RON WYDEN
OREGON

RANKING MEMBER 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

833

November 6, 2019

The Honorable Ajit Pai
Chairman
Federal Communications Commission
445 12th Street Southwest
Washington, D.C. 20554

Dear Chairman Pai:

I write to urge you to act to secure our nation's next-generation, 5G telephone networks.

Unencrypted cellular phone calls and other wireless communications have long been vulnerable to interception by criminals and spies. Surveillance technology companies openly sell products that exploit these flaws to intercept calls, track phones and infect phones with malware. Indeed, last year, DHS revealed that it discovered cell phone spying devices near the White House. This decades-long cybersecurity vulnerability has undoubtedly caused massive harm to our national security, and the damage continues with each sensitive call or text that is tapped.

According to technical experts, it simply isn't feasible to secure current phone networks due to the flaws in the 2G, 3G and 4G technology. However, the wireless industry is now in the early stages of building out the new 5G cellular technology, which includes cybersecurity protections that address many of the known vulnerabilities that have been exploited for years by hackers and foreign governments. Many of these important security defenses are optional in 5G, leaving it up to each wireless carrier to turn them on.

In September 2018, the FCC's Communications Security, Reliability, and Interoperability Council (CSRIC) recommended that carriers encrypt user data and signaling information. However, to date, the wireless networks have not publicly committed to turning on these optional cybersecurity protections. The FCC must act to ensure that encryption and authentication features included in 5G standards are enabled by AT&T, Verizon and T-Mobile as they upgrade their networks.

For decades, wireless carriers have ignored known cybersecurity vulnerabilities that foreign governments were and are still actively exploiting to target Americans. The market has failed to incentivize cybersecurity, in part because consumers have no way of comparing the cybersecurity practices of phone companies.

The FCC has the authority to regulate wireless carriers and their use of the public airwaves, particularly in areas that involve public safety and national security. The FCC must stop leaving

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

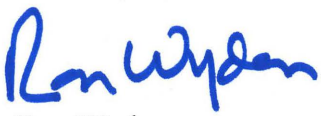
the cybersecurity of American consumers, businesses and government agencies to wireless carriers and finally secure America's next-generation 5G networks against interception and hacking by criminals and foreign spies. In order to help Congress and the American people understand the FCC's plans to address this national security threat, please provide me with answers to the following questions by December 6, 2019:

1. The National Institute of Standards and Technology has recommended since 2005 that phone calls and text messages be encrypted in order to prevent security breaches. Does the FCC agree with this recommendation? If yes, what steps has the FCC taken to encourage or require that wireless carriers encrypt phone calls and text messages?
2. Does the FCC believe that AT&T, T-Mobile and Verizon will all enable the optional security features in their 5G networks necessary to protect communications from being intercepted by commercially available interception technology?
3. Does the FCC know when carriers still operating 2G, including rural roaming carriers, will be retiring their 2G networks?
4. Does the FCC believe that phone operating system and handset vendors should provide users with a way to disable the use of 2G networks in order to avoid unintentionally connecting to malicious 2G networks?
5. Does the FCC believe that handset and operating system makers should automatically disable the capability to connect to 2G networks when a phone is in an area where newer, more secure networks are available?
6. What steps has the FCC taken to assess the cybersecurity of Rich Communication Services (RCS), the next-generation of voice and text services that U.S. carriers have recently announced they are upgrading to?
7. Does the FCC believe that voice calls and text messages should be encrypted end-to-end within 5G mobile networks? If yes, has it taken action to require carriers to do so? If not, does the FCC believe it has the legal authority to require carriers to enable end-to-end encryption?
8. The FCC's 2018 Restoring Internet Freedom Order includes a transparency requirement that "will ensure that consumers have the information necessary to make informed choices about the purchase and use of broadband Internet access service." Does the FCC consider the wireless carriers' current disclosure practices regarding the security of their networks to be sufficient for consumers to evaluate and compare wireless providers' cybersecurity?
9. Paragraph 220 of the 2018 Order requires the disclosure of "[a]ny practices used to ensure end-user security or security of the network." Does the FCC believe that wireless carriers have an obligation to disclose to consumers whether a given call or text messages is encrypted end-to-end? If yes, how should consumers and other network users do so?

10. The FCC has successfully used neutral third parties to measure network characteristics, such as the on-going Measuring Broadband America program for measuring fixed and mobile network performance, providing consumers and policy makers with trustworthy information on the performance of networks. Security is at least as important as performance. Do you believe that neutral, third-party assessments of wireless carriers' network security would help consumers and businesses make decisions about which company to whom they will entrust their communications?

Thank you for your attention to this important matter.

Sincerely,



Ron Wyden
United States Senator