

BRETT GUTHRIE, KENTUCKY
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED NINETEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON ENERGY AND COMMERCE

2125 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6115

Majority (202) 225-3641

Minority (202) 225-2927

July 20, 2026

MEMORANDUM

To: Subcommittee on Communications and Technology Members and Staff
From: Committee Majority Staff
Re: Subcommittee on Communications and Technology Hearing on July 22, 2026

I. INTRODUCTION

The Subcommittee on Communications and Technology will hold a legislative hearing on Wednesday, July 22, 2026, at 2:00 PM ET in 2123 Rayburn House Office Building. The hearing is entitled, “Legislative Hearing on Protecting Communications Networks and Improving Connectivity.” The hearing will review the following legislation:

- H.R. 9129, GUARD Act (Reps. Moolenaar and McClellan)
- H.R. 6152, Foreign Robocall Elimination Act (Reps. McDowell and Morrison)
- H.R. 1027, QUIET Act (Reps. Sorensen and Ciscomani)
- H.R. 7294, AI for Secure Networks Act (Reps. Menendez and Pfluger)
- H.R. 2805, PLAN for Broadband Act (Reps. Walberg and Peters)
- H.R. 4950, Data BRIDGE Act (Reps. Houchin and Kelly (IL))

II. WITNESSES

- Michael Robbins, President & CEO, Association for Uncrewed Vehicle Systems International (AUVSI)
- Kevin Rupy, Partner, Wiley Rein LLP
- Andrew Von Ah, Director, Physical Infrastructure, Government Accountability Office (GAO)
- Lindsay Gorman, Former Senior Policy Advisor for Technology Strategy, Biden White House

III. BACKGROUND

A. National Security and Competition with the People's Republic of China

The leadership of the Chinese Communist Party (CCP) has taken aggressive steps to position the People's Republic of China (PRC) as a global economic power and a dominate force in multiple industries, including by strategically increasing U.S. dependence on the PRC for critical supply chains.¹ In the case of communications infrastructure, CCP-backed companies have developed unsecure telecommunications equipment and exported it around the world in order to assist in its espionage activities.² The PRC's 2017 National Intelligence Law requires "individuals, organizations, and institutions to assist the PRC security and intelligence services in carrying out a wide variety of intelligence work."³ Further, the opaque ownership structures of Chinese companies raise more questions related to how much influence the Chinese government asserts over them, leading to uncertainty about the national security threats posed by Chinese technology.⁴

On March 12, 2020, President Donald J. Trump signed the Secure and Trusted Communications Networks Act (STCNA) of 2019 into law.⁵ The law prohibits a Universal Service Fund (USF) recipient from purchasing, obtaining, or maintaining any equipment or services from companies posing a national security threat, and requires the Federal Communications Commission (FCC) to publish a list of "covered communications equipment or services" that pose such a threat, which includes CCP-affiliated companies such as Huawei and ZTE.⁶ Since the enactment of STCNA, Congress has passed additional legislation signed by President Biden requiring that the drone industry be analyzed for national security vulnerabilities and potential inclusion of related entities on the covered list, specifically including Shenzhen Da-Jiang Innovations Sciences and Technologies Company Limited (known as DJI) and Autel Robotics.⁷ Following determination by the National Security Council and the U.S. intelligence community of unacceptable risk to U.S. national security, the FCC added all foreign-

¹ UNCLASSIFIED 2026 ANNUAL THREAT ASSESSMENT OF THE U.S. INTELLIGENCE COMMUNITY, OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE (Mar. 2026), <https://www.dni.gov/files/ODNI/documents/assessments/ATA-2026-Unclassified-Report.pdf>.

² A Report by Chairman Mike Rogers and Ranking Member C.A. Dutch Ruppersberger of the Permanent Select Committee on Intelligence, Permanent Select Committee on Intelligence, U.S. House of Representatives 112th (Oct. 8, 2012), [https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20report%20\(final\).pdf](https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20report%20(final).pdf).

