LAW360

Portfolio Media. Inc. | 230 Park Avenue, 7th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

What To Watch As The FCC Leans Into National Security

By **David Plotinsky and Patricia Cave** (October 24, 2023, 5:13 PM EDT)


David Plotinsky


Patricia Cave

Recent actions by the U.S. Federal Communications Commission indicate that it continues to lean forward on national security issues, and that the FCC is not merely comfortable acting in this space but rather is actively seeking additional opportunities to effectively become a national security regulator.

During the tenure of former FCC Chair Ajit Pai, the FCC's exercise of authority on national security matters was generally limited — its most significant national security action was arguably promulgating new rules restricting a small subset of providers from using FCC funds to purchase or use telecommunications network equipment from certain Chinese-owned manufacturers.

Under the leadership of Chair Jessica Rosenworcel, however, the FCC has increasingly sought to insert itself in efforts to address national security risk, including by taking more expansive views of how FCC jurisdiction should be exercised.

Expanded Exercise of FCC Jurisdiction

Most recently, at the FCC's Oct. 19 meeting, the FCC commissioners voted 3-2, along party lines, **to issue** a notice of proposed rulemaking that would reinstate the FCC's 2015-era net neutrality rules, reclassifying broadband internet access service, or BIAS, as a telecommunications service under Title II of the Communications Act.[1]

In the 2015 net neutrality proceeding, national security took a back seat to other consumer-focused policy priorities, with barely a mention in the FCC's Open Internet Order.[2] Now, however, Rosenworcel is highlighting reclassification of BIAS under Title II as a way for the FCC to take further action in the interest of safeguarding national security.

Just a few days after her proposal was publicly announced, the FCC released a fact sheet outlining all the ways that restoring Title II status would allow the FCC greater ability to protect national security as a key component of the agency's regulatory objectives.[3]

The FCC has also proposed expansions of other tools that, if adopted, would affect telecommunications providers, owners of FCC licensees, network and consumer equipment vendors and suppliers, service suppliers, and consumers.

For example, in April 2023, the commission launched a rulemaking to overhaul its licensing requirements and review process for providers that hold international Section 214 authorization, by requiring enhanced disclosures about licensees' foreign ownership and use of so-called untrusted equipment and foreign-owned managed network service providers, as well as making those licenses subject to periodic national security reviews.[4]

The FCC has also proposed expanding its equipment-authorization rules to apply to equipment components, and potentially enable revocation of current authorizations for national security reasons.[5]

Furthermore, the FCC is soliciting comments about a new voluntary cybersecurity labeling program that would allow manufacturers of smart devices connected to the Internet of Things to use a "U.S. Cyber Trust Mark" as a way to allow consumers to more easily compare device security, and ultimately make better informed purchase decisions.[6]

Filling Gaps

In the public comments submitted regarding the U.S. Cyber Trust Mark, some commenters noted that this sort of program seems to go beyond the FCC's traditional purview. The commission itself appears to recognize that in its efforts to lean forward on national security matters, there is potential for its actions to overlap, or even conflict, with the roles and responsibilities of other government agencies.

In the notice of proposed rulemaking issued in connection with the net neutrality proceeding, the FCC asked how "the Commission's role fit[s] with that of other agencies that help to address potential security threats from foreign actors to the nation's communications network and equipment, and how would enhancements to the Commission's regulatory authority as a result of reclassification bolster that role?"[7]

Indeed, there has been at least one recent instance of the FCC getting involved in a national security matter that could also have been addressed by the U.S. Department of Commerce.

In August, Chairman Mike Gallagher, R-Wisc., and Ranking Member Raja Krishnamoorthi, D.-Ill., of the U.S. House of Representatives Select Committee on the Chinese Communist Party wrote to Rosenworcel about concerns that Chinese-made cellular modules used in IoT devices could be used for infiltration, tracking and sabotage.[8]

In response, the FCC requested that other executive branch agencies, including the U.S. Department of Justice and U.S. Department of Defense, provide the commission with a determination of whether certain Chinese manufacturers of IoT modules should be added to the FCC's Covered List, which is a list of communications equipment and services determined to pose an unacceptable national security risk.

