

RON WYDEN
OREGON

CHAIRMAN OF COMMITTEE ON
FINANCE

221 DIRKSEN SENATE OFFICE BUILDING
WASHINGTON, DC 20510
(202) 224-5244

United States Senate
WASHINGTON, DC 20510-3703

COMMITTEES:
COMMITTEE ON FINANCE
COMMITTEE ON THE BUDGET
COMMITTEE ON ENERGY AND NATURAL RESOURCES
SELECT COMMITTEE ON INTELLIGENCE
JOINT COMMITTEE ON TAXATION

October 11, 2024

The Honorable Jessica Rosenworcel
Chairwoman
Federal Communications Commission
45 L Street NE
Washington, DC 20554

The Honorable Merrick B. Garland
Attorney General
Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530

Dear Chairwoman Rosenworcel and Attorney General Garland:

I write to insist that your agencies finally act to secure U.S. telephone and broadband companies' wiretapping systems from hackers. Congress required these systems be secure 30 years ago, as part of a 1994 law requiring phone companies to add wiretapping capabilities to their networks. However, instead of adequately implementing this provision, the government has never adopted mandatory security standards for these highly sensitive systems, which has reportedly resulted in serious harm to national security.

The Wall Street Journal recently reported that suspected-Chinese government hackers may have breached the wiretapping systems of major U.S. phone and residential broadband companies, including AT&T, Verizon, and Lumen Technologies. If accurate, this intrusion could enable China to identify targets of U.S. government surveillance and to surveil Americans.

These telecommunications companies are responsible for their lax cybersecurity and their failure to secure their own systems, but the government shares much of the blame. The surveillance systems reportedly hacked were mandated by federal law, through the Communications Assistance for Law Enforcement Act (CALEA). CALEA, which was enacted in 1994 at the urging of the Federal Bureau of Investigations (FBI), forced phone companies to install wiretapping technology into then-emerging digital phone networks. In 2006, acting on a request from the FBI, the Federal Communications Commission (FCC) expanded this backdoor mandate to broadband internet companies.

During the Congressional hearings for CALEA, cybersecurity experts warned that these backdoors would be prime targets for hackers and foreign intelligence services. However, these concerns were dismissed by then-FBI Director Louis J. Freeh, who testified to Congress that experts' fears of increased vulnerability were "unfounded and misplaced." Congress, relying on the FBI Director's assurances that the security risks experts warned about could be addressed, passed the law mandating backdoors. The Department of Justice (DOJ) received \$1 billion in

911 NE 11TH AVENUE
SUITE 630
PORTLAND, OR 97232
(503) 326-7525

405 EAST 8TH AVE
SUITE 2020
EUGENE, OR 97401
(541) 431-0229

SAC ANNEX BUILDING
105 FIR ST
SUITE 201
LA GRANDE, OR 97850
(541) 962-7691

U.S. COURTHOUSE
310 WEST 6TH ST
ROOM 118
MEDFORD, OR 97501
(541) 858-5122

THE JAMISON BUILDING
131 NW HAWTHORNE AVE
SUITE 107
BEND, OR 97701
(541) 330-9142

707 13TH ST, SE
SUITE 285
SALEM, OR 97301
(503) 589-4555

[HTTPS://WYDEN.SENATE.GOV](https://wyden.senate.gov)

PRINTED ON RECYCLED PAPER

today's dollars to provide industry grants for the development and purchase of new wiretapping technology.

The 103rd Congress was clearly concerned about the security and privacy risks to Americans' communications; CALEA directs the FCC to issue regulations requiring companies to secure their wiretapping systems. During the FCC's rulemaking process, cybersecurity professionals urged the agency to require specific cyberdefenses; for example, a 1997 comment to the FCC called for "authentication procedures, audit trails, intrusion detection measures, and other standard components of computer security." But the FCC declined to do so, stating that it did not want to "micro-manage" companies' practices. The FCC has failed to update these regulations to require specific cybersecurity defenses in the 25 years since, even after examples of spies targeting and compromising wiretapping systems became public. Notable examples include the 2009 reported breach of Google's surveillance system by Chinese government hackers and the 2004 breach of Greece's largest phone company, in which the company's lawful interception system was reportedly used to surveil the country's prime minister as well as top officials at the Ministries of Defense and Foreign Affairs.

While the government has released no public information about the most recent hack, if the press reports are accurate, it may have caused enormous harm to U.S. national security.

Chairwoman Rosenworcel, your agency has the authority to require strong cybersecurity defenses in these systems today. The FCC should initiate a rulemaking process to update the CALEA regulations to fully implement the system security requirements in the law. At a minimum, these updated regulations should establish baseline cybersecurity standards for telecommunications carriers, enforced by steep fines; require independent, annual third-party cybersecurity audits; require board-level cybersecurity expertise; and require senior executives annually sign certifications of compliance with the cybersecurity standards.

Attorney General Garland, this latest hack highlights the inadequacies of the DOJ's current approach to cybersecurity. I urge the DOJ to take the following actions:

First, DOJ should recognize the failure of its current approach to combating cyberattacks. These data breaches are the direct result of corporate negligence, yet DOJ goes to extreme lengths to shield companies from accountability, including hiding information about security incidents from Congress, consumers, and investors. Moreover, the DOJ does not share this information with federal regulators that have the authority to force the companies to address these security lapses. While federal investigations and prosecutions of foreign hackers can yield valuable results, it would be short-sighted in the extreme for the DOJ to prioritize criminal prosecutions of foreign hackers who are almost never brought to justice, above holding companies accountable for negligent cybersecurity. These companies are corporate scofflaws that have harmed the public and our national security through their negligence. DOJ can prevent future cyberattacks and incentivize improvements in corporate cybersecurity by working with regulators to hold companies accountable for security failures, which will inform much-needed Congressional

oversight, enable consumers and investors to protect themselves by voting with their wallets, and ultimately, protect national security.

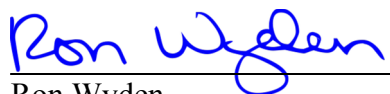
Second, DOJ must stop pushing for policies that harm Americans' privacy and security by championing surveillance backdoors in other communications technologies, like encrypted messaging apps. There is, and has long been, broad consensus among cybersecurity experts that wiretapping capabilities undermine the security of communications technology and create an irresistible target for hackers and spies. Even so, law enforcement officials, including your predecessor, as well as the current and former FBI Directors, have denied this reality, spread disinformation about non-existent secure backdoors, and sought to pressure companies to weaken the security of their products.

Third, DOJ should investigate whether the companies that were reportedly hacked in this incident violated federal law, including CALEA and the False Claims Act. As recent breaches have demonstrated, these companies have been negligent in their cybersecurity across the board, beyond just their wiretap systems. DOJ must use its authorities to investigate these companies' statutory and regulatory compliance and, where these companies are government contractors, ensure that these companies are not falsely claiming to satisfy required cybersecurity standards.

The recently reported hack of U.S. telecommunications companies' wiretapping systems should serve as a major wake-up call to the government. The outdated regulatory framework and DOJ's failed approach to combating cyberattacks by protecting negligent corporations must be addressed. The security of our nation's communications infrastructure is paramount, and the government must act now to rectify these longstanding vulnerabilities.

Thank you for your attention to this important matter. If you have any questions about this request, please contact Chris Soghoian in my office.

Sincerely,



Ron Wyden
United States Senator