AN A.S. PRATT PUBLICATION
MARCH-APRIL 2026
VOL. 12 NO. 3

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

EDITOR'S NOTE: THE FIRST EXCLUSION ORDER
Victoria Prussen Spears

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE ISSUES FIRST FASCSA EXCLUSION AND REMOVAL ORDER
Rajesh De, Adam S. Hickey, John Prairie, Tamer A. Soliman and Aaron Futerman

ANALYZING THE NEW AI COMPANION CHATBOT LAWS
Bianca Nalaschi

PENNSYLVANIA SUPREME COURT HOLDS NO REASONABLE EXPECTATION OF PRIVACY IN INTERNET SEARCH ACTIVITY: KEY TAKEAWAYS FOR EMPLOYERS
Risa B. Boerner, Catherine M. Contino, Jordan A. Jiles and Christopher J. Merken

GRAND JURY SECRECY REINFORCED: NINTH CIRCUIT BARS FOIA DISCOVERY OF SUBPOENAED DOCUMENTS PRODUCED PURSUANT TO RULE 6(e)
Jina L. Choi, Winston Y. Chan, Diana M. Feinstein, Benjamin Wagner and Erin Williams

2025 CYBER INCIDENT TRENDS: WHAT BUSINESSES NEED TO KNOW
Rajesh De, Ana Hadnes Bruder, Marcus A. Christian, Gabriela Kennedy, Justin Herring, Adam S. Hickey, Veronica R. Glick, Stephen Lilley, Amber C. Thomson, Kathryn Allen, Britteny L. Leyva, Hadassah G. Diament, and Oliver Yaros

EU CYBER REFORMS PROPOSED, INCLUDING OVERHAULED CYBERSECURITY ACT
Dessislava Savova, Holger Lutz, Gregory Sroussi, James Wong, Alexander Kennedy and Rita Flakoll

Pratt's Privacy & Cybersecurity Law Report

VOLUME 12 **NUMBER 3** **March-April 2026**

Editor's Note: The First Exclusion Order 69
Victoria Prussen Spears

Office of the Director of National Intelligence Issues First FASCSA Exclusion and Removal Order 71
Rajesh De, Adam S. Hickey, John Prairie, Tamer A. Soliman and Aaron Futerman

Analyzing the New AI Companion Chatbot Laws 75
Bianca Nalaschi

Pennsylvania Supreme Court Holds No Reasonable Expectation of Privacy in Internet Search Activity: Key Takeaways for Employers 82
Risa B. Boerner, Catherine M. Contino, Jordan A. Jiles and Christopher J. Merken

Grand Jury Secrecy Reinforced: Ninth Circuit Bars FOIA Discovery of Subpoenaed Documents Produced Pursuant to Rule 6(e) 86
Jina L. Choi, Winston Y. Chan, Diana M. Feinstein, Benjamin Wagner and Erin Williams

2025 Cyber Incident Trends: What Businesses Need to Know 90
Rajesh De, Ana Hadnes Bruder, Marcus A. Christian, Gabriela Kennedy, Justin Herring, Adam S. Hickey, Veronica R. Glick, Stephen Lilley, Amber C. Thomson, Kathryn Allen, Britteny L. Leyva, Hadassah G. Diament, and Oliver Yaros

EU Cyber Reforms Proposed, Including Overhauled Cybersecurity Act 96
Dessislava Savova, Holger Lutz, Gregory Sroussi, James Wong, Alexander Kennedy and Rita Flakoll

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.

Pennsylvania Supreme Court Holds No Reasonable Expectation of Privacy in Internet Search Activity: Key Takeaways for Employers

By Risa B. Boerner, Catherine M. Contino, Jordan A. Jiles and Christopher J. Merken*

In this article, the authors review a recent privacy-related decision by the Pennsylvania Supreme Court and discuss how this decision could impact private employers.

A recent Pennsylvania Supreme Court ruling could have broad implications for internet privacy, and employers should take note. The state's high court ruled in December that individuals do not have a reasonable expectation of privacy in their internet search activity for purposes of the Fourth Amendment and similar state constitutional protections. Although the case centered on a state police search in a criminal investigation, the decision will likely influence how courts applying Pennsylvania law analyze privacy expectations across a wide range of contexts, including matters concerning employment and the workplace.

This article discusses *Commonwealth v. Kurtz* and how this decision could impact private employers.

BACKGROUND ON *COMMONWEALTH V. KURTZ*

In an investigation into a violent crime, state police obtained a "reverse keyword search warrant" that instructed Google to identify anyone who searched the victim's name or home address in the week before the assault. Google informed the police that someone had searched the victim's address a few hours before the attack, and the investigators used this information (and the IP address used for the searches) to identify, track, obtain DNA evidence, and arrest the suspect, who confessed to the crimes and similar crimes involving four other victims.