³ National Security Council, *Statement from National Security Advisor Robert C. O'Brien* (Jan. 15, 2021), <https://trumpwhitehouse.archives.gov/briefings-statements/statement-national-security-advisor-robert-c-obrien-011521-2/>.

⁴ Raymond Zhong, *Who Owns Huawei? The Company Tried to Explain. It Got Complicated.*, N.Y. Times (Apr. 25, 2019), <https://www.nytimes.com/2019/04/25/technology/who-owns-huawei.html>.

⁵ *Secure and Trusted Communications Networks Act of 2019*, Pub. L. No. 116-124 (2020).

⁶ *List of Equipment and Services Covered by Section 2 of The Secure Networks Act*, The Fed. Communications Comm'n, <https://www.fcc.gov/supplychain/coveredlist> (last visited July 15, 2026).

⁷ *Servicemember Quality of Life Improvement and National Defense Authorization Act for Fiscal Year 2025*, Pub. L. No. 118-159, §1709 (2024).

manufactured Uncrewed Aircraft Systems (UAS) and UAS critical components, as well as all foreign-manufactured routers, to the covered list.⁸

B. Illegal Robocalls

Illegal robocalls continue to be a scourge on Americans. According to the FCC, illegal and spoofed robocalls are its biggest consumer complaint and its top consumer protection priority.⁹ A robocall is “any telephone call that delivers a pre-recorded message using an automatic (computerized) telephone dialing system” or “autodialer.”¹⁰ Robocalls can be legal and are used routinely for legitimate purposes, such as public service and emergency messages, to provide notice of school closures, and to remind consumers of medical appointments and upcoming payments. A large proportion of robocalls, however, are illegal and intended to scam, harass, or otherwise annoy consumers.¹¹ Consumers have lost millions of dollars to these schemes after being deceived into providing financial and other sensitive information or purchasing falsely advertised products.¹² According to one consumer watchdog, scam robocalls and robotexts cost U.S. consumers \$25 billion in 2023.¹³

The Telephone Consumer Protection Act of 1991 (TCPA) restricts telemarketing calls and regulates robocalls made through an automatic telephone dialing system or an artificial or prerecorded voice message. Since its passage, the FCC adopted rules to implement the TCPA, such as maintaining company-specific do-not-call lists, curtailing call times for telemarketers, and requiring the display of caller ID information. The FCC also required that telemarketers obtain prior express written consent from consumers before robocalling them and that telemarketers provide consumers with an automated, interactive “opt-out” mechanism during each robocall. In 2003, the FCC, in coordination with the Federal Trade Commission (FTC), established a national Do Not Call registry, which covers all telemarketers (with the exception of

⁸ *Public Safety and Homeland Security Bureau Announces Addition of Uncrewed Aircraft Systems (UAS) and UAS Critical Components Produced Abroad, and Equipment and Services Listed in Section 1709 of the FY2025 NDAA, To FCC Covered List*, Public Notice, DA 25-1086 (Fed. Communications Comm’n Dec. 22, 2025), <https://docs.fcc.gov/public/attachments/DA-25-1086A1.pdf>; *Public Safety and Homeland Security Bureau Announces Addition of Routers Produced in Foreign Countries to FCC Covered List*, Public Notice, DA 26-278 (Fed. Communications Comm’n Mar. 23, 2026), <https://docs.fcc.gov/public/attachments/DA-26-278A1.pdf>.

⁹ *Consumer Guides: Stop Unwanted Robocalls and Texts*, Fed. Communications Comm’n, <https://www.fcc.gov/consumers/guides/stop-unwanted-robocalls-and-texts> (last visited July 15, 2026).

¹⁰ PATRICIA MOLONEY FIGLIOLA, CONG. RESEARCH SERV., R46311, FEDERAL COMMUNICATIONS COMMISSION: PROGRESS PROTECTING CONSUMERS FROM ILLEGAL ROBOCALLS (2020).

