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

May 8, 2018

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

Dear Mr. Stephenson:

I am writing to insist that AT&T take proactive steps to prevent the unrestricted disclosure and potential abuse of private customer data, including real-time location information, by at least one other company to the government.

I recently learned that Securus Technologies, a major provider of correctional-facility telephone services, purchases real-time location information from major wireless carriers and provides that information, via a self-service web portal, to the government for nothing more than the legal equivalent of a pinky promise. Securus confirmed to my office that its web portal enables surveillance of customers of every major U.S. wireless carrier. This practice skirts wireless carrier's legal obligation to be the sole conduit by which the government may conduct surveillance of Americans' phone records, and needlessly exposes millions of Americans to potential abuse and unchecked surveillance by the government.

Wireless carriers are prohibited from sharing certain customer information, including location data, unless the carrier either has the customer's consent or sharing is otherwise required by law. When responding to law enforcement requests, wireless carriers must take affirmative steps to verify that a request is supported by appropriate legal authority. Further, wireless providers must ensure surveillance of communications and call records using their facilities can only be conducted with the direct and specific oversight of the provider.

The fact that Securus provides this service at all suggests that AT&T does not sufficiently control access to your customers' private information. Securus informed my office that it purchases real-time location information on AT&T's customers—through a third party location aggregator that has a commercial relationship with the major wireless carriers—and routinely shares that information with its government clients. Correctional officers simply visit Securus' web portal, enter any U.S. phone number, and then upload a document purporting to be an "official document giving permission" to obtain real-time location data. Senior officials from Securus have confirmed to my office that it never checks the legitimacy of those uploaded documents to determine whether they are in fact court orders and has dismissed suggestions that it is obligated to do so.

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

Even if Securus carefully vetted each request from its law enforcement clients, it still should not be able to provide AT&T customers' private information directly to law enforcement without AT&T's active oversight and direction. The law requires that your company be the sole conduit for law enforcement surveillance of your customers' communications and call records. I have written to the Federal Communications Commission asking that it investigate AT&T's inability or unwillingness to sufficiently safeguard your customers' private information. Further, I have asked the Commission to investigate whether companies involved in the commercial disclosure of customer location data sufficiently verify that targeted individuals have actually consented to that disclosure. A copy of my letter to the Commission is enclosed.

With good reason, your customers expect AT&T to take seriously its commitment to protect customers' private data. AT&T must deliver on that expectation. As such, I ask that you take the following common-sense steps to ensure that your customers' personal information is not abused:

- Promptly undertake a comprehensive audit of each third party with which you share customers' personal information and
    - determine how the third party uses that information,
    - ensure your customers in fact consented to that disclosure and use, and
    - notify customers whose location information you disclosed without their consent.
- Immediately terminate your data-sharing relationships with all third parties that have misrepresented customer consent or abused their access to sensitive customer data.
- Provide a web portal for your customer so that, upon request, each customer can view a list of the third parties with which you share or have previously shared that customer's private information. Americans should be able to obtain this information from wireless carriers, just as they can obtain from the consumer credit agencies a list of the private parties who have accessed their credit reports.

In addition, please provide me with full responses to the following questions no later than June 15, 2018:

1. Please identify the third parties with which your company shares or has shared customer information, including location data, at any time during the past five years. For each third party with which you share information directly, please also include a list of the ultimate end users of that information, as well as all intermediaries.
2. For each of the third parties identified in response to question one, please detail the types of customer information provided to them and the number of customers whose information was shared. For each of these, please detail whether the third party provided proof of customer consent, and if so, how the third party demonstrated that they had obtained customer consent.
3. Please describe in full your process, if any, for determining that each third party identified in response to question one has obtained appropriate customer consent before your company shared that customer's information with them. Specifically, please describe what criteria and processes your company uses to review claims and evidence that a third party has obtained consent.

4. Please describe any incidents known to your company or uncovered during your responses to the above in which a third party with which your company shared customer data misrepresented that they had customer consent.

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

Sincerely,

Ron Wyden
United States Senator