

ONE HUNDRED SIXTEENTH 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) 225-2927
Minority (202) 225-3641

January 11, 2019

The Honorable Ajit V. Pai
Chairman
Federal Communications Commission
445 12th Street SW
Washington, DC 20554

Dear Chairman Pai:

I write to request that on Monday, January 14, 2019, either you or your designate provide an emergency briefing to Committee staff. This briefing should explain why the Federal Communications Commission (FCC) has yet to end wireless carriers' unauthorized disclosure of consumers' real-time location data and what actions the FCC has taken to address this issue to date. An emergency briefing is necessary in the interest of public safety and national security, and therefore cannot wait until President Trump decides to reopen the government.

Bad actors can use location information to track individuals' physical movements without their knowledge or consent. If recent reports detailing the cheap, accurate, and easy accessibility of legally protected, real-time location data are true, we must work expeditiously to address these public safety concerns.¹ If we don't, the privacy and security of everyone who subscribes to wireless phone service from certain carriers—including government officials, military personnel, domestic violence victims, and law enforcement officials—may be compromised.²

As you know, Congress addressed this issue when it passed the Communications Act in 1996. That law and its implementing rules require wireless carriers—and their vendors with

¹ *I Gave a Bounty Hunter \$300. Then He Located Our Phone*, Motherboard (Jan. 8, 2019) (motherboard.vice.com/en_us/article/nepxbz/i-gave-a-bounty-hunter-300-dollars-located-phone-microbilt-zumigo-tmobile).

² *See id.*

whom the information is shared³—to safeguard such information⁴ and to get users' consent before disclosing it with anyone else.⁵

Last May investigative journalists and Senator Wyden helped bring to light the ease with which consumers' real-time location data was being made available to the public.⁶ Following those revelations, the FCC referred the allegations to its Enforcement Bureau for investigation.⁷ In June, some wireless carriers publicly committed to addressing the issue and put an end to this unauthorized disclosure.⁸ Yet new reports indicate this unfortunate practice continues.⁹

The FCC once again appears to have dragged its feet in protecting consumers. While some carriers have now recommitted to stopping such unauthorized disclosure, the public can no longer rely on their voluntary promises to protect this extremely sensitive information. The FCC must take immediate action to ensure no wireless carrier is allowing the rampant disclosure of real-time location data, and take enforcement action against carriers that violated the Commission's rules and the trust of their customers.¹⁰

In light of this Committee's commitment to protect the privacy of the American people, I request an emergency staff briefing on this issue, so we can understand when the FCC will put an

³ 47 U.S.C. § 217.

⁴ 47 C.F.R. § 64.2010.

⁵ 47 U.S.C. § 222(f)(1).

⁶ *Service Meant to Monitor Inmates' Calls Could Track You, Too*, New York Times (May 10, 2018); *Hacker Breaches Securus, the Company That Helps Cops Track Phones Across the US*, Motherboard (May 16, 2018) (motherboard.vice.com/en_us/article/gykgv9/securus-phone-tracking-company-hacked); *Tracking Firm LocationSmart Leaked Location Data for Customers of All Major U.S. Mobile Carriers Without Consent in Real Time Via Its Web Site*, Krebs on Security (May 18, 2018) (krebsonsecurity.com/2018/05/tracking-firm-locationsmart-leaked-location-data-for-customers-of-all-major-u-s-mobile-carriers-in-real-time-via-its-web-site/); *A Location-Sharing Disaster Shows How Exposed You Really Are*, Wired (May 19, 2018) (www.wired.com/story/locationsmart-securus-location-data-privacy/).

⁷ *FCC Is Investigating A Website Flaw That Exposed Mobile Phone Locations*, CNBC (May 21, 2018) (www.cnbc.com/2018/05/21/fcc-is-investigating-a-website-flaw-that-exposed-mobile-phone-locations.html).

⁸ See e.g., *Verizon to Stop Selling Phone Location Data to Third Parties*, Reuters (June 19, 2019) (www.reuters.com/article/us-verizon-privacy-idUSKBN1JF28D).

⁹ See note 1.

¹⁰ *AT&T to Stop Selling Location Data to Third Parties After Motherboard Investigation*, Motherboard (Jan. 10, 2019) (motherboard.vice.com/en_us/article/nepab8/att-stop-selling-location-data-tmobile-sprint-microbilt-zumigo).

The Honorable Ajit V. Pai
January 11, 2019
Page 3

end to the unauthorized sharing of this data. Thank you for your attention to this serious matter. If you have any questions, please contact Gerald Leverich of the Democratic Staff at (202) 225-3641

Sincerely,

A handwritten signature in blue ink that reads "Frank Pallone, Jr." in a cursive style.

Frank Pallone, Jr.
Ranking Member