

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. Diamant, 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 Victoria Prussen Spears	69
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	71
Analyzing the New AI Companion Chatbot Laws Bianca Nalaschi	75
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	82
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	86
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	90
EU Cyber Reforms Proposed, Including Overhauled Cybersecurity Act Dessislava Savova, Holger Lutz, Gregory Sroussi, James Wong, Alexander Kennedy and Rita Flakoll	96

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.

Grand Jury Secrecy Reinforced: Ninth Circuit Bars FOIA Discovery of Subpoenaed Documents Produced Pursuant to Rule 6(e)

*By Jina L. Choi, Winston Y. Chan, Diana M. Feinstein, Benjamin Wagner
and Erin Williams**

In this article, the authors review a decision by the Ninth Circuit Court of Appeals that clarifies ambiguity around pre-existing documents and the scope of Federal Rule of Criminal Procedure 6(e), providing strong protection for companies responding to federal grand jury subpoenas.

In a significant ruling for companies responding to federal grand jury subpoenas, the Ninth Circuit has issued what may be its most definitive decision to date on the scope of Federal Rule of Criminal Procedure 6(e) and its interaction with the Freedom of Information Act (FOIA).

In *Kalbers v. U.S. Department of Justice and Volkswagen AG*,¹ the court held that FOIA Exemption 3, incorporating Rule 6(e) bars disclosure of documents that the government possesses solely because they were produced in response to a grand jury subpoena. This includes pre-existing documents such as emails, corporate records and other documents created before and independent of the grand jury investigation.

TAKEAWAYS

- The Ninth Circuit held that documents in the government's possession solely because of a grand jury subpoena are categorically protected from disclosure by the government under Rule 6(e), even if the documents predated the grand jury investigation.
- The decision should give greater assurance to companies producing documents in response to a grand jury subpoena that the documents will not subsequently be obtained from the DOJ by plaintiff's counsel, state regulators or other interested parties.
- While *Kalbers* was decided in the context of a FOIA request addressed to DOJ, companies may still face discovery requests in civil litigation for

* The authors, attorneys with Gibson, Dunn & Crutcher LLP, may be contacted at jchoi@gibsondunn.com, wchan@gibsondunn.com, dfeinstein@gibsondunn.com, bwagner@gibsondunn.com and ewilliams@gibsondunn.com, respectively.

¹ *Kalbers v. Volkswagen AG*, Nos. 24-1048 & 24-1477 (9th Cir. Jan. 30, 2026).

documents they produced pursuant to a grand jury subpoena. Companies should attempt to use the language and reasoning in *Kalbers* to reject demands for wholesale reproduction or cloned discovery requests by other regulators or civil litigants who try to get these documents.

- Documents being produced pursuant to Rule 6(e) should be clearly labeled as such to strengthen confidentiality protections.

BACKGROUND

Rule 6(e) of the Federal Rules of Criminal Procedure strictly prohibits the government from disclosing any “matter occurring before the grand jury.”² This has been widely understood to prevent the disclosure of grand jury transcripts, witness testimony, subpoenas, and other documents relating to the grand jury proceedings themselves. However, the degree to which the rule prevents the disclosure of pre-existing documents that are simply received by a grand jury pursuant to subpoena has been less clear.³ That uncertainty has posed risks for companies responding to grand jury subpoenas, particularly because plaintiffs’ counsel, state regulators, and other parties frequently seek access to the evidence considered by the federal grand jury to advance their own subsequent civil or regulatory claims.

The *Kalbers* case arose when Lawrence Kalbers, a professor at Loyola Marymount University, took an interest in a settlement agreement between the DOJ and the Defendant in a matter involving emissions testing. Kalbers filed a FOIA request with the Department of Justice seeking all documents that the Defendant produced to the DOJ during a criminal grand jury investigation that ultimately resulted in a plea agreement. The DOJ had obtained approximately six million documents through a grand jury subpoena, nearly all of which were labeled “FOIA Confidential – Produced Pursuant to Rule 6(e).”

The district court ordered production of the documents, adopting the Special Master’s recommendation that—unlike witness lists, subpoenas, or testimony summaries—the documents themselves did not reveal grand jury deliberations. DOJ and the Defendant appealed.⁴

THE NINTH CIRCUIT’S DECISION

The Ninth Circuit reversed in substantial part, holding that Rule 6(e) bars disclosure of documents that the government possesses only because of a grand jury subpoena. The

² See Federal Rules of Criminal Procedure (Dec. 1, 2024), https://www.uscourts.gov/sites/default/files/2025-02/federal-rules-of-criminal-procedure-dec-1-2024_0.pdf.

³ See Article, Toward a Safety Valve for Sharing Documents Obtained by Grand Jury Subpoena in Parallel Investigations, in Department of Justice Journal of Federal Law and Practice Volume 70, Issue 3, 105, 113, (Aug., 2022), <https://www.justice.gov/usao/page/file/1532986/dl?inline>.

