AN A.S. PRATT PUBLICATION
SEPTEMBER 2023
VOL. 9 NO. 7

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 9 **NUMBER 7** **September 2023**

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Alexandra Jefferies at ..... (937) 560-3067
Email: ..... alexandra.jefferies@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*, [1] 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

(2023–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 Launches Privacy and Data Protection Task Force

By Megan L. Brown, Kathleen E. Scott and Kyle M. Gutierrez*

In this article, the authors provide an overview of what is known about the Federal Communications Commission's new Privacy and Data Protection Task Force, potential privacy-related actions the Commission may take now that the Task Force is in place, and questions that the Task Force's creation raises about the Commission's future role in the privacy regulatory space.

In a speech[1] at the Center for Democracy and Technology (CDT), Federal Communications Commission (FCC or Commission) Chairwoman Jessica Rosenworcel announced that the FCC is launching a new, "first-ever" "Privacy and Data Protection Task Force" (Task Force) at the Commission.

Emphasizing that the FCC "has an important role to play in ensuring the privacy of consumer communications" and that it needs to "concentrate [its] efforts" on the "magnitude of privacy challenges we face," Chairwoman Rosenworcel explained that the Task Force will bring "technical and legal experts together from across the agency to maximize coordination and use the law to get results – by evolving [the agency's] policies and taking enforcement action."

This article provides an overview of what we know about the Task Force thus far, potential privacy-related actions the Commission may take now that the Task Force is in place, and questions that the Task Force's creation raises about the Commission's future role in the privacy regulatory space.

WHAT IS THE TASK FORCE, WHO WILL BE ON IT, AND WHAT WILL IT DO?

According to the press release[2] announcing its launch, the Task Force is an FCC staff working group that will "coordinate across the agency on the rulemaking, enforcement, and public awareness needs in the privacy and data protection sectors." Those needs include "data breaches – such as those involving telecommunications providers and related to cyber intrusions – and supply chain vulnerabilities involving third-party vendors that service regulated communications providers."

---

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

1 https://docs.fcc.gov/public/attachments/DOC-394386A1.pdf.

2 https://docs.fcc.gov/public/attachments/DOC-394384A1.pdf.

The Commission has launched a page[3] on its website dedicated to the Task Force that provides an overview of the Task Force, commentary on the Commission's past and ongoing privacy actions, and notes on potential future FCC privacy actions (see below), though without much in the way of detail. The Task Force's website also includes a set of privacy protection tips for consumers.

The Commission has not provided much information on how the Task Force will be staffed. Enforcement Bureau Chief Loyaan A. Egal[4] will lead the Task Force, but beyond that, the Commission has only explained that the Task Force will be made up of "staff from across the agency that handle topics including enforcement, equipment authorization, data breach reporting requirements, and undersea cables."

According to the Task Force's website, the Bureaus and Offices that will be included on the Task Force are: 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.

Based on the Task Force website, enforcement appears to be a key focus. The website explains that the 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 that 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."

The website further emphasizes that the Enforcement Bureau "will use its resources and the FCC's discovery and subpoena authorities to procure information not only from regulated communications providers, but also from relevant third parties, including companies that are part of the communications supply chain and who handle customer data[,]" and will "exercise its monetary penalty authority to ensure compliance with the Act and its rules."

THE TASK FORCE COMES AMIDST SEVERAL PRIVACY AND SECURITY-RELATED WORKSTREAMS AT THE FCC

Chairwoman Rosenworcel's remarks to the CDT make clear that the Task Force "will have input in several ongoing efforts at the agency[,]" making privacy and data protection a top priority for the Commission. Specifically, she explained that the Task Force will:

---

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

[4] https://www.fcc.gov/sites/default/files/loyaan-a-egal-bio.pdf.

1. Be involved in the FCC's efforts to "modernize" its data breach rules to address breaches that "make vulnerable [customer's] sensitive data[,]" and be charged "with overseeing the investigations and enforcement actions that follow these data breaches."

2. "[H]elp with the development of rules to crack down on SIM-swapping fraud." To this end, the Commission intends to "follow up with an effort to adopt new rules in place to put a stop to these scams."

3. "[P]lay a role in [the Commission's] work under the Safe Connections Act[,]" which helps support access to communications for survivors of domestic violence.

4. "[T]ake a look at the data [the Commission] amassed last year" when Chairwoman Rosenworcel sought information about geolocation data retention and privacy practices from the nation's 15 largest mobile carriers. According to Chairwoman Rosenworcel, the Commission has "investigations underway to follow up on this data gathering, and the Task Force will assume Responsibility for this effort."

