Congress of the United States
Washington, DC 20515

June 24, 2019

Ajit Pai
Chairman
Federal Communications Commission
445 12th Street SW
Washington, DC 20554

Dear Chairman Pai,

Nearly 12 million people experience domestic violence, sexual violence, or stalking each year. Abusers and stalkers often exploit technology to gain access to their victims' location through GPS tracking and other cell phone apps, forcing victims to get new phones or wipe their current ones when they are trying to leave these dangerous situations.[1] For this reason and countless others, we were extremely troubled to read about the ease with which wireless customers' real-time location data can be acquired. We write today to weigh in on behalf of domestic violence victims across the country and to ask you to protect this information to the fullest extent possible.

Over a year ago, we learned that the major wireless carriers were using third-party aggregators to share their customers' real-time location data for a number of legitimate reasons, including emergency services, roadside assistance, and fraud prevention. The third-party aggregators were then reselling the data to other companies and people, apparently without customers' consent and with little to no ongoing oversight by the wireless companies.[2] For example, one aggregator, LocationSmart, sold data to a company called Securus, who then provided phone tracking services to local law enforcement without requiring a warrant.[3] LocationSmart also sold their data through a "buggy website panel" that allowed anyone without prior authorization or authentication to search for real-time location.[4] At that time, the carriers pledged to stop sharing this data with third-parties, and the FCC said it would investigate.[5]

But according to a Motherboard investigative report six months later, wireless customers' real-time location data was still being widely shared and easily obtainable by anyone.[6] Additional reports indicate individuals have been able to purchase another person's geolocation for only a

---

[1] https://www.consumer.ftc.gov/blog/2015/02/technology-tips-domestic-violence-and-stalking-victims
[2] https://www.multichannel.com/news/rep-walden-on-edge-over-geolocation-data-sharing
[3] https://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/
[4] https://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/
[5] https://money.cnn.com/2018/06/19/technology/telecom-location-data/index.html
[6] https://www.vice.com/en_us/article/nepxbz/i-gave-a-bounty-hunter-300-dollars-located-phone-microbilt-zumigo-tmobile

couple of hundred dollars, allowing this critical information to be easily found by anyone interested in obtaining it.[7]

Though the major wireless companies have apparently stopped sharing this information, we are concerned about who may have access to the data that has already been shared and want to ensure there is no confusion about its protection under the law. In the wrong hands, domestic violence perpetrators could use this information to track down victims, even when these victims have been intentionally housed in locations otherwise undisclosed, such as domestic violence shelters, where victims believe themselves to be safe.

We urge you to take this matter seriously and to protect real-time location data to the fullest extent allowed under law, because domestic violence victims, victims of sex trafficking, and individuals in sensitive locations are at risk.

Sincerely

Gwen S. Moore
MEMBER OF CONGRESS

Debbie Dingell
MEMBER OF CONGRESS

[7] https://www.vice.com/en_us/article/nepxbz/i-gave-a-bounty-hunter-300-dollars-located-phone-microbilt-zumigo-tmobile