¹¹ See generally Howard Packowitz, *Parents Told Livingston County High School is Safe after Robocall Threat*, 25 NEWS NOW (Mar. 14, 2025), <https://www.25newsnow.com/2025/03/15/parents-told-livingston-county-high-school-is-safe-after-robocall-threat/>; DO Staff, *DOs Receive Unwanted Robocalls from Company Urging Them to Consider an MD Degree*, THE DO (Dec. 4, 2024), <https://thedo.osteopathic.org/2024/12/dos-receive-unwanted-robocalls-from-company-urging-them-to-consider-an-md-degree/>; Nick Perry, *Company that Sent AI calls Mimicking Joe Biden to New Hampshire Voters Agrees to Pay \$1 Million Fine*, AP NEWS (Aug. 22, 2024), <https://apnews.com/article/joe-biden-artificial-intelligence-deceptive-phone-calls-33bab2049c12f952eb683a83039ddbba>.

¹² GOV’T ACCOUNTABILITY OFFICE, GAO-20-153, *FAKE CALLER ID SCHEMES: INFORMATION ON FEDERAL AGENCIES’ EFFORTS TO ENFORCE LAWS, EDUCATE THE PUBLIC, AND SUPPORT TECHNICAL INITIATIVES* (2019), <https://www.gao.gov/assets/gao-20-153.pdf>.

¹³ TRUECALLER, *AMERICA UNDER ATTACK: THE SHIFTING LANDSCAPE OF SPAM AND SCAM CALLS IN AMERICA* (2024), <https://pirg.org/edfund/resources/ringing-in-our-fears-2024/>.

certain nonprofit organizations), and applies to both interstate and intrastate calls. These efforts help stop unwanted live and robocall sales calls from legitimate businesses, but do not block calls from scammers who fail to abide by the law.

The TCPA provides a variety of enforcement mechanisms, including private rights of action for individuals. In addition, the FCC, FTC, and the Department of Justice (DOJ) take enforcement actions against violators, such as the imposition of fines and other legal penalties. However, the private rights of action under the TCPA have led to a proliferation of litigation, including class-action lawsuits, often targeting legitimate businesses over minor or technical violations instead of penalizing bad actors responsible for placing illegal robocalls. This has created a rewarding environment for plaintiff's lawyers without improving consumer privacy or reducing the number of illegal robocalls. Although the U.S. Supreme Court's decision in *Facebook v. Duguid*,¹⁴ which narrowly interpreted the definition of an "automated telephone dialing system," proved favorable to reduce liability exposure for businesses using automated calling technologies, greater action is required to ebb the tide of abusive litigation.

Congress and the FCC have taken significant steps recently to address this problem. In 2019, Congress passed the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act, which directed the FCC to require voice service providers to implement call authentication to the Internet Protocol (IP) portions of their networks and provided the FCC with authority to issue additional civil and criminal penalties under the TCPA.¹⁵

The TRACED Act also required the FCC "to establish a registration process for the registration of a single consortium that conducts private-led efforts to trace back the origin of suspected unlawful robocalls."¹⁶ The FCC first selected USTelecom—The Broadband Association's Industry Traceback Group (ITG) as the single registered consortium to conduct private-led traceback efforts, and has re-designated the ITG each year since.¹⁷ The ITG collaborates with providers across wireline, wireless, Voice over Internet Protocol (VoIP), and cable services; and with U.S. federal and state law enforcement agencies, including the FCC, FTC, DOJ, Social Security Administration (SSA), and states attorneys general offices "in identifying voice service providers and their customers responsible for illegal robocalls."¹⁸

In addition, the FCC requires all providers—including voice service providers, gateway providers (U.S.-based intermediate providers that receive calls directly from a foreign originating or intermediate provider), and intermediate providers that receive unauthenticated calls directly from originating providers—to implement robocall mitigation programs and file these plans

¹⁴ 592 U.S. 395 (2021).

