

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

October 25, 2022

The Honorable Lina Khan
Chair
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

The Honorable Avril Haines
Director
Office of the Director of National Intelligence
Washington DC, 20511

Dear Chair Khan and Director Haines:

I write with serious concern that the Federal Trade Commission (FTC) — the nation's top data security regulator — is not meaningfully participating in the intelligence community-led effort to counter the wholesale theft of Americans' data by foreign governments, including China.

As senior U.S. government officials have made clear, over the past decade, the Chinese government has been engaged in a methodical effort to acquire through both legal and illegal means large databases containing Americans' personal information. This includes the hacks of Anthem, Equifax, Marriott, and the Office of Personnel Management. While each of the databases stolen in these hacks contains vast amounts of sensitive data, when combined, they could reveal even more information about Americans and their personal lives. This enriched data could be used to target disinformation, identify targets for espionage and hacking campaigns, and, according to one former Attorney General, identify undercover U.S. personnel.

While state-sponsored hackers are often skilled, patient, and resourceful, these hackers are not omnipotent. The companies and government agencies who have been hacked are not faultless, and often, deserve significant amounts of blame for the lax state of their cybersecurity which the hackers were able to exploit. These organizations have a responsibility to protect the sensitive data to which they have been entrusted, and far too often, have wholly failed.

As the primary federal data security and privacy regulator, the FTC has the authority and responsibility to hold accountable companies whose negligent cybersecurity has resulted in the theft of their customers' personal data. However, I am concerned that the FTC is not meaningfully working with the intelligence community to counter these foreign hacking efforts. That is, while the intelligence community has the greatest visibility into foreign governments' U.S.-focused hacking and data theft efforts, including likely future targets, the intelligence community is sharing very little information with the FTC to inform its data security investigations.

Specifically, the FTC recently informed my office in a September 26, 2022, email that only four FTC staff currently have a Top Secret/Sensitive Compartmented Information (TS/SCI)

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)

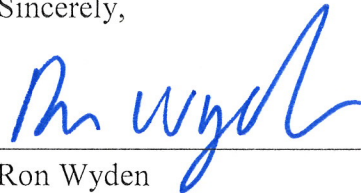
PRINTED ON RECYCLED PAPER

clearance. TS/SCI clearances are necessary to be eligible to access information derived from the government's most sensitive sources and methods. The FTC also confirmed that its Chair and the other Commissioners only have a TS clearance, and not TS/SCI. Most troublingly, the FTC confirmed to my office that no staff in the agency's Division of Privacy and Identity Protection, who conduct investigations into data security and privacy cases, have even a Secret clearance, which is effectively the lowest level federal clearance. The FTC also confirmed to my office that while it has participated in interagency discussions that included the Office of the Director of National Intelligence (DNI) and other national security stakeholders, such as the Federal Bureau of Investigation and Department of Homeland Security, these conversations have been at a general level and did not involve the exchange of classified information.

The U.S. government cannot protect Americans' privacy and U.S. national security from the serious threat posed by sophisticated foreign hackers if the FTC does not have a seat at the table. The FTC should promptly request TS/SCI clearances for its Chair and the other Commissioners, other senior leadership, and some of the staff in the FTC's Division of Privacy and Identity Protection. The DNI should expand its cooperation with the FTC and invite FTC staff to classified briefings. The DNI should also identify for the FTC the kinds of datasets that are being or are likely to be targeted by foreign hackers. With this information, the FTC could then identify the companies that hold such data, scrutinize their security and, if it is found lacking, force the firms to shore up their security before they are hacked.

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 Shalanda Young, Director, Office of Management and Budget