



TECHNOLOGY
POLICY
INSTITUTE

The FCC Got the Router Ban Wrong. It Knew Better.

Scott Wallsten

March 2026

The FCC Got the Router Ban Wrong. It Knew Better.

Scott Wallsten*
March 27, 2026

On March 23, the FCC effectively banned all new foreign-made routers from the U.S. commercial market by adding them to its so-called “covered list.”¹ The action followed a White House-convened interagency National Security Determination issued just three days earlier.² The Commission took this action with no notice-and-comment proceeding, no published cost-benefit analysis, and without providing a broad transition process for the affected industry. The only path forward for manufacturers is to apply for “Conditional Approval” from the Department of Defense or the Department of Homeland Security.³

The security concerns are real. Chinese state-sponsored hacking groups, including Volt Typhoon, Salt Typhoon, and Flax Typhoon, have exploited vulnerabilities in consumer routers to penetrate American networks, conduct surveillance, and build botnets for attacks on critical infrastructure.⁴ Router security deserves serious attention.

But in the past, the FCC addressed threats like these in a way that was more targeted, more precisely designed, and better built to survive legal challenge. Comparing the FCC's handling of the Huawei and ZTE threat in 2019-2022 to the new router ban reveals what happens when an agency abandons the deliberative process that makes its expertise useful.

How the FCC used to handle supply chain threats

To respond to national security risks posed by Huawei and ZTE, the FCC followed a deliberative process and produced a carefully constructed regulatory framework.

* President and Senior Fellow, Technology Policy Institute. These comments reflect my views alone, and not necessarily those of the TPI's boards, staff, or donors.

¹ Federal Communications Commission, “FCC Updates Covered List to Include Foreign-Made Consumer Routers, Prohibiting Approval of New Models,” Federal Communications Commission, March 23, 2026, <https://www.fcc.gov/document/fcc-updates-covered-list-include-foreign-made-consumer-routers>.

² Federal Communications Commission, “FCC Public Notice DA 26-278,” Federal Communications Commission, March 23, 2026, <https://docs.fcc.gov/public/attachments/DA-26-278A1.pdf>.

³ Federal Communications Commission, “FAQs on Recent Updates to FCC Covered List Regarding Routers Produced in Foreign Countries,” Federal Communications Commission, March 23, 2026, <https://www.fcc.gov/faqs-recent-updates-fcc-covered-list-regarding-routers-produced-foreign-countries>.

⁴ Federal Communications Commission, “Fact Sheet: FCC Updates Covered List to Include Foreign-Made Consumer Routers,” Federal Communications Commission, March 23, 2026, <https://docs.fcc.gov/public/attachments/DOC-420034A1.pdf>.

Congress identified the specific companies as threats in Section 889 of the FY2019 National Defense Authorization Act. The FCC designated Huawei and ZTE as national security threats in June 2020, published its initial Covered List in March 2021, and adopted a Notice of Proposed Rulemaking and Notice of Inquiry on June 17, 2021, initiating two separate dockets and inviting public comment.⁵ The Commission then adopted a Report and Order in November 2022, with a unanimous 4-0 vote, and simultaneously issued a Further Notice of Proposed Rulemaking seeking additional comment on issues it hadn't yet resolved.⁶

That process took time. But it also produced outcomes that it could never have achieved in a weekend.

The comment process produced differentiated treatment based on actual risk. The FCC did not treat all five Chinese companies identically. It fully banned new Huawei and ZTE equipment, but took a more nuanced approach with Hikvision, Dahua, and Hytera. The FCC agreed with commenters who argued that these companies posed different levels and kinds of risk. The FCC required those three companies to document the safeguards they would put in place, and froze their applications pending that review.⁷ The router ban, by contrast, treats a Netgear router assembled in Vietnam identically to a TP-Link router designed in China.