¹⁵ *Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act*, Pub. L. No. 116-105 (2019).

¹⁶ *Id.* § 13(a).

¹⁷ Indus. Traceback Grp., About, <https://tracebacks.org/about/> (last visited July 15, 2026); *Implementing Section 13(d) of the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (TRACED Act)*, Report and Order, DA 20-785 (Fed. Communications Comm'n July 27, 2020), <https://docs.fcc.gov/public/attachments/DA-20-785A1.pdf>.

¹⁸ Indus. Traceback Grp., About, <https://tracebacks.org/about/> (last visited July 15, 2026).

along with certifications in the Robocall Mitigation Database.¹⁹ Providers may only accept voice calls directly from another provider if that provider’s filing appears in the database.

Unfortunately, rapid technological advancements have proliferated illegal and scam robocalls. Making this problem worse, a significant proportion of illegal and scam robocalls calls, if not the majority, originate from overseas.²⁰ Illegal and scam robocalls that originate abroad, and difficulties reaching foreign-based robocallers, present “one of the most vexing challenges facing” the FCC.²¹

C. Rural Broadband Programs

In May 2022, the Government Accountability Office (GAO) released a study analyzing federal broadband programs. It identified over 130 federal programs—administered by 15 agencies—that could be used to expand broadband access.²² Given the number of programs, interagency coordination is critical. Historically, federal agencies have not coordinated their funding decisions. As a result, they have awarded funds that overbuilt areas that already have broadband service from a private sector provider or are served by a project funded by another agency. Further, navigating the myriad federal broadband support programs can be challenging, as these programs often have different qualifications and applications, address different needs, and may not be well promoted.

Congress has worked to improve interagency coordination. The Consolidated Appropriations Act, 2021 established the Office of Internet Connectivity and Growth at the National Telecommunications and Information Administration (NTIA),²³ which is tasked with tracking broadband support programs within the Executive Branch and streamlining and standardizing the process for applying for federal broadband support. Congress also directed the FCC, NTIA, and the Department of Agriculture to enter into an interagency agreement to coordinate the distribution of federal funds for broadband programs, to prevent duplication of support, and ensure stewardship of taxpayer dollars.²⁴ The agencies have since added Treasury to this agreement.²⁵

¹⁹ *Combating Spoofed Robocalls with Caller ID Authentication*, Fed. Communications Comm’n, <https://www.fcc.gov/call-authentication> (last visited July 15, 2026).

²⁰ Press Release, Fed. Trade Comm’n, *FTC Ramps Up Fight to Close the Door on Illegal Robocalls Originating from Overseas Scammers and Imposters* (Apr. 11, 2023), <https://www.ftc.gov/news-events/news/press-releases/2023/04/ftc-ramps-fight-close-door-illegal-robocalls-originating-overseas-scammers-imposters>.

²¹ *Report to Congress on Robocalls and Transmission of Misleading or Inaccurate Caller Identification Information*, Report, DOC-378593 (Fed. Communications Comm’n Dec. 2021), <https://docs.fcc.gov/public/attachments/DOC-378593A1.pdf>.

²² U.S. GOV’T ACCOUNTABILITY OFFICE, GAO-22-104611, NATIONAL STRATEGY NEEDED TO GUIDE FEDERAL EFFORTS TO REDUCE DIGITAL DIVIDE (2022), <https://www.gao.gov/products/gao-22-104611>.

²³ Consolidated Appropriations Act, 2021, Pub. L. No. 116-260, div. FF, tit. IX, § 903 (2020).

²⁴ *Id.*, § 904; Press Release, NTIA, *NTIA, FCC and USDA Announce Interagency Agreement to Coordinate Broadband Funding Deployment* (June 25, 2021), <https://www.ntia.doc.gov/press-release/2021/ntia-fcc-and-usda-announce-interagency-agreement-coordinate-broadband-funding>.

