Published on *The National Law Review* https://natlawreview.com

FCC Partners With States to Increase on Privacy and Data Protection Investigations, Signaling Increased Focus on Future Enforcement

Article By:

Jonathan P. Garvin

The Federal Communications Commission ("FCC") announced Thursday that in furtherance of the work of the agency's Privacy and Data Protection Task Force, the FCC's Enforcement Bureau signed Memoranda of Understanding ("MOU") with the Attorneys General of Connecticut, Illinois, New York, and Pennsylvania to share expertise and resources and to coordinate efforts conducting privacy, data protection and cyber-security-related investigations. These states have been some of the most aggressive privacy and data security regulators in the past, making these MOUs especially noteworthy.

In addition, the announcement indicates that the FCC intends to rely on authority under Sections 201 and 222 of the Communications Act to increase its investigation and enforcement activity concerning privacy, data protection, and cybersecurity issues. Section 222 generally requires carriers and VoIP providers to protect their customer proprietary network information ("CPNI"), such as service-related billing information. Under the current rules implementing Section 222, carriers and VoIP providers must notify customers, the Federal Bureau of Investigation, and the U.S. Secret Service of data breaches that may have exposed CPNI. The FCC also has the authority to investigate breaches involving intentional unauthorized access to, use, or disclosure of CPNI.

Like the current announcement, the FCC has taken other actions this year

indicating that it believes its authority under Title II of the Communications Act (the "Act"), including Section 222, permits the agency to expand its current privacy, data protection, and cybersecurity activities.

First, as we reported in January, the FCC has proposed rules that would expand the scope of its breach-reporting requirements to include inadvertent breaches as well as breaches involving "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." In that proceeding, the FCC proposes to rely on its authority under Section 222.

Likewise, the FCC has recently proposed reclassifying broadband internet access service ("BIAS") as a telecommunications service under Title II of the Communications Act. One stated reason behind the proposed change has been that by reclassifying BIAS as a telecommunications service, the FCC can, among other things, expand its privacy, data protection, and cybersecurity authority, with Chairwoman Rosenworcel explaining that "[r]eclassification would place the Commission on firm footing to protect Americans and partner even more effectively with our sister national security agencies on the same goal. Those partners have already asked the FCC to examine all solutions and authority to help secure our networks. And gaps in our authority have already manifested and hindered our ability to defend against known threats."

Taken together, these Commission actions signal that the agency plans to focus on and take a more active approach to privacy, data protection, and cyber security issues going forward. While the timing and scope of these new partnerships have not yet crystalized, it is worth monitoring the further actions as well as those of its new state-based partners and other agencies like the Federal Trade Commission that operate in this area.

National Law Review, Volume XIII, Number 342