It is notable that the congressional letter went to the FCC rather than to Commerce, which was given new authorities more than four years ago to regulate the supply chain for information and communications technology and services, or ICTS, but thus far has yet to take a single regulatory action under that authority.

Specifically, initial regulations implementing Executive Order No. 13873 on securing the ICTS supply chain, issued in May 2019,[9] were promulgated by Commerce, which set forth a broad-sweeping and aggressive framework to identify, investigate, mitigate, block and unwind transactions between U.S.

persons and ICTS equipment and services from foreign adversary vendors.[10]

In addition, to implement a separate executive order,[11] Commerce recently adopted a final rule to expand its ICTS supply chain regulations to specifically include connected software applications as a covered technology, and to clarify the criteria that the secretary of commerce should use when determining whether transactions in connected software applications present undue or unacceptable risks.[12]

Notably, the rules cover not just single transactions but also classes of similar transactions, which enables an efficient and broad control when a vendor, product or service has been found to pose an unacceptable risk.

Under the ICTS supply chain regulations, ICTS is defined broadly to include "any hardware, software, including connected software applications, or other product or service, including cloud-computing services, primarily intended to fulfill or enable the function of information or data processing, storage, retrieval, or communication by electronic means (including electromagnetic, magnetic, and photonic), including through transmission, storage, or display."[13]

An ICTS transaction that could be subject to restriction by Commerce includes "any acquisition, importation, transfer, installation, dealing in, or use of any information and communications technology or service, including ongoing activities, such as managed services, data transmission, software updates, repairs, or the platforming or data hosting of applications for consumer download."[14]

If a product or service will be used in communications networks — whether they are wireless local area networks, mobile networks, satellites, cable or other wirelines, tertiary or core networks — the ICTS supply chain regulations would appear to cover that product or service — whether the underlying service offered to customers is considered a telecommunications service or an information service.[15]

The U.S. government has taken a liberal interpretation of words such as "integral" and "essential" in the context of restrictions on Chinese ICTS equipment, and presumably Commerce would deem IoT modules within the scope of its jurisdiction.

However, Commerce has been extremely slow to use this four-year-old authority. Although Commerce sought comment on creating a licensing framework to give parties more certainty about whether specific ICTS equipment and services would be regulated, no licensing rules have been proposed or adopted.

Commerce announced several years ago that it had launched a handful of investigations into Chinese suppliers, but to date those investigations have not resulted in any formal actions to limit, prohibit or unwind any ICTS transactions.

For this reason, the FCC may indeed be more responsive than Commerce would have been to the letter from Gallagher and Krishnamoorthi regarding IoT modules, and more willing to act.

This, combined with the FCC's other aggressive actions on national security-related matters, indicates that the commission is increasingly comfortable acting as a national security agency and not just as a regulatory agency.

It is also worth noting that if the net neutrality proceeding results in BIAS providers being subject to FCC

jurisdiction, that could create yet further overlap between the commission's jurisdiction and Commerce's ICTS supply chain jurisdiction. If Commerce continues to be inactive in this space, the FCC could very well move into the breach.

Continued Focus on National Security

The FCC can be expected to continue leaning in on national security issues, and leveraging its authorities as broadly as it can to be an active partner with the other government agencies with national security functions. If some of the commission's pending proceedings result in new rules, the effects on companies may be significant.

As one example, currently a relatively small number of FCC licenses are subject to national security review. Specifically, applications for several types of licenses that involve foreign ownership above a certain threshold typically get referred by the FCC to the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector, more commonly known as Team Telecom. Team Telecom then recommends whether the FCC should grant the license, condition the license on mitigation measures or deny the license.

In the FCC proceeding noted above that is examining licensing practices for international Section 214 authorizations, the FCC is contemplating an expansion of the types of licenses that get referred to Team Telecom, including licenses with no foreign ownership whatsoever; and is contemplating periodic reviews by Team Telecom of licenses previously approved.

The FCC also expanded the scope of potential Team Telecom reviews when it decided in a September order to refer — on a case-by-case basis — foreign-owned or foreign-controlled Voice over Internet Protocol providers seeking access to U.S. numbering resources to Team Telecom for national security review.[16]

In the separate net neutrality proceeding, it will be interesting to see whether, in subjecting BIAS providers to FCC jurisdiction, the FCC also seeks to subject any of them to Team Telecom review.

