AN A.S. PRATT PUBLICATION
JANUARY 2026
VOL. 12 NO. 1

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

Insurance Coverage Considerations for Privacy Class Action Lawsuits in This Technology Driven World

By Gretchen Hoff Varner, Darren S. Teshima and Hakeem Rizk*

Plaintiffs' law firms have been looking to monetize alleged privacy risks associated with data collection, spurring waves of putative class action lawsuits that are not only costly but can also severely damage a company's reputation. This article provides a brief overview of recent privacy class action lawsuits and discusses some insurance coverage considerations to keep in mind as your company seeks to protect itself against these evolving threats.

In this increasingly growing digital landscape, companies are entrusted with vast amounts of sensitive personal information. From names and email addresses to browsing habits and location data, companies routinely collect users' personal data all to enhance convenience and functionality, advertise products, personalize experiences for consumers, and improve services. Plaintiffs' law firms, however, have been looking to monetize alleged privacy risks associated with this data collection, spurring waves of putative class action lawsuits that are not only costly but can also severely damage a company's reputation. This unfolding legal landscape accentuates the need for robust insurance coverage, and in particular, insurance that will respond to privacy-related claims.

You may have heard that there is no coverage for consumer privacy class actions, and as such, be persuaded not to seek coverage for those lawsuits. Do not be so persuaded. Instead, ask for your company's insurance policies, assess the available coverages under them, and seek all coverage that may apply.

This article provides a brief overview of recent privacy class action lawsuits and discusses some insurance coverage considerations to keep in mind as your company seeks to protect itself against these evolving threats.

PRIVACY CLASS ACTION LAWSUITS

Privacy class action lawsuits have gained significant momentum targeting corporations over alleged mishandling, misuse, and unauthorized sharing of personal data. These

* The authors, attorneys at Covington & Burling LLP, may be contacted at ghoffvarner@cov.com, dteshima@cov.com and hrizk@cov.com, respectively.

lawsuits often claim that companies violate privacy laws such as the California Consumer Privacy Act (CCPA), the Illinois Biometric Information Privacy Act (BIPA), and federal and state wiretapping and eavesdropping laws by collecting, storing, or sharing users' personal information without proper notice or consent. Although these lawsuits focus on violations of laws, at the heart of many of them are alleged violations of privacy policies that companies have promised to uphold.

Of late, major technology companies, global retailers, social media platforms, healthcare providers, and data brokers have been the primary targets of these lawsuits, which have focused on these companies' alleged unauthorized use of website marketing tools such as pixels. But these lawsuits also have targeted these companies' use of artificial intelligence and biometric data, highlighting concerns about privacy rights in relation to facial recognition technologies and fingerprint scans. For example:

- In 2025, a leading facial recognition technology company settled for north of $50 million a multidistrict, class action lawsuit alleging violations of the Illinois Biometric Information Privacy Act regarding the company's alleged automatic collection, storage, and use of biometric data.

- Also in 2025, a healthcare provider settled for approximately $6 million a class action lawsuit asserting claims of unauthorized disclosure of personally identifiable information, including health-related information, to third parties through pixel tools. This is only one of many recent settlements by healthcare systems, as those corporations have faced a barrage of class action lawsuits alleging privacy violations from use of tracking pixels.

- Starting in 2024, a technology company settled various lawsuits alleging statutory privacy violations concerning the use of biometric identifiers for amounts totaling over $1 billion.

Numerous lawsuits like these alleging privacy violations have been filed throughout the country. As use of artificial intelligence and ubiquitous data collection technologies continues to rise, legal battles over consumer privacy will only intensify.

INSURANCE COVERAGE FOR PRIVACY CLASS ACTION LAWSUITS

With the proliferation of privacy class action lawsuits, having insurance that adequately responds to these lawsuits has become even more critical. But not all insurance policies offer the same coverage, and because of the increased litigation and regulatory enforcement around data privacy, many insurers have been attempting to restrict coverage for certain privacy violation claims.

Here are five considerations companies should be mindful of when placing and assessing coverage for lawsuits asserting privacy claims.

1. CONSIDER ALL POTENTIALLY APPLICABLE POLICIES

Various insurance policies may respond to a privacy class action complaint, and therefore, it is important to consider all potentially applicable policies as possible sources of coverage. Such potentially applicable policies include:

- *Cyber Policies*: These policies can vary greatly, and while they typically provide cover for data breaches, related regulatory investigations, or losses stemming from a network outage or service disruption, they also provide valuable coverage for privacy class action lawsuits, including coverage for defense costs, settlements, and regulatory fines or penalties that may arise from lawsuits alleging privacy law violations.

- *Media Liability Policies*: This insurance typically protects businesses from claims of defamation, trademark infringement, and copyright infringement arising from their media-related activities but frequently also provide coverage for invasion of privacy claims, particularly if those claims allege violations of privacy rights through media-related activities.