²⁵ *Memorandum of Understanding Regarding Information Sharing* dated as of May 9, 2022, between the Fed. Communications Comm’n, U.S. Dep’t of Agric., Nat’l Telecommunications & Info. Admin., & U.S. Dep’t of the Treasury, https://www.ntia.doc.gov/files/ntia/publications/interagency_broadband_mou.pdf.

Increased federal broadband spending also highlights the importance of broadband mapping to identify which areas have broadband and which do not. In 2020, Congress enacted the Broadband DATA Act to reform the FCC's mapping process,²⁶ which previously overstated broadband availability. The law directed the FCC to identify every broadband-serviceable location in the country, collect location-based broadband availability data from providers every six months, establish a challenge process to verify the accuracy of that data, and develop a process for state and local governments and third parties to submit availability data. The FCC released the first edition of this map in November 2022 and has released updates every six months since then.²⁷ In addition, the IIJA directed the FCC to establish a map showing where the Federal government (FCC, NTIA, USDA, and Treasury) is funding broadband deployment to ensure better interagency coordination to avoid overbuilding and duplication of funding.²⁸

D. Artificial Intelligence

The United States is on the cutting edge in artificial intelligence (AI) innovation. As development continues to advance, it's crucial that we leverage its powerful capabilities to benefit our communications and technology industries. AI is currently being deployed throughout communications networks to help optimize network usage, enhance cybersecurity, and improve public safety operations.²⁹ Networks using AI can leverage advanced analytics to determine the most efficient allocation of resources during peak usage.³⁰ AI can automate certain processes, including troubleshooting network issues and managing routine maintenance, which reduces the hands-on time needed to do these tasks.³¹ Some network operators deploy AI to monitor and automate core network functions, which they have found to reduce the number of outages.³²

Additionally, AI enables communications providers to improve customer service, with providers using AI to improve the speed and quality of responses to consumer inquiries³³ and detect and block robocalls.³⁴ When it comes to cybersecurity, AI can be used to bolster the security of our networks by implementing systems to detect malware, run pattern recognition, and identify even the smallest, unusual behaviors or specific patterns before they compromise the

²⁶ Broadband Deployment Accuracy and Technological Availability (DATA) Act, Pub. L. No. 116-130 (2020).

²⁷ *FCC National Broadband Map*, Fed. Communication Comm'n, <https://broadbandmap.fcc.gov/home> (last visited July 15, 2026).

²⁸ *Id.*

²⁹ Diana Goovaerts & Julia King, *Money Pit or Money Maker: AT&T, Windstream Talk AI ROI*, Fierce Network (Jan. 2, 2025), <https://www.fierce-network.com/cloud/money-pit-or-money-maker-att-windstream-talk-ai-roi>.

³⁰ Niall Byrne & Krishnamurthy Srinivasan, *AI-Powered Network Optimization: Unlocking 5G's Potential with Amdocs* (Feb. 27, 2025), <https://cloud.google.com/blog/topics/telecommunications/ai-powered-network-optimization-unlocking-5gs-potential-with-amdocs/>.

³¹ *Id.*

³² Jeff Heynen, *AI's Impact on Broadband Networks*, Dell'Oro Group (Aug. 10, 2023), <https://www.delloro.com/ais-impact-on-broadband-networks/>.

³³ Rose de Fremery, *How AI Customer Service Can Help Enable Better Interactions*, Verizon, <https://www.verizon.com/business/resources/articles/s/how-ai-customer-service-can-help-enable-better-interactions/> (last accessed Apr. 1, 2025).