The comment process identified a clear scope. The FCC had to define what counted as “covered” equipment. For example, it established that handset equipment designed for broadband operation with connection speeds of at least 200 kbps fell within the scope of “telecommunications equipment,” while equipment below that threshold did not.⁸ That line was not in the original proposal. It emerged from the comment process, as affected companies argued that basic radio equipment should not be treated the same as broadband-capable devices. The FCC drew a principled boundary. The router ban draws no such lines. Its definition of “produced in a foreign country” encompasses “any major stage of the process through which the device is

⁵ Federal Communications Commission, “Protecting Against National Security Threats to the Communications Supply Chain Through the Equipment Authorization Program,” Federal Register, February 6, 2023, <https://www.federalregister.gov/documents/2023/02/06/2022-28263/protecting-against-national-security-threats-to-the-communications-supply-chain-through-the>.

⁶ Nextgov, “FCC Bans Sale of New Devices From Chinese Companies Huawei, ZTE and Others,” Nextgov/FCW, November 28, 2022, <https://www.nextgov.com/emerging-tech/2022/11/fcc-bans-sale-new-devices-chinese-companies-huawei-zte-and-others/380214/>.

⁷ Nextgov, “FCC Bans Sale of New Devices From Chinese Companies Huawei, ZTE and Others.” (“For these three companies, we will require them to document what safeguards they will put in place on marketing or sale for these purposes, and we are putting in place a freeze on all of their telecommunications and video surveillance equipment authorization applications until that work is done.”)

⁸ Urgent Communications, “FCC Bans Authorization of New ‘covered’ Products from Five Chinese Vendors,” Urgent Communications, October 29, 2024, <https://urgentcomm.com/policy/fcc-bans-authorization-of-new-covered-products-from-five-chinese-vendors>.

made, including manufacturing, assembly, design, and development,” potentially sweeping in routers designed by American companies and assembled overseas.⁹

The Huawei/ZTE response included transition assistance. The FCC’s decision imposed real costs on carriers. Rural carriers told the FCC they couldn’t afford to remove Huawei and ZTE equipment without financial help. Congress responded by creating the Secure and Trusted Communications Networks Reimbursement Program, initially funded at \$1.9 billion, which funded the removal and replacement of insecure equipment from carrier networks.¹⁰ The program has problems, such as a lack of evaluation and careful tracking of funds. But if the cost imposed on a company is due to a government mandate, the government should at least consider how to pay for it.

The comment process produced legal durability. During the rulemaking, commenters raised constitutional challenges, including arguments that the rules were an unconstitutional bill of attainder, violated the Equal Protection Clause, and amounted to an unconstitutional taking of property.¹¹ The FCC addressed each of these arguments in its order, building a legal record. When Huawei challenged the related NDAA restrictions in court, a federal district court found the restrictions lawful because the government had demonstrated they reasonably furthered non-punitive national security goals.¹² The router ban has no comparable record, and former FCC officials have already predicted it will face legal challenge.¹³

The process was iterative. The FCC recognized that its initial rules were a first step and continued refining them. A Second Report and Order clarified that covered equipment includes modular transmitters, proposed a definition of “critical infrastructure,” and sought further comment on the scope of marketing prohibitions.¹⁴ The agency learned from industry input how supply chains actually work and adjusted its rules accordingly.

None of this happened with the router ban. The White House convened a panel. The panel issued a determination. Three days later the FCC implemented it.

⁹ Federal Communications Commission, “FAQs on Recent Updates to FCC Covered List Regarding Routers Produced in Foreign Countries.”

¹⁰ Federal Communications Commission, “Secure and Trusted Communications Networks Reimbursement Program,” Federal Communications Commission, 2026, <https://www.fcc.gov/supplychain>.

¹¹ Congressional Research Service, “New FCC Rules Ban Authorizations for Equipment Posing National Security Risks,” [Congress.gov](https://www.congress.gov/crs-product/LSB10895), 2023, <https://www.congress.gov/crs-product/LSB10895>.

