Insight

FCC May Be Overstepping on Cybersecurity

JEFFREY WESTLING | FEBRUARY 4, 2025

Executive Summary

- Over the past two years, a hacking group linked to Chinese intelligence known as Salt Typhoon accessed U.S. telephone networks and systems used for court-appointed surveillance, collecting significant data on American users and government surveillance information.
- In an attempt to prevent future attacks, the Federal Communications Commission (FCC) broadly interpreted its authority over telephone networks and some broadband internet service providers to include the regulation of cybersecurity practices, and could extend these regulations to other forms of communication such as broadcast television or satellite broadband.
- While defending American networks from Chinese cyberattacks is a key federal priority, drastically expanding the FCC's authority without congressional approval could hinder any whole-of-government approach to secure American networks and unintentionally make those networks less secure by deterring collaboration between industry and federal regulators.

Introduction

Late last year, it was revealed that at least nine American telecommunications networks had been breached by a hacking group linked to Chinese intelligence known as Salt Typhoon. According to reports, the breach largely focused on "high-value targets," collecting call-log data and unencrypted texts and call audio. Even more worrisome, the hackers also accessed wiretap-surveillance systems, which telephone companies must employ under the Communications Assistance for Law Enforcement Act (CALEA). While the immediate threat has been largely contained, many security experts warn that the extent of the breach is not

fully known and could be exploited again in time-sensitive attacks.

In an attempt to address these concerns, the Biden Federal Communications Commission (FCC) issued a declaratory ruling and notice of proposed rulemaking (NPRM) days before the transition to the Trump Administration, under Republican objection. The declaratory ruling, which is an agency interpretation of existing law and not a binding rule under the Administrative Procedure Act, stated that section 105 of CALEA affirmatively requires telephone companies (and some similar technologies) to secure their networks from unlawful access to or interception of communications. Further, the FCC proposed a series of formal rules that would require a wide range of communications providers, most of which are outside the scope of CALEA, to develop "reasonable" cybersecurity risk management plans and provide them to the FCC upon request.

Undoubtedly securing American networks against cybersecurity vulnerabilities is a national priority, but the FCC proposal has drawn significant scrutiny from both members of Congress and members of the FCC. Among other concerns, the FCC claims to have authority over telephone companies' and ISPs' cybersecurity practices, which goes beyond previous orders relying on CALEA largely focused on equipment that could provide access to telephone networks, particularly the switching premises. This is especially troubling considering current FCC rules already require CALEA-regulated providers to submit their security policies and procedures to the FCC for review, and the agency signed off on these policies before the hack. If the agency already has the authority it claims, that doesn't speak well of its use of this authority if it approved procedures insufficient to prevent hacks.

What's more, the NPRM would go beyond the companies covered by CALEA and include additional means of communications, including broadcast television stations to satellite broadband. Another concern is that, by independently issuing these rules and requirements on telephone companies and ISPs, the FCC runs the risk of alienating both industry and the intelligence community, and may make potential partnerships to address these vulnerabilities more difficult moving forward. While fruitful FCC action can be taken, the agency should do so with clear guidance from Congress and in collaboration with the intelligence community.

Salt Typhoon and Chinese Hacks Into American Infrastructure

In recent years, the Chinese government has conducted widespread cyberattacks on U.S. infrastructure in a variety of sectors. These attacks targeted arenas that are usually under-protected but critical to the country, such as a water utility in Hawaii and a port in Houston. Most alarming, reports indicate Chinese hackers had gained the ability to shut down dozens of U.S. ports, power grids, and other infrastructure targets at will.

The Salt Typhoon hacks are the latest Chinese hacking efforts (at least of those that are publicly known), and largely targeted telecommunications networks. According to reports, nine firms have been affected and the attackers collected information on so-called "high value targets." The hackers accessed data from over a million users and collected audio from government officials, including some calls with President Trump according to *The Wall Street Journal*, using known software flaws that had yet to be patched. While the companies have largely contained the attacks, there is still uncertainty about the depth of these attacks and what vulnerabilities still exist in the networks.

