wiley

ALERT

FCC Expands Privacy and Data Protection Work with States to Increase Investigations

December 7, 2023

Federal Communications Commission (FCC or Commission) Chairwoman Jessica Rosenworcel issued a Press Release yesterday announcing that the agency's Privacy and Data Protection Task Force (Task Force) 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 advisory draws on the firm's experience before FCC and state enforcers and in dealing with privacy and data security investigations, to lay 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?

As we explained when it was announced, Chairwoman Rosenworcel launched the Task Force in a speech this June. The Task Force is led by FCC Enforcement Bureau Chief Loyaan A. Egal, 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 awareness needs in the privacy and data protection sectors." [1] 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

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Duane C. Pozza
Partner
202.719.4533
dpozza@wiley.law

Kevin G. Rupy
Partner
202.719.4510
krupy@wiley.law

Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law

Sydney M. White
Special Counsel
202.719.3425
swhite@wiley.law

Stephen J. Conley
Associate
202.719.4572
sconley@wiley.law

Practice Areas

FTC and Consumer Protection
Privacy, Cyber & Data Governance
State Privacy Laws
Telecom, Media & Technology

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 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." 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. 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."

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." This move has received substantial pushback from regulated entities.

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 agency has been pioneering robocalling investigations with states and other agencies, and the FCC has executed MOUs with 48 states, and the District of Columbia. The FCC 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. 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.

***

Wiley's Privacy, Cyber & Data Governance Team has helped companies of all sizes from various sectors manage multijurisdictional government investigations, including FCC investigations under Sections 201 and 222 of the Communications Act. Please reach out to any of the authors with questions.

[1] 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.