¹² Congressional Research Service, “New FCC Rules Ban Authorizations for Equipment Posing National Security Risks.”

¹³ Derek B. Johnson, “Critics Call FCC Router Rule a ‘big Swing’ That Could Create More Supply Chain Uncertainty,” [CyberScoop](https://cyberscoop.com/fcc-bans-foreign-routers-critics-warn-about-supply-chain/), March 24, 2026, <https://cyberscoop.com/fcc-bans-foreign-routers-critics-warn-about-supply-chain/>.

¹⁴ Federal Communications Commission, “Second Report and Order and Second Further Notice of Proposed Rulemaking, Fact Sheet,” Federal Communications Commission, October 7, 2025, <https://docs.fcc.gov/public/attachments/DOC-415051A1.pdf>.

To be fair, the Secure Networks Act may leave the FCC little discretion over whether to add items to the Covered List once the White House makes a qualifying determination. But the FCC still retains substantial leeway over how to implement the resulting equipment authorization restrictions, including its scope, transition periods, and what guidance it issues for affected parties. In the Huawei/ZTE proceeding, the Covered List addition itself was relatively quick, but the FCC spent more than a year designing the implementing rules through a public process. Nothing in the Secure Networks Act prevented the FCC from doing the same here. It chose not to.

What the absence of process produced

The router ban bears all the hallmarks of a policy that never faced serious analytical scrutiny.

The stated justification is cybersecurity risk from foreign manufacturing.¹⁵ But the evidence the FCC itself cited undercuts the case for a country-of-manufacture approach. According to the Department of Justice, Volt Typhoon primarily targeted Cisco and Netgear routers, devices designed by American companies.¹⁶ The routers were vulnerable not because of where they were manufactured but because those companies had stopped providing security updates for discontinued models. The FBI's own guidance urged router owners to replace end-of-life devices, and CISA's mitigation advice to manufacturers focused on secure design and automated updates, not supply chain origin.¹⁷ Salt Typhoon compromised major U.S. telecommunications carriers through network equipment made by Cisco, though Cisco's own security researchers reported that most intrusions it reviewed involved stolen credentials rather than software vulnerabilities.¹⁸ The national security determination includes supporting evidence from NIST,

¹⁵ Ironically, given the security justification for the ban, the Covered List restrictions do not apply to federal government procurement. This exemption is hard to explain if these devices truly pose unacceptable security risks. But it also demonstrates that the government apparently believes security risk from foreign routers can be managed through its own procurement review processes rather than a blanket ban. That option could have been available for consumers, too.

Federal Communications Commission, "FAQs on Recent Updates to FCC Covered List Regarding Routers Produced in Foreign Countries." ("The Covered List does not restrict the import or sale of routers for the exclusive use by the federal government.").

¹⁶ U.S. Department of Justice, "U.S. Government Disrupts Botnet People's Republic of China Used to Conceal Hacking of Critical Infrastructure," U.S. Department of Justice, January 31, 2024, <https://www.justice.gov/opa/pr/us-government-disrupts-botnet-peoples-republic-china-used-conceal-hacking-critical>.

¹⁷ U.S. Department of Justice, "U.S. Government Disrupts Botnet People's Republic of China Used to Conceal Hacking of Critical Infrastructure"; CISA et al., *PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure* (Cybersecurity and Infrastructure Security Agency, 2024), <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a>.

¹⁸ Cisco Talos Intelligence Group, "Weathering the Storm: In the Midst of a Typhoon," Cisco Talos, February 20, 2025, <https://blog.talosintelligence.com/salt-typhoon-analysis/>.

