

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.

Securities and Exchange Commission Settles With Companies Over Charges Relating to Cybersecurity Disclosures

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

In this article, the authors discuss recent settlements reached by the Securities and Exchange Commission with four current or former publicly traded companies that allegedly disseminated materially misleading disclosures regarding cybersecurity risks and actual infiltrations.

In October 2024, the Securities and Exchange Commission (SEC) charged four current or former publicly traded companies with disseminating materially misleading disclosures regarding cybersecurity risks and actual infiltrations. The charges arose from an investigation of companies impacted by the well publicized 2020 cybersecurity incident involving SolarWinds Corporation's flagship Orion software platform.

The SEC charged that each of these companies learned in either 2020 or 2021 that the perpetrator of the SolarWinds Orion cyberattack had also infiltrated their respective systems, but in their respective public disclosures in 2021 and/or 2022, each company negligently minimized the impact of the cybersecurity incident.

The SEC staff reiterated its position that, although public companies may be victims of cyberattacks, they may not harm their shareholders or the investing public by issuing misleading disclosures about such cybersecurity incidents. The SEC alleged that each company violated Section 13(a) of the Securities Exchange Act of 1934, as amended, as well as the respective rules promulgated thereunder that require public companies to file annual, quarterly and current reports in conformity with the SEC's rules and regulations.

THE SETTLEMENTS

The companies agreed to settle the SEC's charges as follows:

- Company A agreed to a \$990,000 civil penalty:
 - In multiple Forms 8-K filed in 2021, Company A minimized the severity of the attack on it by, among other things, failing to disclose the quantity of encrypted credentials accessed by the threat actor;
- Company B agreed to a \$1 million civil penalty:

* The authors, attorneys with Polsinelli, may be contacted at ewu@polsinelli.com, psternberg@polsinelli.com and mquinn@polsinelli.com, respectively.

- Company B disclosed in a Form 10-Q filed in February 2021 that the threat actor had accessed a limited number of email messages; in reality, Company B was already aware the threat actor accessed over 100 files in its cloud file sharing environment;
- Company C agreed to a \$995,000 civil penalty:
 - Even though Company C was aware of the intrusion, it described cyber intrusions and related risks in a generic fashion in its Annual Reports on Form 20-F filed in both 2021 and 2022; and
- Company D agreed to a \$4 million civil penalty:
 - Company D described its risks from hypothetical future cybersecurity events in its Annual Reports on Form 10-K filed in both 2021 and 2022, even though it was aware it had already experienced two intrusions related to SolarWinds; and
 - In addition, the SEC charged Company D with violations relating to disclosure controls and procedures, resulting in such materially misleading disclosures.

According to the SEC, the latter two companies, in particular, did not comply with SEC Staff guidance articulated in 2011 and 2018 that registrants refrain from drafting cybersecurity risk factors as hypothetical or generic when already aware that those risks had fully materialized.¹

At the time of the SolarWinds incident, ransomware was just beginning to enter the public consciousness. Since then, cybersecurity attacks have become more sophisticated and at the same time more common. Ransomware attacks and widespread third-party incidents have especially gained prominence as companies increasingly grapple with vendor risk management and supply chain attacks. In part because of the “success” of those attacks, ransomware is now one of, if not the most, common type of attack companies experience. Attacks on vendors that are focal points in a particular industry

¹ In the 2018 Commission Statement and Guidance on Public Company Cybersecurity Disclosure (SEC Release Nos. 33-10459; 34-82746), the SEC’s interpretive guidance specified that “. . . if a company previously experienced a material cybersecurity incident involving denial-of-service, it likely would not be sufficient for the company to disclose that there is a risk that a denial-of-service incident may occur . . . Instead, the company may need to discuss the occurrence of that cybersecurity incident and its consequences. . . .”

In the 2011 SEC Division of Corporation Finance Disclosure Guidance: Topic No. 2, the Division specified that “. . . if a registrant experienced a material cyber attack in which malware was embedded in its systems and customer data was compromised, it likely would not be sufficient for the registrant to disclose that there is a risk that such an attack may occur.”

or that act as a key point in a supply chain can cripple an entire sector of the economy or simultaneously provide hackers with access to data or networks of a wide range of companies. Examples of supply chain attacks are the 2023 MoveIt vulnerability that compromised the data of hundreds of organizations and the June 2024 CDK Global attack, which disrupted auto sales nationwide.

REPORTING OBLIGATIONS HAVE EXPANDED

As cybersecurity attacks have expanded become more prevalent, the reporting obligations have also expanded. In July 2023, the SEC adopted new cybersecurity disclosure rules, which create more prescriptive data security incident disclosure requirements. Significantly, a “material cybersecurity incident” now must be disclosed under Item 1.05 of Form 8-K within four business days of the date such cybersecurity incident is determined to be material.

While any cybersecurity attack can create challenges to comply with the SEC’s reporting obligations, especially in light of the new requirement to disclose within four business days of a materiality determination, the ransomware and vendor focused attacks present unique challenges. In the case of a ransomware attack, assessing the incident and communicating about it publicly can be very difficult when an organization is trying to recover from the attack and restore operations. And, in the case of a vendor incident, the lack of access to the compromised network and the often limited information about the incident makes accurately reporting an incident challenging.²

CONCLUSION

The SEC’s 2023 rulemaking and its actions described above illustrate its continued focus on public companies’ cybersecurity disclosures. Accordingly, reporting companies should review their disclosure controls and procedures to confirm their effectiveness in enabling compliance with the SEC’s cybersecurity disclosure rules in connection with future cybersecurity incidents that may impact them directly or indirectly.

² The July 2023 adopting release clarifies that “the definition of ‘information systems’ contemplates those resources owned by third parties and used by the registrant” (SEC Release Nos. 33-11216; 34-97989, *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*). As such, a third-party incident may result in a material cybersecurity incident for a reporting company.