FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF
THE CHAIRMAN

January 3, 2020

The Honorable Ron Wyden
United States Senate
221 Dirksen Senate Office Building
Washington, DC 20510

Dear Senator Wyden:

Thank you for your letter regarding the security of 5G wireless networks. For my part, I have frequently discussed my support for addressing 5G security issues upfront.[1] Making the right choices before deployment is much easier than trying to correct mistakes once network construction and operation is well underway. 5G security decisions must be made with the long-term in mind and in coordination with our international partners (where possible). Last May, more than 140 representatives from 32 countries came together to develop the Prague Proposals, a consensus approach for protecting next-generation networks. As acknowledged in the Proposals, there are no universal solutions to security. Rather, "[t]he decision on the most optimal path forward when setting the proper measures to increase security should reflect unique social and legal frameworks, economy, privacy, technological self-sufficiency and other relevant factors important for each nation."[2]

In 2019, the FCC tasked the Communications Security, Reliability, and Interoperability Council (CSRIC), a Federal Advisory Committee designed to promote the security, reliability, and resiliency of the Nation's communications systems, with identifying the optional features in proposed 3GPP standards that, if not implemented, can diminish the effectiveness of 5G security. The CSRIC was further asked to recommend ways to address these gaps. This work is ongoing, with recommendations due by March 2021. The group is well represented by experts in this area, which should make their recommendations more likely to be implemented.

Notably, the FCC historically has adopted flexible-use policies for spectrum bands. The FCC does not mandate a particular technology or air interface that licensees must deploy on a particular spectrum band. Rather, the FCC adopts minimal technical and operating rules to protect against harmful interference to co-channel and adjacent-channel operations in the band. Licensees, through standards-setting bodies like 3GPP, develop standards and protocols for mobile wireless network technologies such as 4G LTE and 5G.

---

[1] *See, e.g.*, Remarks of Chairman Ajit Pai at the Prague 5G Security Conference 2 (May 2, 2019), https://docs.fcc.gov/public/attachments/DOC-357288A1.pdf.

[2] https://www.vlada.cz/en/media-centrum/aktualne/prague-5g-security-conference-announced-series-ofrecommendations-the-prague-proposals-173422/.

End-to-end encryption of voice calls and text messages raises a number of important legal, economic, privacy, technological and other considerations that must be taken into account. The need to deploy this technology is likely to vary depending on the circumstances, such as the type of customer, the subject matter of the communication, the locations of the communicating parties, and other considerations. End users are usually in best positioned to make risk-based determinations as to whether or not end-to-end encryption is needed. In addition, mobile wireless carriers must be able to continue to meet their obligations under the Communications Assistance for Law Enforcement Act.

Today, there are several applications available to consumers that encrypt voice calls and messages.[3] In addition, both AT&T and Verizon currently offer encryption services for enterprise and government customers according to publicly available information. AT&T's Encrypted Mobile Voice service "provides mobility customers with end to end security features for confidential and sensitive calls."[4] Verizon's Cypher encryption software offers end-to-end encryption for commercial smartphones.[5] Verizon previously has stated that "[t]he evolution toward a fully-realized 5G environment will bring even stronger security—more encryption, more defense at the edge, and greater potential for creating secure enclaves or 'slices.'" Verizon also has stated that it "intend[s] to leverage all of these tools as the network develops."[6] These carriers and T-Mobile appear to compete with one another to differentiate themselves on the security of their mobile wireless service offerings—at least to certain customer segments that may find particular value in these services.

While the Commission has not taken a formal stance on the use of encryption, the issue has been addressed in the context of advisory committees. In 2009, FCC tasked the CSRIC to recommend best practices that encourage communications service providers to secure their networks. In March 2011, CSRIC recommended that the Commission encourage communications service providers to incorporate standards-based encryption services on their networks. CSRIC recommended that communications service providers "incorporate cellular voice encryption services and ensure that such encryption services are enabled for end users" and "encourage the use of IPsec VPN, wireless TLS, or other end-to-end encryption services over the cellular/wireless network." While the Commission does not track service provider implementation of CSRIC best practices, they were developed and recommended by practitioners, which increases the likelihood that they will be implemented by communications providers. The Commission makes CSRIC best practices available to the public through a Commission-hosted database, which is available at https://opendata.fcc.gov/Public-Safety/CSRIC-Best-Practices/qb45-rw2t/data.