The Biden FCC's Response

The attacks on American infrastructure may justify government action to establish specific rules and regulations to prevent unauthorized access to consumer data. The FCC's action here is twofold. First, the FCC issued a declaratory ruling that concludes section 105 of CALEA affirmatively requires telephone companies and some ISPs to secure their networks from unlawful access to or interception of communications. CALEA, more broadly, requires telephone companies to provide sensitive consumer information to law enforcement after a court order. Section 105 requires that these companies implement measures to make sure wiretaps and other surveillance only occur through proper procedures and access to the public switches is not accessible to unauthorized individuals. Previous interpretations have extended the requirements to some ISPs, particularly those offering services such as voice-over-internet-protocol that function similarly to traditional telephone networks.

Second, the FCC issued an NPRM seeking comment on rules that would require telecommunications carriers to develop cybersecurity plans and deliver them to the FCC upon request. Of note, the NPRM would extend the provisions of section 105 to a wide range of services that have nothing to do with publicly switched telephone networks, the original subject of CALEA. These include facilities-based fixed and mobile broadband providers, broadcasting stations, cable companies, and satellite communications providers. All covered companies would then need to develop cybersecurity plans that the FCC finds reasonable.

Concerns With the FCC's Actions

While the Salt Typhoon hacks demonstrate the imperative of securing of our nation's infrastructure, the FCC's action likely goes beyond the authority granted to it by Congress and could jeopardize future collaborative efforts between industry and the intelligence community.

First, with regard to agency authority, CALEA is largely focused on publicly switched

telecommunications networks and the so-called “backdoors” telephone companies are required to provide to law enforcement. The provisions in section 105 were specifically designed in this context: If a telephone company is required to implement a tool to collect information on its users, it must ensure that that tool is secure and can only be used for lawful purposes. Traditionally, this required limiting the number of individuals who have access to that system or ensuring their equipment won’t provide a backdoor to malicious actors. The declaratory ruling goes beyond these bounds and instead states that CALEA gives the FCC broad authority to manage the cybersecurity practices of telecommunications writ large, and not just the systems or the switching premises covered in CALEA.

Further, a declaratory ruling is just an interpretation of existing law, and currently the FCC requires CALEA-regulated providers to submit CALEA-related policy and procedures to the agency. If the FCC already has this authority and signed off on these companies’ plans – but the hacks still occurred – the procedures were apparently insufficient, or the FCC failed in its duty by allowing the hacks to continue. Further, if FCC’s new interpretation were the current law, and the agency signed off on companies’ policies without previously diving deeply into their cybersecurity practices, it seems unlikely that any court would find the agency had such authority after the overturning of *Chevron* doctrine and the expansion of the major questions doctrine.

Second, although the expansion of agency authority is problematic, the FCC’s actions could also be counterproductive to the goal of securing American networks. Designing an appropriate response will take collaboration between private industry and the intelligence community. Imposing broad cybersecurity requirements on communications companies adds risk and uncertainty to their businesses, especially when these companies aren’t a part of the process in developing the requirements. As a result, these companies could act defensively, fail to work with intelligence officials, and ultimately act primarily to avoid liability rather than best protect their consumers.

These concerns are more significant due to the last-minute, partisan nature of the vote immediately prior to the transition to the Trump Administration. And while Biden Administration National Security Adviser endorsed action, FCC Chairman Brendan Carr has indicated that members of the intelligence community have argued against the proposal, calling it counterproductive. Ultimately, any action taken likely should stem from direct congressional authority and incorporate feedback and representation from both industry and the intelligence community.

Conclusion

After the Salt Typhoon hacks, the security of telecommunications networks should receive

heightened focus from both industry and the Trump Administration. But it is also critical that agencies remain bound by the authority granted to them by Congress, and that any actions taken ultimately produce the desired outcomes. It is unclear whether the FCC's declaratory ruling and NPRM meet the standard on either count.