These changes would likely be significant for the industry, and among other things could increase the amount of time needed to close many deals involving telecommunications companies and assets, and subject providers to licensing and national security oversight where none had previously been required.

Both ICTS operators and investors should therefore keep a close eye on the FCC's increased appetite to be proactive in national security matters and be prepared for further regulatory and compliance burdens that may result.

David Plotinsky is a partner at Morgan Lewis & Bockius LLP. He previously served as acting chief of the DOJ's Foreign Investment Review Section.

Patricia Cave is an associate at the firm.

[1] Safeguarding and Securing the Open Internet, Notice of Proposed Rulemaking, WC Docket No. 23-320, FCC 23-83 (rel. Oct. 20, 2023), https://docs.fcc.gov/public/attachments/FCC-23-83A1.pdf.

[2] Protecting and Promoting the Open Internet, Report and Order on Remand, Declaratory Ruling, and Order, 30 FCC Rcd 5601 (2015), https://docs.fcc.gov/public/attachments/FCC-15-24A1.pdf.

[3] FCC, Fact Sheet: National Security and Public Safety Impacts of Restoring Broadband Oversight, https://docs.fcc.gov/public/attachments/DOC-397494A1.pdf.

[4] Review of International Section 214 Authorizations to Assess Evolving National Security, Law Enforcement, Foreign Policy, and Trade Policy Risks et al., Order and Notice of Proposed Rulemaking, IB Docket No. 23-119 et al., FCC 23-28 (rel. Apr. 25, 2023), https://docs.fcc.gov/public/attachments/FCC-23-28A1.pdf.

[5] Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program et al., Report and Order, Order, and Further Notice of Proposed Rulemaking, ET Docket No. 21-232 et al., FCC 22-84 (rel. Nov. 25, 2022), https://docs.fcc.gov/public/attachments/FCC-22-84A1.pdf.

[6] Cybersecurity Labeling for Internet of Things, Notice of Proposed Rulemaking, PS Docket No. 23-239, FCC 23-65 (rel. Aug. 10, 2023), https://docs.fcc.gov/public/attachments/FCC-23-65A1.pdf.

[7] Net Neutrality Notice of Proposed Rulemaking, ¶ 29.

[8] Letter from Mike Gallagher, Chair, and Raja Krishnamoorthi, Ranking Member, to The Honorable Jessica Rosenworcel, Chair, FCC (Aug. 7, 2023), https://selectcommitteeontheccp.house.gov/sites/evo-subsites/selectcommitteeontheccp.house.gov/files/evo-media-document/2023-08-07-cellular-iot-modules.pdf.

[9] Exec. Order No. 13873, 84 Fed. Reg. 22689 (May 15, 2019), https://www.federalregister.gov/documents/2019/05/17/2019-10538/securing-the-information-and-communications-technology-and-services-supply-chain.

[10] Securing the Information and Communications Technology and Services Supply Chain, Interim Final Rule, Request for Comments, 86 Fed. Reg. 4909 (2021), https://www.federalregister.gov/documents/2021/01/19/2021-01234/securing-the-information-and-communications-technology-and-services-supply-chain (codified at 15 C.F.R. pt. 7).

[11] Exec. Order No. 14034, 86 Fed. Reg. 31423 (Jun 9, 2021), https://www.federalregister.gov/documents/2021/06/11/2021-12506/protecting-americans-sensitive-data-from-foreign-adversaries.

[12] Securing the Information and Communications Technology and Services Supply Chain, Final Rule, 88 Fed. Reg. 39353 (2023), https://www.federalregister.gov/documents/2023/06/16/2023-12925/securing-the-information-and-communications-technology-and-services-supply-chain-connected-software.

[13] 15 C.F.R. § 7.2.

[14] Id.

[15] See 15 C.F.R. § 7.3(a)(4)(ii).

[16] Numbering Policies for Modern Communications et al., Second Report and Order and Second Further Notice of Proposed Rulemaking, WC Docket No. 13-97 et al., FCC 23-75, ¶ 26 (rel. Sep. 22, 2023), https://docs.fcc.gov/public/attachments/FCC-23-75A1.pdf.