When the cases went to trial, the defendant asked the court to suppress the evidence pulled from the police's search of Google's records, challenging the validity of the search warrant used to obtain them. After the trial court denied that request, a jury found Kurtz guilty on all counts, and the state's Superior Court affirmed.

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

PENNSYLVANIA SUPREME COURT: NO ENFORCEABLE EXPECTATION OF PRIVACY IN MOST INTERNET SEARCHES

The Supreme Court of Pennsylvania affirmed on December 16.[1]

- Kurtz argued that the state police violated his Fourth Amendment and state constitutional rights because the police failed to establish probable cause individualized to him when they obtained the search warrant for the Google records.

- However, the court held that the Fourth Amendment was not triggered at all because Kurtz did not have a reasonable expectation of privacy in his unprotected internet searches. It therefore declined to reach the probable cause challenge.

In deciding the case, the state's high court:

- emphasized that internet users knowingly and voluntarily transmit information to third-party service providers when they conduct online searches – and therefore cannot reasonably expect that such information will remain private. (In the court's words, although internet users may *believe* their searches are private, "even the ordinary, everyday use of the internet provides strong indicators that there is no privacy in the terms or information that the user voluntarily enters into a search engine.");

- rejected arguments that the Pennsylvania Constitution provides broader privacy protections for internet search activity than the federal Constitution, expressly holding that no reasonable expectation of privacy exists under either framework; and

- distinguished internet use from the Fourth Amendment protections granted to cell-site location information in a 2018 U.S. Supreme Court decision.[2] (The court explained that "the use of the internet is not an inextricable and involuntary aspect of our daily life in the same way that mobile phones have become" and "[t]hat the internet is helpful, readily available, and convenient does not render its use involuntary in such a way that a person today has no choice but to rely upon it and, derivatively, has no choice but to share information with third parties.")

---

[1] Commonwealth v. Kurtz, Nos. 98, 99, 100 MAP 2023 (Pa. Dec. 16, 2025), available at https://www.pacourts.us/assets/opinions/Supreme/out/J-36A-2024oajc%20-%20106611829340009817.pdf?cb=1.

[2] Carpenter v. United States, No. 16–402 (U.S. June 22, 2018), available at https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf.

Importantly, however, the Pennsylvania high court limited its decision to "general, unprotected internet use." The court made clear that internet users who take efforts "to secure some degree of privacy" may be afforded greater constitutional privacy protections. The court pointed to use of virtual private networks, internet browsers that do not collect or share data, and websites that are password-protected as examples of internet use that may permit users to "retain a constitutionally recognizable expectation of privacy."

HOW THIS DECISION COULD IMPACT THE WORKPLACE

Constitutional bans (whether state or federal) on unreasonable searches and seizures do not apply at all to purely private conduct. A private employer that is not acting as an agent of the government cannot violate an employee's constitutional privacy protections – though many other privacy laws and concerns must be considered. Although the *Commonwealth v. Kurtz* ruling directly addressed law enforcement's access to internet search information during criminal investigations, its practical implications could be far-reaching:

- *Workplace Investigations*: Internet searches and browsing history often are probative in workplace investigations of employee conduct, where employers confront questions about employee internet usage, browsing history, and online searches conducted on employer-provided devices or networks. This decision reinforces the principle that such activity lacks a reasonable expectation of privacy and supports an employer's ability to collect and rely on search data during internal investigations without triggering privacy violations, particularly when coupled with strong acceptable-use and electronic communications policies, as noted below.

- *Electronic Discovery and Litigation*: The court's reasoning may also influence how courts address privacy objections in civil discovery disputes. Litigants frequently resist producing browsing history, search terms, and related metadata because they argue that such information is highly personal or intrusive. However, now that the court has ruled that constitutional privacy protections do not automatically apply to internet search activity, Pennsylvania courts evaluating discovery disputes may be less receptive to objections where parties are found to have shared their search history or browsing data with third-party platforms, provided the requested information is relevant and proportional.

- *Technology and Privacy Policies*: As courts continue to recognize diminished expectations of privacy in online activity, employers should ensure that their acceptable-use and electronic communications policies accurately reflect how workplace technology is used and monitored. Clear policies can help set employee expectations, reduce the risk of privacy-based challenges, and strengthen an employer's position when reviewing internet

activity on employer-provided devices and networks in connection with investigations, compliance reviews, or litigation.

KEY TAKEAWAYS FOR EMPLOYERS

- Courts are increasingly skeptical of claims that internet search activity is private.
- The voluntary transmission of data to third parties significantly undermines privacy expectations.
- Employers should ensure their electronic communications and internet-use policies accurately reflect modern privacy realities.
- Even though this was a criminal case, its reasoning is likely to influence civil and employment-related disputes involving digital information.