⁴ *Kalbers v. Volkswagen AG*, Nos. 24-1048 & 24-1477, slip op. at 9–10 (9th Cir. Jan. 30, 2026).

court explained that disclosure of such materials—particularly in the aggregate—would allow requesters to “reverse engineer” the grand jury’s investigation by revealing what topics, time periods, and individuals were of interest to prosecutors.⁵

Critically, the court rejected the argument that pre-existing documents lose Rule 6(e) protection simply because they were created outside the grand jury process. Instead, the relevant inquiry is how the government obtained the documents, not when or why the documents were originally created.⁶

The court further clarified that prior Ninth Circuit cases like *U.S. v. Dynavac, Inc.* and *In re Optical Disk Drive Antitrust Litig.*, allowed the disclosure of documents that were in the possession of an independent source (a private corporation, in the case of *Dynavac*) or were in the possession of the government independent of a grand jury proceeding (FBI recordings made independent of the grand jury proceeding, in the case of *Optical Disk*).⁷ If the documents are in the government’s possession only through the grand jury subpoena, Rule 6(e) protection applies.⁸

SIGNIFICANCE AND PRACTICE CONSIDERATIONS

This decision clarifies ambiguity around pre-existing documents and the scope of Rule 6(e), providing strong protection for companies responding to federal grand jury subpoenas. It confirms that Rule 6(e) shields not only grand jury transcripts and deliberations, but also the document productions themselves, as disclosure would reveal the nature or scope of the investigation.

The language in *Kalbers* supports broad protections over documents produced pursuant to grand jury subpoenas. The circuits are varied on the level of protection that Rule 6(e) provides. While few cases have held that the subpoena file itself is protected,⁹ the Sixth Circuit has established a strong presumption that any documents provided for a grand jury investigation constitute “matters occurring before the grand jury,” and are therefore protected.¹⁰

By contrast, the Second Circuit has taken a narrower view of Rule 6(e), emphasizing that “documents are not cloaked with secrecy merely because they are presented to a grand jury,”¹¹ and that the government must show that disclosing the documents would reveal protected aspects of the grand jury’s investigation in order to justify withholding them.¹²

⁵ *Kalbers v. Volkswagen AG*, Nos. 24-1048 & 24-1477, slip op. at 14–16 (9th Cir. Jan. 30, 2026).

⁶ *Kalbers v. Volkswagen AG*, Nos. 24-1048 & 24-1477, slip op. at 17–18, 21–22 (9th Cir. Jan. 30, 2026).

⁷ *Kalbers v. Volkswagen AG*, Nos. 24-1048 & 24-1477, slip op. at 17–18, 21–22 (9th Cir. Jan. 30, 2026); *United States v. Dynavac, Inc.*, 6 F.3d 1407, 1411–14 (9th Cir. 1993); *In re Optical Disk Drive Antitrust Litig.*, 801 F.3d 1072, 1077–78 (9th Cir. 2015).

⁸ *Kalbers v. Volkswagen AG*, Nos. 24-1048 & 24-1477, slip op. at 21 (9th Cir. Jan. 30, 2026).

⁹ *Kalbers v. Volkswagen AG*, Nos. 24-1048 & 24-1477, slip op. at 16 (9th Cir. Jan. 30, 2026).

¹⁰ *In re Grand Jury Proc.*, 851 F.2d 860, 863 (6th Cir. 1988).

¹¹ *United States v. Lartey*, 716 F.2d 955, 964 (2d Cir. 1983).

¹² *Grynberg v. U.S. Dep’t of Justice*, 758 F. App’x 162, 164 (2d Cir. 2019).

The D.C. Circuit has held that there is “no per se rule against disclosure of any and all information which has reached the grand jury chambers” and it required a case-specific inquiry into whether disclosure would reveal a secret aspect of the grand jury’s investigation.¹³

Overall, *Kalbers* is a favorable decision for targets of grand jury investigations and third parties alike, reinforcing the confidentiality of grand jury processes and providing meaningful assurance that the DOJ will not be compelled under FOIA to produce documents to third parties. While companies may still face discovery requests and demands in civil litigation for documents produced pursuant to grand jury subpoena, the language and reasoning in *Kalbers* provide compelling arguments to reject wholesale reproduction and cloned discovery requests.

The *Kalbers* decision also underscores the practical importance of labeling documents produced in response to a grand jury subpoena as grand jury material. The Ninth Circuit relied heavily on the fact that the vast majority of documents at issue were expressly marked as produced pursuant to Rule 6(e), treating those labels as strong evidence that disclosure would reveal matters occurring before the grand jury.¹⁴ At the same time, *Kalbers* makes clear that production to the grand jury limits disclosure only by the government—principally by barring third parties from obtaining the documents through FOIA. It does not transform the documents themselves into privileged material or otherwise shield them from disclosure by the producing company if sought from an independent source, including through civil discovery.¹⁵

The decision may also affect how companies weigh voluntary production versus responding to a grand jury subpoena at least within the Ninth Circuit. While voluntary production can signal cooperation, only documents produced in response to a grand jury subpoena are eligible to receive stronger protection from FOIA disclosure because of Rule 6(e) under *Kalbers*, which in some cases may favor compelled production where disclosure risk is a key concern.

¹³ *Lopez v. Dep’t of Justice*, 393 F.3d 1345, 1349 (D.C. Cir. 2005).

¹⁴ *Kalbers v. Volkswagen AG*, Nos. 24-1048 & 24-1477, slip op. at 22–23 (9th Cir. Jan. 30, 2026).

¹⁵ *Kalbers v. Volkswagen AG*, Nos. 24-1048 & 24-1477, slip op. at 17–18, 21–22 (9th Cir. Jan. 30, 2026); cf. *United States v. Dynavac, Inc.*, 6 F.3d 1407, 1411–12 (9th Cir. 1993).