

RON WYDEN
OREGON

CHAIRMAN 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 THE BUDGET
COMMITTEE ON ENERGY AND NATURAL RESOURCES
SELECT COMMITTEE ON INTELLIGENCE
JOINT COMMITTEE ON TAXATION

May 21, 2025

Dear Colleague:

Our Senate communications face serious cyber and surveillance risks, directly threatening the Senate's independence and the separation of powers. An investigation by my staff revealed that until recently, Senators have been kept in the dark about executive branch surveillance of Senate phones, because the three major phone carriers — AT&T, Verizon, and T-Mobile — failed to establish systems to notify offices about surveillance requests, as required by their Senate contracts. While now rectified for Senate-funded lines, significant gaps remain, especially for the campaign and personal phones used by most Senators. I urge your support for legislative changes to allow the Sergeant at Arms (SAA) to protect Senators' phones and accounts from cyber threats, both foreign and domestic. I also urge you to consider switching your campaign and personal phone lines to other carriers that will provide notice of government surveillance.

Two troubling incidents last year exposed just how vulnerable the Senate's communications are. First, in the Salt Typhoon hacks China reportedly intercepted the communications of specific Senators and senior staff. Second, the Department of Justice's Inspector General revealed that the DOJ, as part of a leak investigation, collected phone records of Senate staff — including national security advisors to leadership, and staff from the Intelligence and Judiciary Committees. Democrats and Republicans were targeted in equal numbers. Together, these incidents highlight the vulnerability of Senate communications to foreign adversaries, but also to surveillance by federal, state and local law enforcement.

Executive branch surveillance poses a significant threat to the Senate's independence and the foundational principle of separation of powers. If law enforcement officials, whether at the federal, state, or even local level, can secretly obtain Senators' location data or call histories, our ability to perform our constitutional duties is severely threatened. This kind of unchecked surveillance can chill critical oversight activities, undermine confidential communications essential for legislative deliberations, and ultimately erode the legislative branch's co-equal status. Recognizing such dangers, Congress enacted protections in 2020 for Senate data held by third parties, after which the SAA updated its contracts with the major wireless carriers to require these companies to inform the Senate when its records are demanded. However, my staff discovered that, alarmingly, these crucial notifications were not happening, likely in violation of the carriers' contracts with the SAA, leaving the Senate vulnerable to surveillance. One carrier

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

[HTTPS://WYDEN.SENATE.GOV](https://wyden.senate.gov)

PRINTED ON RECYCLED PAPER

confirmed that it turned over Senate data to law enforcement without notifying the Senate, even after its SAA contract was updated to require notice. As a result of the oversight investigation conducted by my staff, AT&T, Verizon and T-Mobile have indicated that they are all now providing such notice.

Even with this recent positive change in policy by the carriers, Senators still remain in the dark about executive branch surveillance of their phone records, including location data. This is because it is common for Senators to use campaign phones, rather than Senate-issued phones, for all kinds of communications — including official business. This widespread practice is allowed by the Ethics and Rules Committees under Interpretive Ruling 444. But since these phones are paid for by our campaigns, they are not subject to the contractual notice of surveillance for Senate-issued phones.

In addition, because the SAA is currently barred from providing cybersecurity help for Senators' campaign and personal phones and online accounts, these devices and accounts remain incredibly juicy targets for foreign hacks and espionage. The Appropriations Committee has stated clearly that it "recognizes the threat of hacking and cyberattacks on Senators and staff on their official and personal devices and accounts." Meanwhile, Congress has already acted to protect the personal devices of employees at the Intelligence Community, State Department, and Department of Defense.

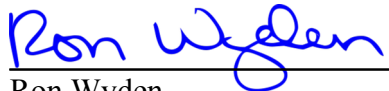
Given these serious risks, I believe the Senate must act. First, I urge you to support common sense changes I have proposed via the annual legislative branch appropriations bill that would allow the SAA to protect Senators' phones and accounts — whether official, campaign, or personal — against cyber threats, just as we have for Executive Branch employees.

Second, Senators and staff should seriously consider switching mobile carriers for their campaign and personal phones to carriers that will provide them with notice of government demands. While AT&T and Verizon only provide notice of surveillance of phone lines paid for by the Senate, T-Mobile has informed my staff that it will provide notice for Senators' campaign or personal lines flagged as such by the SAA. Three other carriers — Google Fi Wireless, U.S. Mobile, and Cape — have policies of notifying all customers about government demands whenever they are allowed to do so. The latter two companies adopted these policies after outreach from my office.

Finally, I urge you all to request from the Government Accountability Office the most recent annual non-public report on cyber and surveillance threats to the Senate. While this report is not routinely distributed to all Senators, the report contains important information that every Senator should be aware of, and GAO has informed my staff that it will provide the report to any Senator upon request.

The security of our communications isn't a luxury — it's essential for protecting our ability to do our jobs, defend the Constitution, and serve the American people. The risks we face are serious, but with focus and action, we can fix them. I look forward to working with all of you to make sure the Senate rises to meet this challenge. If you have any questions about this letter, please contact Chris Soghoian in my office.

Sincerely,

A handwritten signature in blue ink that reads "Ron Wyden". The signature is fluid and cursive, with the first name "Ron" and last name "Wyden" clearly distinguishable. It is positioned above a horizontal line.

Ron Wyden
United States Senator