

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 BUDGET

COMMITTEE ON ENERGY & NATURAL RESOURCES

SELECT COMMITTEE ON INTELLIGENCE

JOINT COMMITTEE ON TAXATION

March 13, 2019

Michel Combes
Chief Executive Officer and President
Sprint Corp.
6200 Sprint Parkway
Overland Park, KS 66251

John Legere
Chief Executive Officer
T-Mobile US, Inc.
12920 Southeast 38th Street
Bellevue, WA 98006

Randall L. Stephenson
Chairman and Chief Executive Officer
AT&T Inc.
208 South Akard Street
Dallas, TX 75202

Hans Vestberg
Chief Executive Officer
Verizon Communications Inc.
1095 Avenue of the Americas
New York, NY 10036

Dear Mr. Combes, Mr. Legere, Mr. Stephenson, and Mr. Vestberg:

I write to seek additional information regarding your companies' repeated sale and improper disclosure of customer location data to bail bondsmen, data brokers, and other individuals.

It is now abundantly clear that you have failed to be good stewards of your customers' private location information. In May of 2018, I revealed that Securus, a major provider of prison phone service, created a self-service website through which prison guards could covertly track any phone in America, using location data that Securus purchased from one of your data broker partners. Subsequent reporting by Motherboard revealed numerous examples of shady individuals obtaining your customers' location data.

In letters that your companies sent me on February 15, 2019, you collectively revealed four new incidents, separate from the Securus incident that you had previously acknowledged, in which third parties improperly obtained your customers' location information. While these incidents all involved data brokers, it seems that this is not the only method by which unauthorized individuals have tracked your customers. A March 6, 2019, Motherboard story revealed that stalkers and debt collectors have also obtained location information directly from your companies—by impersonating the police and claiming they needed the information as part of an emergency.

As you know, wireless carriers are required under federal law to protect Customer Proprietary Network Information (CPNI), which includes location data. You are also required to report breaches of CPNI to federal law enforcement agencies. Given your companies' atrocious track record protecting location data, Americans have good reason to doubt your compliance with your

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

[HTTP://WYDEN.SENATE.GOV](http://wyden.senate.gov)

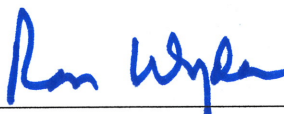
PRINTED ON RECYCLED PAPER

legal obligation to report such data breaches. To that end, please provide me with complete answers to the following questions by April 5, 2019:

1. Please list and describe all incidents since January 1, 2010 (previously disclosed, or newly discovered) in which a third party with whom your company shared location data misrepresented that it had customer consent, impersonated law enforcement, or otherwise fraudulently obtained location data.
2. For each incident in (1), did your company properly report this breach to the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) through the FCC's Data Breach Reporting Portal (<https://www.cpnireporting.gov>) as required by law?
 - a. For each incident in (1) that your company reported to the USSS and FBI through the FCC's Data Breach Reporting Portal, please provide me with a copy of the report submitted to these law enforcement agencies.
 - b. For each incident in (1) that was not reported to the USSS and FBI through the FCC's Data Breach Reporting Portal, please explain why your lawyers did not believe that it was necessary to report the breach to law enforcement.

If you have any questions about this request, please contact Chris Soghoian in my office.

Sincerely,



Ron Wyden
United States Senator