

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

July 28, 2025

The Honorable Tulsi Gabbard
Director of National Intelligence
Office of the Director of National Intelligence
Washington, D.C. 20511

Dear Director Gabbard:

I write to request that you conduct and make public an assessment of the national security threat posed by the United Kingdom (U.K.)'s surveillance laws and its reported secret surveillance demands of U.S. companies.

Earlier this year, after press stories reported that the U.K.'s Home Secretary issued a secret order forcing Apple to undermine the security of its iCloud backup service, Congressman Andy Biggs and I wrote a bipartisan letter to you about the matter. In your February 25, 2025, response letter, you wrote that you shared our "grave concern about the serious implications of the United Kingdom, or any foreign country, requiring Apple or any company to create a 'backdoor' that would allow access to Americans personal encrypted data." You added that "this would be a clear and egregious violation of Americans' privacy and civil liberties, and open up a serious vulnerability for cyber exploitation by adversarial actors."

Unfortunately, because recipients of these orders are prohibited from disclosing them, it is not possible to confirm which U.S. technology companies have received them, much less the extent to which they may be complying with them. When my office sought to confirm the press reports, Apple stated that if it had received a technical capabilities notice, it would be barred by U.K. law from telling Congress whether or not it received such a notice. But Apple is not the only major U.S. technology that uses end-to-end encryption to protect sensitive customer data from hackers.

Apple's end-to-end encrypted backup feature that is reportedly the subject of the U.K.'s backdoor demand, Advanced Protection Mode, is disabled by default. Since most users don't change the default settings, it is likely that only a very small percentage of Apple's customers are benefiting from this important cybersecurity defense. In contrast, Google also protects Android smartphone backups with end-to-end encryption, and Google has enabled this cybersecurity defense by default, protecting billions of people using Android phones. When my office asked Google about backdoor demands from the U.K., the company did not answer the question, only stating that if it had received a technical capabilities notice, it would be prohibited from disclosing that fact.

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

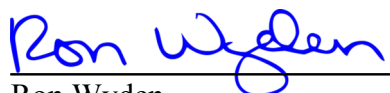
Meta uses end-to-end encryption to protect texts and calls made with WhatsApp and Facebook Messenger by default. The company offers end-to-end encryption to protect Instagram direct messages, but not by default. Meta also offers an end-to-end encryption feature to protect WhatsApp backups, which is not enabled by default. When my office asked Meta about backdoor demands from the U.K., Meta offered an unequivocal denial on March 17, 2025, stating that “we have not received an order to backdoor our encrypted services, like that reported about Apple.”

I am concerned that the threat posed by the U.K.’s surveillance laws is not limited to demanding that U.S. companies weaken their encryption with backdoors. I am concerned that under the Investigatory Powers Act 2016 (IPA), the U.K. could also secretly force U.S. companies to store the data of U.S. users in the U.K., where it could then be seized by the U.K. government. My office has repeatedly asked the U.K. Embassy to clarify the scope of its controversial surveillance law, and sought assurances that it could not be used to collect Americans’ communications. While the U.K. Embassy has clarified that the IPA cannot be used to force U.S. companies to make a U.K.-based copy of existing data held in the U.S., the U.K. Embassy has not denied the concerns raised by my office that the IPA could be used to force U.S. companies to store newly created U.S. customer data in the U.K., instead of in the U.S. as the companies would normally do. Such U.K.-located data could then be seized by the U.K. government. In addition, despite multiple requests from my office, the U.K. Embassy has been unable to provide any assurances that the U.K. cannot use the Equipment Interference provisions under the IPA, which permits the U.K. to demand companies infect their customers with spyware, to hack Americans.

The cybersecurity of Americans’ communications and digital lives must be defended against foreign threats. As you noted in your letter to me, the reported U.K. order, which could have the effect of weakening the encryption that protects millions of Americans’ private communications, creates vulnerabilities that can be exploited by our adversaries. This scenario is even more concerning given the possibility that the IPA could be used to force U.S. companies to store data in the U.K. The national security implications are serious, not least because the communications of U.S. government officials could be subjected to both weakened encryption and storage in the U.K. Accordingly, I urge you to provide Congress and the American public with a frank assessment of the national security risks posed by the U.K.’s surveillance laws and its reported secret demands of U.S. companies.

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