- *Commercial General Liability Policies*: Policyholders often neglect to consider coverage for privacy law violations under this traditional insurance product likely because these policies generally cover claims for bodily injury and property damage, which often are not the types of damages sought by privacy class action lawsuits. In addition, these policies generally exclude coverage for claims arising out of violation of laws, cyber risks, and electronic data liability. Nevertheless, these policies are worth a careful review as they just may provide cover for some privacy-related risks, including, for example, "personal and advertising injury" arising out of the publication of personal data or material in violation of an individual's right to privacy.

- *Directors & Officers (D&O) and Errors & Omissions (E&O) Policies*: These policies generally protect (1) a company's directors and officers from claims arising out of their management of the company or (2) a company from claims regarding misconduct in the provision of professional services, respectively. They are not ones that immediately come to mind when faced with a privacy class action lawsuit, but do not forget to carefully check the coverages afforded by them, particularly if the lawsuit's allegations arise from an officer's alleged misconduct or the services provided by the company. While these policies often contain exclusions for violations of privacy laws or the mishandling of third-party data (and therefore, will not cover damages or settlements arising from such claims), they may nonetheless provide critical defense costs coverage.

2. DO NOT HASTILY DISCOUNT THE POTENTIAL BENEFITS OF YOUR COVERAGE

After conducting a careful review of all potentially applicable policies, do not fail to seek coverage under any such policy for which the privacy class action lawsuit does not appear on its face to be the type of claim covered thereunder. Doing so discounts the potential benefits that your insurance can provide and for which your company paid substantial premiums. For instance, one benefit you could be foregoing by not seeking coverage is defense costs coverage—a valuable coverage provided under triggered policies.

The availability of defense cost coverage is determined by the allegations in the complaint, and is triggered if any claim in the complaint is potentially covered. Thus, if there is a potentially covered claim somewhere in the complaint, even if the main focus of the privacy class action is an allegation that may not ultimately be covered (or perhaps expressly excluded), your company may be able to recover valuable defense costs for its defense against the entire action. That coverage comes into play once the insurer's duty to defend or duty to advance defense costs has been triggered, which can only happen after the lawsuit has been noticed to the insurer and applicable deductibles/retentions are satisfied.

3. DETERMINE NOTICE REQUIREMENTS AND GIVE PROMPT NOTICE

Every insurance policy contains requirements about when the policyholder must notify the insurer of a claim (or potential claim). Compliance with such notice requirements is vital to coverage, especially so when dealing with "claims made" policies like cyber policies. Coverage under such policies is triggered based on the date of the underlying claim (as opposed to the date of the alleged injury), and thus, the notice provisions in these policies ensure that notice is provided during the current policy period. Failure to provide notice could negate coverage. More importantly, insurers often refuse to cover any defense costs that are incurred prior to the policyholder's tender of notice of the claim, so it is useful to provide prompt notice.

Timely notice is typically one of many conditions precedent to coverage. Thus, it is important for policyholders to comply with all of their policies' terms and conditions, including cooperation, consent to settlement, and voluntary payment requirements. An insurer may look to avoid its coverage obligations if you fail to comply with these terms and conditions.

4. WHEN IN DOUBT, CONSULT EXPERIENCED COVERAGE COUNSEL

Undoubtedly, there can be a number of complexities in seeking insurance coverage for privacy class action lawsuits. Thus, when in doubt, consulting counsel that are well versed and experienced in such coverage efforts is highly recommended. These individuals can help you avoid costly missteps that may make it more challenging to obtain coverage, including by explaining obtuse (and at times, archaic) policy language and advising on

what is needed to safeguard coverage. More importantly, these individuals can help you maximize the value and scope of your insurance coverage.

5. OBTAIN INSURANCE THAT PROVIDES ADEQUATE PRIVACY RISK COVERAGE

Each of the considerations discussed above focuses on steps to take once faced with a privacy class action lawsuit. But equally important if not more critical are the steps your company should take to protect against the inevitable onslaught of such lawsuits going forward.

One of those steps must be investing in insurance that will come into play when faced with privacy class action lawsuits. That in turn requires a few additional considerations.

- Fully assess your company's privacy risks for which insurance coverage is needed.
- Evaluate whether your insurance program safeguards against those risks, including by reviewing the privacy risk coverages potentially afforded by your current policies.
- Consult a broker on whether your insurance program is sufficiently robust to cover those privacy risks, and if not, what the appropriate coverages needed to do so are.
- Invest in appropriate and adequate cyber and privacy insurance.
- Negotiate exclusion wording (preferably in consultation with counsel and your broker) to ensure that those exclusions do not defeat your company's reasonable expectations for buying coverage. Given the influx of privacy class action lawsuits, insurers have pushed for broad exclusions for biometric privacy violations, website tracking tools and activities, and absolute artificial intelligence exclusions.

With the right coverage in place, your company will be better positioned to protect itself from financial losses stemming from privacy class action lawsuits in today's digital landscape.

Pratt's Privacy & Cybersecurity Law Report

VOLUME 12 **NUMBER 1** **January 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)

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.