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

July 16, 2026

The Honorable Marco Rubio
Acting Assistant to the President for National Security Affairs
The White House
1600 Pennsylvania Avenue, NW
Washington, DC 20500

The Honorable Todd Blanche
Acting Attorney General
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530

Dear Secretary Rubio and Acting Attorney General Blanche:

I write to urge you to protect U.S. national security and the communications of American citizens—including U.S. government officials—from the serious counterintelligence threat posed by Canada's proposed spying law, Bill C-22. This proposed Canadian legislation threatens to weaponize American technology infrastructure by enabling the Canadian government to force U.S. companies to secretly facilitate surveillance of Americans, while systematically undermining the security of their products.

Canada is not the first foreign government to go down this path. In February 2025, the press revealed that Apple received a secret demand from the United Kingdom (U.K.) to weaken the security of encrypted iCloud backups in order to facilitate surveillance demands. Then-Director of National Intelligence Tulsi Gabbard confirmed in a letter to Congress that foreign mandates requiring U.S. firms to engineer surveillance backdoors violate privacy rights and create severe vulnerabilities for cyber exploitation by hostile actors. These concerns were echoed by President Trump and Vice President Vance, who ultimately encouraged the U.K. government to scale back its demands of Apple.

These foreign surveillance laws pose a particularly serious national security threat, because U.S. law does not explicitly prohibit American companies from secretly facilitating foreign surveillance of U.S. citizens—even if the target is the President or another senior U.S. government official. As such, this is not a dilemma of U.S. companies being caught between conflicting international legal obligations; it is a glaring statutory vacuum.

Under the CLOUD Act, foreign countries that enter into an agreement with the DOJ can seek data directly from U.S. companies, except where the surveillance target is known to be an American. Only two countries to date have CLOUD Act agreements: the U.K. and Australia. Other countries seeking communications content from U.S. companies must instead request assistance from the DOJ, which can take months, or even

years. Canada is presently negotiating an initial CLOUD Act agreement with the DOJ, giving the U.S. government significant leverage to extract binding commitments against surveillance targeting Americans. Currently, U.S. law provides no shield to stop American companies from complying with secret demands from foreign governments that target U.S. persons or federal personnel. After the press revealed the existence of the UK's surveillance demand to Apple in February 2025, my staff engaged with the U.K. government and leading U.K. surveillance law experts to evaluate the real-world boundaries of these sweeping foreign powers and the CLOUD Act agreements. Alarmingly, the U.K. government could not offer any assurances that their laws or their CLOUD Act agreement with the DOJ prevented specific surveillance demands designed to facilitate espionage against the United States. These high-risk scenarios involve foreign governments enforcing local data-storage mandates specifically so local authorities can physically enter U.S. companies' foreign data centers and seize data of Americans. They include:

1. Mandating Local Backups: Requiring that new data backups for American targets that have not enabled end-to-end encryption be stored in the foreign jurisdiction.
2. Disabling End-to-End Encryption for Target Backups: Forcibly disabling end-to-end encryption for specific American targets and requiring new unencrypted data be stored on the company's local servers.
3. Implementing a "Ghost Key": Requiring that new encrypted data backups for American targets be stored in the foreign jurisdiction but rendered accessible via a hidden, government-controlled "ghost" decryption key.
4. Relocating and Demanding Software Signing Keys: Requiring that the company store in the foreign jurisdiction a copy of the encryption keys used to sign software updates for the devices of American targets—keys that are ordinarily secured within the U.S.—rendering them vulnerable to foreign government seizure.
5. Delivering Spyware via Software Updates: Forcing trusted American firms to assist in the delivery of foreign-government spyware to American targets via compromised software updates.

The U.S. government cannot allow foreign governments to coerce U.S. companies into conducting surveillance against Americans, least of all our own intelligence, military, and diplomatic personnel. The U.S. government must ensure that U.S. companies cannot be secretly ordered to facilitate surveillance of Americans, encompassing both traditional demands for stored data under the CLOUD Act and the technical engineering mandates described above. Accordingly, I urge you to take the following actions to protect U.S. national security:

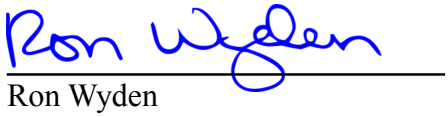
- Evaluate Bill C-22: Determine whether Canada's proposed spying law will permit the Canadian government to demand surveillance assistance from U.S. companies like Apple and Google targeting Americans, including the previously listed scenarios.
- Leverage CLOUD Act Negotiations: Utilize the ongoing U.S.-Canada CLOUD Act agreement negotiations to establish ironclad, explicit prohibitions against these extraterritorial technical and prospective engineering mandates.

- Defend U.S. Government Infrastructure: Take all necessary administrative and regulatory steps to insulate U.S. government officials and the American public from foreign surveillance demands against American firms.

Bilateral trust with our closest intelligence partners cannot be built on the secret subversion of American cybersecurity infrastructure. We must ensure that Canada's domestic legislation does not create a back door into the devices of American officials.

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