CISA, the FBI, and other agencies on router vulnerabilities generally. But none of it persuasively establishes that country of production, standing alone, is a useful proxy for cybersecurity risk.¹⁹

An agency exercising careful judgment would have noticed this disconnect. If the problem is that manufacturers abandon security updates for older devices, the solution might be to mandate some kind of software maintenance or to require vulnerability disclosures, not a blanket import ban organized around the country of manufacture. The FCC has an interdisciplinary expert staff who could have evaluated whether country of origin is actually a useful proxy for cybersecurity risk. Given the speedy timeline, it seems unlikely that they were consulted in a meaningful way.

In principle, country of manufacture could matter in hardware supply chains if a state actor could theoretically compromise hardware during production. This concern is real and deserves a serious policy response. But a blanket ban covering routers from every country on earth is not that response. A targeted action against manufacturers with documented ties to adversarial intelligence services, combined with supply chain integrity requirements for all manufacturers seeking FCC authorization, would address the hardware concern far more precisely. That is roughly what the FCC did with Huawei and ZTE. But the current ban treats a router from Finland the same as one from China.

Making the matter worse is that virtually no consumer-grade routers are manufactured in the United States. The only widely cited exception is some Starlink Wi-Fi routers that SpaceX says are made in Texas.²⁰ Even major American brands including Netgear, Eero, and Google manufacture their products overseas.²¹

The conditional approval process, the supposed escape valve, requires companies to disclose their management structure, detail their supply chain, and present a plan for onshoring manufacturing to the United States.²² That is not a security audit. It is industrial policy masquerading as a national security framework. No comment period helped shape it. And while Annex A to the determination publishes extensive submission requirements, there appears to be no public review timeline or clear decision standard.

¹⁹ Executive Branch Interagency Body, *National Security Determination on the Threat Posed by Routers Produced by Foreign Countries* (Federal Communications Commission, 2026), <https://www.fcc.gov/supplychain/coveredlist>.

²⁰ Joe Lancaster, “FCC Bans Nearly All Wireless Routers Sold in the U.S.,” Reason, March 25, 2026, <https://reason.com/2026/03/25/fcc-bans-nearly-all-wireless-routers-sold-in-the-u-s/>.

²¹ iDrop News, “Is Your Router Banned? The 2026 FCC Ruling Explained,” iDrop News, March 24, 2026, <https://www.idropnews.com/news/fcc-router-security-risk-2026/261467/>.

²² Mayer Brown, “FCC Expands Its Covered List to Include Foreign-Produced Routers,” Mayer Brown, March 2026, <https://www.mayerbrown.com/en/insights/publications/2026/03/fcc-expands-its-covered-list-to-include-foreign-produced-routers>. (analyzing Annex A guidance). The guidance requires “a detailed, time-bound US manufacturing and onshoring plan, on which updates must be provided quarterly.” Conditional Approvals last up to 18 months.

Meanwhile, the ban creates the very vulnerability it claims to address. Firmware and software updates for existing covered devices are permitted through at least March 2027, thanks to a blanket waiver from the FCC's Office of Engineering and Technology.²³ But that waiver expires. A router that cannot receive security updates becomes exactly the kind of unpatched, vulnerable device that Volt Typhoon and Salt Typhoon exploited.

Some may argue that the post-Salt Typhoon threat environment necessitates faster action than the multi-year Huawei process allowed. But if that is true, it becomes hard to justify an action that does nothing about the millions of foreign-made routers already deployed in American homes and businesses, which are the actual devices that Volt Typhoon and Salt Typhoon exploited. If the threat were urgent enough to justify bypassing all deliberation, one would expect the FCC to be taking emergency action on the installed base. It is not. The ban addresses only future models, making this a forward-looking regulatory action for which a deliberative process was both feasible and appropriate.

A serious response would combine targeted restrictions on specific manufacturers with supply chain integrity and software maintenance requirements for all manufacturers seeking FCC authorization. The FCC has the expertise to design such a framework. It did exactly that with Huawei and ZTE.