---

[3] Andy Greenberg, *How to Encrypt All of the Things*, Wired (Dec. 9, 2017), https://www.wired.com/story/encrypt-all-of-the-things/ (noting that "[t]hanks in part to drop-dead simple, increasingly widespread encryption apps like Signal, anyone with a vested interest in keeping their communications away from prying eyes has no shortage of options.").

[4] https://www.wireless.att.com/businesscenter/en_US/pdf/terms-and-conditions-PB-EMV-20788-V05-10-13-10.pdf.

[5] https://enterprise.verizon.com/resources/articles/verizon-cypher-encryption-software/.

[6] https://www.linkedin.com/pulse/verizons-approach-5g-security-craig-silliman.

You also ask about the retirement of predecessor wireless technologies. According to publicly available information, AT&T has already discontinued its 2G network and Verizon Wireless and T-Mobile are expected to shut-down their 2G networks in the near future. Specifically, AT&T discontinued service on its 2G wireless network in January 2017.[7] Consistent with its public statements, in its recently filed FCC Form 477 data AT&T no longer reports having 2G service. Verizon Wireless has stated that it planned to shut down its 2G CDMA network by the end of 2019.[8] T-Mobile previously has stated that it will support 2G until December 2020,[9] and Sprint has indicated that the termination of its CDMA network is not expected to commence prior to January 2021.[10] Among the aforementioned 2G service providers, T-Mobile and Verizon have made changes to their devices' configuration settings that allow users to disable 2G. The Commission is also aware that certain smaller carriers have not announced their plans to switch-off their 2G networks. The Commission will continue to monitor communications service providers' efforts to phase out 2G networks and encourage them to invest in more secure networks.

Finally, you ask about the FCC's 2018 *Restoring Internet Freedom Order*'s transparency requirement. Given the sheer number of ISPs offering service throughout the country, the Commission has determined that the most effective way for it to monitor compliance is to require public disclosure of an ISP's practices so that "consumers, entrepreneurs, and other small business [can] report to the Commission any market-barriers they discover."[11] The FCC has provided a portal and instructions for consumers to access ISPs' transparency disclosures,[12] and consumers can file informal complaints using the FCC's Consumer Complaint Center as well as by phone or by mail.[13] Notably, the transparency rule only applies to broadband Internet access service, not to voice and text-messaging services.

Our transparency rules amplify the power of antitrust law and the FTC Act to deter—and where needed, remedy—behavior that harms consumers. Although the rules require providers to disclose security practices, they do not specifically address encryption and "[t]he Commission's primary concern is those security measures likely to affect a consumer's ability to access the content, applications, services, and devices of his or her choice."[14] The Commission "do[es] not expect ISPs to disclose internal network security measures that do not directly bear on a

---

[7] https://about.att.com/innovationblog/2g_sunset.

[8] *See Applications of T-Mobile US, Inc., and Sprint Corp. for Consent to Transfer Control of Licenses and Authorizations, et al.*, Memorandum Opinion and Order, Declaratory Ruling, and Order of Proposed Modification, WT Docket No. 18-197, FCC 19-103 at para. 335 & n.1177 (2019) (*Sprint/T-Mobile Order*).

[9] https://www.geotab.com/blog/2g-network-shutdown/.

[10] *Sprint/T-Mobile Order* at para. 298.

[11] *RIF Order* at para. 228.

[12] https://www.fcc.gov/isp-disclosures.

[13] *See* https://www.fcc.gov/consumers/guides/filing-informal-complaint; https://consumercomplaints.fcc.gov/hc/en-us.

[14] *RIF Order* at para. 220 & n.814.

consumer's choices."[15] Finally, as noted in the *Restoring Internet Freedom Order*, the Commission has had transparency requirements in place since 2010, and there have been very few incidents in the U.S. since then that plausibly raise openness concerns.[16]

Please let me know if I can be of any further assistance.

Sincerely,

Ajit V. Pai

[15] *Id.*

[16] *RIF Order* at para. 241.