AN A.S. PRATT PUBLICATION
FEBRUARY 2024
VOL. 10 NO. 2

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 10 **NUMBER 2** **February 2024**

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 [82] (LexisNexis A.S. Pratt)

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

(2024–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

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. 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.

Federal Communications Commission Expands Privacy and Data Protection Work with States to Increase Investigations

By Megan L. Brown, Duane C. Pozza, Kevin G. Rupy, Kathleen E. Scott, Sydney M. White and Stephen J. Conley*

In this article, the authors lay out implications of the new Memoranda of Understanding the Federal Communications Commission recently signed with several states "to share expertise, resources, and coordinated efforts in conducting privacy, data protection, and cybersecurity-related investigations to protect consumers."

Federal Communications Commission (FCC or Commission) Chairwoman Jessica Rosenworcel has issued a press release (Press Release)[1] announcing that the agency's Privacy and Data Protection Task Force (Task Force) has signed Memoranda of Understanding (MOUs) with the Connecticut, Illinois, New York, and Pennsylvania Attorneys General "to share expertise, resources, and coordinated efforts in conducting privacy, data protection, and cybersecurity-related investigations to protect consumers."

These states have traditionally been aggressive on data security investigations, so this is a notable development. The announcement also continues to stake out claims to new agency authorities under Sections 201 and 222 of the Communications Act (the Act). This article lays out implications of the new MOUs in the context of expanding regulation and oversight of communications sector privacy and security.

WHAT IS THE FCC'S PRIVACY AND DATA PROTECTION TASK FORCE?

Chairwoman Rosenworcel launched the Task Force in a speech in June.[2] The Task Force[3] is led by FCC Enforcement Bureau Chief Loyaan A. Egal,[4] a former official in the Department of Justice's National Security Division. The FCC describes the Task Force as an FCC staff working group that will "coordinate across the agency on the rulemaking, enforcement, and public awarenes needs in the privacy and data protection sectors."[5]

---

* The authors, attorneys with Wiley Rein LLP, may be contacted at mbrown@wiley.law, dpozza@wiley.law, krupy@wiley.law, kscott@wiley.law, swhite@wiley.law and sconley@wiley.law, respectively.

[1] https://docs.fcc.gov/public/attachments/DOC-398939A1.pdf.

[2] https://docs.fcc.gov/public/attachments/DOC-394386A1.pdf.

[3] https://www.fcc.gov/privacy-and-data-protection-task-force.

[4] https://www.fcc.gov/about-enforcement-bureau/loyaan-egal-2.

[5] https://docs.fcc.gov/public/attachments/DOC-394384A1.pdf. The Task Force is made up of the Office of the Chairwoman, the Enforcement Bureau, the Public Safety and Homeland Security Bureau, the Wireline Competition Bureau, the Consumer and Governmental Affairs Bureau, the Space Bureau, the Media Bureau, the Office of the General Counsel, the Office of the Managing Director, the Office of International Affairs, the Office of Engineering and Technology, and the Office of Economics and Analytics.

The FCC's Enforcement Bureau has a team specifically dedicated to "investigat[ing] and enforc[ing] violations of the Commission's privacy and data protection laws and rules[,]" and this team will be expanded going forward, including by adding personnel with national security experience and clearances necessary "to review classified information and better coordinate with national security colleagues in assessing risks involving the communications . . . and supply chain sectors."[6] The Task Force focuses attention on privacy and security issues, on which the agency has been increasingly assertive.

THE PRESS RELEASE FOCUSES ON THE FCC'S AUTHORITY UNDER SECTIONS 201 AND 222

According to the Press Release, the MOUs assert that the FCC and the state attorneys general "share close and common legal interests" in working to investigate and take enforcement action concerning "privacy, data protection or cybersecurity issues."[7] Notably, the Press Release characterizes the FCC's regulatory interest as arising under Sections 201 and 222 of the Act, provisions that the agency has been using lately in a controversial way.

Section 222 of the Act requires telecommunications carriers and interconnected VoIP providers (collectively, carriers) to protect the privacy and security of their customers' telecommunications service-related data and billing information, which the statute defines as "customer proprietary network information" (CPNI). The Commission's rules implementing Section 222 also require carriers to notify customers, the Federal Bureau of Investigation, and the U.S. Secret Service of breaches that expose CPNI. Section 201(b) of the Act, meanwhile, provides that the FCC "may prescribe such rules and regulations as may be necessary in the public interest to carry out the provisions" of the Act related to wire and radio communication services.[8] In addition to Sections 201 and 222, the Press Release also notes that "[c]oordination action and information sharing will take place under all applicable Federal and State laws and privacy protections."[9]

Although the Act presently gives the Commission authority to investigate carrier breaches involving the intentional unauthorized access to, use, or disclosure of CPNI, the agency is about to expand its carrier breach reporting requirement to cover "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual."[10] This move has received substantial pushback from regulated entities.

---

[6] https://www.fcc.gov/privacy-and-data-protection-task-force.
[7] https://docs.fcc.gov/public/attachments/DOC-398939A1.pdf.
[8] 47 U.S.C. § 201(b).
[9] https://docs.fcc.gov/public/attachments/DOC-398939A1.pdf.
[10] https://docs.fcc.gov/public/attachments/DOC-398669A1.pdf.

LOOKING AHEAD

Like the FCC's establishment of the Task Force in June, this announcement is a reminder that the Commission is taking an assertive approach to privacy and data security. The Press Release encourages "other state leaders" and "other federal agencies" to work with the Task Force. The FCC has been pioneering robocalling investigations with states and other agencies, and the FCC has executed MOUs with 48 states,[11] and the District of Columbia. It is moving increasingly into more novel uses of investigative powers to explore areas that traditionally would have been in the purview of the Federal Trade Commission (FTC) and the states.

Indeed, regulated companies that receive letters of inquiry (LOI) or other communications from the FCC, FTC, or states should consider that multiple enforcement agencies may be involved in any investigation. The LOIs may be more extensive, and agencies may share information subject to their statutory authorities and MOUs. For example, the FCC and FTC also have an existing MOU on consumer protection matters that reinforces their coordination and information sharing.[12] In our experience, the presence of multiple investigating agencies increases the complexity of investigations and negotiations, and should be factored into companies' approaches in responding to inquiries of all types.

We can expect increased collaboration between the FCC and federal and state agencies in the cyber and privacy enforcement space. However, timelines and the scope of future partnerships are unclear, so it will be worth keeping an eye on the Task Force to see how this initiative progresses.

[11] https://www.fcc.gov/fcc-state-robocall-investigation-partnerships.

[12] https://www.ftc.gov/system/files/documents/cooperation_agreements/151116ftcfcc-mou.pdf.