The lesson

In December 2025 testimony before the Senate Commerce Committee, Chairman Carr told lawmakers that the FCC “is not an independent agency, formally speaking.”²⁴ The router ban is a case study in what happens when that posture translates into skipping the processes that make regulation work. The comparison between the Huawei/ZTE process and the router ban is not just a story about two different policy decisions. It is a controlled experiment in what deliberative process is worth.

Same agency. Same statutory framework. Same category of threat. But the 2019-2022 process, in which the FCC used its full deliberative toolkit, produced targeted bans, differentiated treatment based on risk, precise scoping informed by industry expertise, billions in transition funding, and a legal record durable enough to survive court challenge. The 2026 process, in which the Commission used none of those tools, produced a blanket ban on an entire product category, no

²³ Wiley Rein LLP, “FCC Adds Foreign-Produced Consumer-Grade Routers to Covered List,” Wiley, March 2026, <https://www.wiley.law/alert-FCC-Adds-Foreign-Produced-Consumer-Grade-Routers-to-Covered-List>.

²⁴ Axios, “FCC Chair Suggests Agency Isn’t Independent, Word Cut from Mission Statement,” Axios, December 17, 2025, <https://www.axios.com/2025/12/17/brendan-carr-fcc-independent-senate-testimony-website>; The Wrap, “FCC Updates Website in Real-Time to Reflect Brendan Carr’s Testimony That the Agency Is Not Independent,” The Wrap, December 17, 2025, <https://www.thewrap.com/fcc-brendan-carr-website-not-independent/>.

differentiation, no scoping analysis, no transition assistance, and a legal record so thin that former FCC officials are already predicting litigation.

The Secure Networks Act is the mechanism that enables this arrangement. Under the statute, the FCC says it cannot update the Covered List on its own but rather must implement determinations made by national security agencies.²⁵ When those determinations were narrow and entity-specific, this was a manageable arrangement, and the FCC still exercised its own judgment in designing the implementing rules. Now that the determinations have expanded to cover entire product categories, and the FCC has chosen not to exercise its implementation authority, the agency is implementing sweeping trade and technology policy without the deliberation such decisions require.

The same pattern produced the December 2025 ban on foreign-made drones, which is already being challenged in court.²⁶ In that case, Section 1709 of the FY2025 NDAA gave national security agencies one year to complete an evidence-based review of DJI drones, with an automatic Covered List addition as a fallback. Instead of a targeted review of DJI, the executive branch issued a broad national security determination covering all foreign-made drones, which the FCC implemented immediately. DJI has since sued to challenge the action.²⁷

Process is not just a bureaucratic waste of time. It is the mechanism through which an agency's expertise improves the quality of its decisions. The FCC demonstrated this in 2022 when it banned Huawei and ZTE equipment through a deliberative process that produced a more targeted, more durable, and more precisely designed result. Whatever the reasons the Commission did not follow the same approach here, the outcome speaks for itself.

Congress should pay attention. The Secure Networks Act created a mechanism that, when combined with sweeping executive branch determinations and an FCC willing to implement them without deliberation, allows the President to ban entire categories of consumer technology without notice, without comment, without cost-benefit analysis, and without any of the procedural safeguards that normally govern consequential regulatory action. If Congress intended the Covered List to be used this way, it should say so. If it didn't, it should act before the next product category lands on the list.

²⁵ Federal Communications Commission, "FAQs on Recent Updates to FCC Covered List Regarding Routers Produced in Foreign Countries."

²⁶ DroneXL, "FCC Bans Foreign Routers Citing Security Risks - The Same Playbook Used to Ground DJI," DroneXL, March 23, 2026, <https://dronexl.co/2026/03/23/fcc-bans-foreign-routers-citing-security-risks-dji/>.

²⁷ DroneDJ, "DJI Sues FCC: Drone Giant Fights 'unconstitutional' US Market Ban," DroneDJ, February 24, 2026, <https://dronedj.com/2026/02/24/dji-us-ban-lawsuit-fcc/>.