³⁴ John Popham, *Robocalls No Match for AI-powered Virtual Assistant*, Georgia Tech College of Computing (Feb. 20, 2023), <https://www.cc.gatech.edu/news/robocalls-no-match-ai-powered-virtual-assistant>.

network. Across the board, companies are utilizing AI to increase efficiency, performance, and service, while reducing their operation and expenditure costs.³⁵

IV. LEGISLATION

The Subcommittee will discuss the following legislation:

A. H.R.9129, the Guarding the U.S. Against Adversarial Robotics Dominance (GUARD) Act of 2026 (Rep. Moolenaar)

This legislation is led by Representative John Moolenaar (R-MI), Representative Jay Obernolte (R-CA), and Representative Jennifer McClellan (D-VA). The bill would require national security agencies to study whether certain humanoid or quadruped robotics communications equipment and services pose unacceptable risk to U.S. national security or the security and safety of U.S. persons. If such determination is made, the FCC would then add such covered equipment or services to the covered list. The legislation also includes a rule of construction preventing the underlying provisions from being applied to any country that is not a country of concern.

B. H.R. 6152, Foreign Robocall Elimination Act (Rep. McDowell)

This legislation is led by Representative Addison McDowell (R-NC), Representative Kelly Morrison (D-MN), Representative Gregory Steube (R-FL), and Representative Jimmy Panetta (D-CA). The bill would create an interagency task force on unlawful robocalls and directs it to prepare a report with recommendations on effective ways to combat unlawful robocalls made into the United States from abroad. It would also extend the term for the registered consortium to conduct private-led traceback efforts from one year to three, provide immunity for receiving, sharing and publishing traceback information, and require providers to post a bond if the FCC determines that posting such a bond is necessary to preserve the integrity of the Robocall Mitigation Database.

C. H.R. 1027, QUIET Act (Reps. Sorensen and Ciscomani)

This legislation is led by Rep. Eric Sorensen (D-IL) and Rep. Juan Ciscomani (R-AZ). It would update the TCPA to require disclosing the use of AI to emulate a human being in a robocall. It would also enhance penalties for using AI to impersonate an individual or entity when making a call or sending a text, with the intent to defraud, cause harm, or wrongfully obtain anything of value.

³⁵ Mischa Dohler, *AI and Automation Revolutionizing Telecom AI* (Jan. 23, 2025), <https://mischadohler.com/ai-and-automation-revolutionizing-telecom-ai>.

D. H.R. 7294, AI for Secure Networks Act (Reps. Menendez and Pfluger)

This legislation is led by Representative Robert Menendez (D-NJ) and Representative August Pfluger (R-TX). It would require the Department of Commerce to conduct a study on the impacts of AI technology with respect to the security of telecommunications networks.

E. H.R.2805, PLAN for Broadband Act (Rep. Walberg)

This legislation is led by Representative Tim Walberg (R-MI) and Representative Scott Peters (D-CA). It would direct NTIA to develop a National Strategy to Close the Digital Divide to improve management and coordination of federal broadband programs and deployment efforts. It would also direct NTIA to develop a plan for implementing the strategy.

F. H.R.4950, Data Broadband Reporting and Integration for Deployment in Geographically Essential Areas Act (Rep. Houchin)

This legislation is led by Representative Erin Houchin (R-IN) and Representative Robin Kelly (D-IL). It would direct the FCC to update its broadband maps to include data on the location of agricultural areas.

V. KEY QUESTIONS

The hearing may include discussion on the following key issues:

- What are the lessons learned from implementation of the Secure and Trusted Communications Networks Act and the FCC's subsequent addition of drones and routers to the covered list? And should we consider any related updates to the GUARD Act?
- How can we reduce the number of illegal robocalls originating from other countries?
- How can we better coordinate federal broadband programs?
- Why is it crucial that we get a head start on utilizing artificial intelligence to improve and secure our telecommunications networks?

VI. STAFF CONTACTS

If you have any questions regarding this hearing, please contact Michael Essington, John Lin, Elaina Murphy, or Dylan Rogers of the Majority Committee Staff at (202) 225-3641.