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

February 29, 2024

The Honorable Joseph R. Biden, Jr.
President
The White House
1600 Pennsylvania Avenue, N.W.
Washington, D.C. 20500

Dear President Biden:

I write to request that you address the grave threats posed by wireless carriers' lax cybersecurity practices, which are not regulated, but should be. Surveillance companies and their authoritarian foreign government customers have exploited lax security in U.S. and foreign phone networks for at least a decade to track phones anywhere in the world. Authoritarian governments have abused these tools to track Americans in the United States and journalists and dissidents abroad, threatening U.S. national security, freedom of the press, and international human rights.

Surveillance technology companies sell access to phone company hacking services, through which their foreign government customers can enter any phone number and track the device associated with it, wherever it is in the world. In contrast to spyware-based surveillance, these services do not interact with the target's phone. Instead, they trick wireless carriers' servers into revealing the information. As a result, these services cannot be detected or prevented by Google and Apple — which make the most popular Android and iOS mobile operating systems — nor by third party security tools installed on a phone. Whether or not a given person can be surveilled using such services depends entirely on the security of their wireless carrier.

These phone company hacking services exploit flaws in two obscure technologies, known as Diameter and Signaling System 7 (SS7). These two technologies are used by wireless carriers around the world to deliver text messages between phone companies, and for roaming by their customers traveling abroad. For the last decade, cybersecurity researchers and investigative journalists have highlighted how wireless carriers' failure to secure their networks against rogue SS7 and Diameter requests for customer data has been exploited by authoritarian governments to conduct surveillance.

There is a simple reason for the wireless industry's failure to protect subscribers, including federal agencies: the U.S. government has failed to set minimum cybersecurity standards for wireless carriers like AT&T, T-Mobile, and Verizon. The FCC, Cybersecurity and Infrastructure

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

Security Agency (CISA), and National Security Agency (NSA) have all acknowledged the serious threat of SS7 surveillance and of the importance of securing America's communications networks. Yet no official or agency has taken responsibility for this problem, and consequently, very little has been done. In addition to not taking responsibility for this problem, CISA is actively hiding information about it from the American people. The agency commissioned an independent expert report on this topic in 2022 which it permitted my staff to read at CISA's office in the fall of 2023. CISA refuses to publicly release this unclassified report, which includes details that are relevant to policymakers and Americans who care about the security of their phones.

Effectively addressing this threat will require a whole-of-government effort, and diplomatic partnership with our allies. To that end, I urge you to direct the National Cyber Director to coordinate action among agencies and provide Congress with updates at least twice a year until this threat is meaningfully addressed. I also urge you to direct agencies to take the following specific actions to address this threat:

First, to protect U.S. government employees from surveillance by foreign governments, the Office of Management and Budget (OMB), in consultation with CISA and NSA, should establish minimum cybersecurity standards for wireless services purchased by federal agencies.

Second, to protect the American public from such surveillance, the FCC should exercise its authority to establish minimum cybersecurity requirements for U.S. wireless carriers and aggregators that deliver SS7 and Diameter messages to and from carriers. The FCC should also require companies buying access to SS7 and Diameter by leasing Global Titles to comply with registration and know your customer requirements.

The administration should verify the wireless carriers' efforts to comply with the OMB and FCC cybersecurity standards, on an annual basis, through red team independent assessments. Moreover, OMB and the FCC should look to the United Kingdom's (UK) Telecommunications Security Code of Practice as a model. That 149-page document specifies in significant detail the steps the UK government requires wireless carriers to take to secure their networks from phone company hacking services and other cyber threats.

Third, to prevent the abuse by foreign governments of phone company hacking services offered by American companies, such as Florida-based Titan-Geo and California-based SS8, the Department of Commerce's Bureau of Industry and Security (BIS) should expand U.S. export rules to cover phone company hacking services. BIS informed my office by email on January 10, 2022, that while exports of some surveillance software and hardware are restricted and require a license from the U.S. government, software that is remotely controlled through a web browser is not.

Fourth, to ensure that U.S. government agencies are not giving taxpayer money to surveillance mercenary companies that have enabled human rights abuses, you should expand the scope of

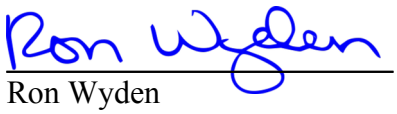
Executive Order 14093 so that the same restrictions that you created for spyware companies also apply to firms that sell phone company hacking services.

Fifth, to ensure that foreign surveillance companies are not able to benefit from the U.S. financial system, including investments from the U.S, the Departments of Treasury and State should impose Global Magnitsky sanctions. Specifically the government should sanction the major players in this industry, including Circles, Cognyte, the Rayzone Group and Defentek. The government should also investigate for potential sanctions FlowLive and Inno Networks, two foreign telecommunications companies that press reports have alleged are fronts for surveillance companies.

Sixth, to encourage allied countries to take similar steps to regulate the sale of phone company hacking services, BIS and the Departments of State and Defense should support efforts at the Wassenaar Arrangement — a multi-country forum for collaboration on export controls — to regulate phone company hacking services. On January 15, 2024, the Swiss government informed my office that it submitted a proposal along these lines, in response to reporting in May 2023 from an international consortium of news organizations into a Swiss company enabling such surveillance, which the press linked to the murder of a journalist in Mexico. I also request that you provide me with a copy of the Swiss proposal.

Thank you for your attention to this important matter. If you have any questions about this request, please contact Chris Soghoian in my office.

Sincerely,



Ron Wyden
United States Senator

CC: The Honorable Antony Blinken, Secretary, Department of State
The Honorable Gina Raimondo, Secretary, Department of Commerce
The Honorable Janet Yellen, Secretary, Department of Treasury
The Honorable Lloyd J. Austin III, Secretary, Department of Defense
The Honorable Jessica Rosenworcel, Chairwoman, Federal Communications Commission
The Honorable Jen Easterly, Director, Cybersecurity and Infrastructure Security Agency
The Honorable Timothy D. Haugh, Director, National Security Agency
The Honorable Harry Coker, Jr., National Cyber Director
Mr. Jake Sullivan, Assistant to the President for National Security Affairs
Ms. Clare Martorana, Federal Chief Information Officer, Office of Management and Budget