. This means that before a user inputs financial data, one of two things must occur: the website (i) must obtain consent to continue utilizing SRCs or, (ii) terminate the use of SRCs if the user is not given the choice to opt-in to the collection of this information. The same is likely true of other categories of sensitive personal data, including health-related information.

- *How can you design an SRC-compliant website from the outset?*

In its decisions, the Third Circuit specifically called out the "surreptitious" nature of SRCs, and the fact that websites often do not give users the option to opt-out, nor does the average user even know that SRCs are embedded in the websites they visit. It is this element of secrecy that creates potential legal liability for website operators. As such, in the same way that cookie banners have come to be viewed as a means of limiting exposure for tracking a user's internet activity, it may be prudent for companies using SRCs on their website to consider deploying similar disclosure notices.