Chairwoman Rosenworcel also addressed pending enforcement actions, and emphasized that she intends to show "that this Task Force means business" from the get-go.

THE TASK FORCE ENTERS A CROWDED FIELD OF FEDERAL ACTION ON PRIVACY, CYBERSECURITY, AND DATA PROTECTION

The Task Force's launch is just one of a myriad of recent federal privacy, cybersecurity, and data protection actions. In March, the White House Office of the National Cyber Director released the National Cybersecurity Strategy,[5] which calls for new regulations in several areas. Multiple workstreams have been underway for years, many promoting collaborative and innovative solutions while others are more prescriptive.

The Federal Trade Commission (FTC) released revisions to its Safeguards Rule[6] for financial institutions, which went into effect on June 9, 2023, and issued a policy statement on biometric information in May, among many ongoing proceedings, including consideration of new rules. The Department of Homeland Security (DHS) is working on several cybersecurity programs including new incident reporting mandates from Congress. DHS is the cybersecurity risk management agency for the Communications Sector and has been the locus of important security work.

[5] https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

[6] https://www.ftc.gov/legal-library/browse/rules/safeguards-rule.

While the Commission's role in federal privacy efforts has long been relatively siloed to regulating "customer proprietary network information" (CPNI), the FCC has been dipping its proverbial toe in the broader privacy regulation waters for some time. For example, in January, the Commission released a Notice of Proposed Rulemaking[7] proposing major changes to the agency's regulation of customer data, and in doing so inquired about its authority to require breach reporting for social security numbers and other financial information far afield from the CPNI it has traditionally regulated.

By launching the Task Force, the agency has made clear that it is throwing its hat in the ring to be a player in the future of the federal privacy regulatory landscape. But though the Task Force website provides some level of information about what the Task Force will be doing, important questions remain about how the FCC's foray into this space will work. For example:

- What will the FCC's role be in interacting with other federal agencies that are entrenched in the privacy space? Chairwoman Rosenworcel in 2022 reconstituted a Federal Interagency Cybersecurity Forum, with herself as the chair, but the relation of this and the new FCC Task Force to other councils and interagency efforts is not clear.

- Where does the FCC's authority to launch the Task Force and take these additional privacy actions come from? Chairwoman Rosenworcel explained that "the law provides [the Commission] with clear communications privacy authority, including Section 222 and Section 631 of the Communications Act[,]" and the Task Force website notes that the Telecommunications Act requires carriers to "protect the privacy and security of their customers' service-related and billing information[.]" But to what extent would the Task Force's efforts constitute an expansion of this authority?

- Will the Task Force create tension with or duplication of federal data protection and privacy efforts, like the FTC's rulemakings and enforcement actions or the Cybersecurity and Infrastructure Security Agency's work on critical infrastructure incident reporting?[8]

- Given the cross-disciplinary nature of the Task Force, how will it use and protect information that is provided to the agency by private companies, either through another agency or via the FCC's own investigations. The FCC notes it may seek information from an array of companies through letter of inquiry or subpoena, and the FCC may obtain some information

[7] https://docs.fcc.gov/public/attachments/FCC-22-102A1.pdf.

[8] https://www.federalregister.gov/documents/2022/09/12/2022-19551/request-for-information-on-the-cyber-incident-reporting-for-critical-infrastructure-act-of-2022.

> about breaches and cyber incidents from DHS and other agencies. But federal policy has long emphasized the need to protect security information provided by private companies. For example, in passing the Cybersecurity Information Sharing Act of 2015, Congress made a point to ensure that information voluntarily shared with the government would not be used for regulatory or enforcement purposes. How will the FCC honor this approach, and how will it handle confidential information provided to the agency from collateral uses or abuses?

The Task Force website is notably silent on certain issues, as there is no mention of the Commission's Communications Security, Reliability, and Interoperability Council,[9] Technological Advisory Council,[10] or the National Cybersecurity Strategy.

LOOKING AHEAD

The FCC's announcement is a reminder that the agency is taking an assertive role on privacy and may not defer to other agencies' work or roles. We can expect continued regulatory and enforcement activity in privacy, data protection, and cyber. Timelines and scope of future action by the Commission are unclear, so it will be worth keeping an eye on the Task Force's website to see how its work progresses.

[9] https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-council-0.

[10] https://www.fcc.gov/general/technological-advisory-council.