Congress of the United States
Washington, DC 20515

May 7, 2026

The Honourable Gary Anandasangaree, P.C., M.P.
Minister of Public Safety
Public Safety Canada
269 Laurier Avenue West
Ottawa, ON K1A 0P8
Canada

Dear Minister Anandasangaree:

The Committee on the Judiciary and the Committee on Foreign Affairs of the United States House of Representatives (the "Committees") are conducting oversight of actions by foreign governments that threaten to weaken the security, privacy, and constitutional rights of American citizens. Canada's Bill C-22, currently under consideration in Parliament, would drastically expand Canada's surveillance and data access powers in ways that create significant cross-border risks to the security and data privacy of Americans.[1] We write to express our concerns that, if enacted, Bill C-22 would allow Canadian government officials to compel American companies to build backdoors into their encrypted systems, thereby introducing systemic vulnerabilities that could be exploited by hackers, foreign adversaries, and cybercriminals. This concern is heightened in light of ongoing discussions concerning U.S.-Canada data access frameworks contemplated under the U.S. Clarifying Lawful Overseas Use of Data (CLOUD) Act of 2018.[2]

Bill C-22 would impose broad obligations on electronic service providers to develop, implement, assess, test, and maintain operational and technical capabilities for authorized persons to access encrypted data and information.[3] While the bill states that providers need not comply if doing so would introduce a "systemic vulnerability," the term is vague and ultimately subject to a future regulatory process.[4] Furthermore, the legislation empowers you, as the Minister of Public Safety, to issue secret "ministerial orders," subject only to the Intelligence Commissioner's review and kept confidential, that allow you to issue targeted demands to individual providers.[5] In practice, providers offering end-to-end encryption services will inevitably face directives to create backdoors and architectural changes that bypass or weaken encryption to enable "lawful" interception or data extraction.

---

[1] Bill C-22: An Act respecting lawful access (Lawful Access Act, 2026), 1st Sess. 45th Parl., 2026 (first reading Mar. 12, 2026).
[2] Pub. L. No. 115-141 (2018) (codified in part at 18 U.S.C. § 2523); *See* Press Release, U.S. Dep't of Justice, United States and Canada Welcome Negotiations of a CLOUD Act Agreement (Mar. 22, 2022), https://www.justice.gov/archives/opa/pr/united-states-and-canada-welcome-negotiations-cloud-act-agreement.
[3] Bill C-22, cl. 5(2) (core providers).
[4] *Id.* at cl. 5(5) (systemic vulnerability).
[5] *Id.* at cl. 7(1) (ministerial orders).

We have already seen the consequences of similar laws in other countries. The government of the United Kingdom of Great Britain and Northern Ireland ("UK") reportedly issued a secret order to Apple Inc., an American corporation, compelling the company to provide access to users' encrypted cloud data.[6] According to a February 2025 article in the *Washington Post*, the UK Home Office, under the authority of the Investigatory Powers Act of 2016, issued a Technical Capability Notice (TCN) demanding the capability to access end-to-end encrypted data stored in Apple's iCloud, including content uploaded by users worldwide.[7] This order reportedly targeted Apple's Advanced Data Protection (ADP) feature, which provides optional end-to-end encryption for iCloud backups and ensures that even Apple cannot access its users' private data.[8] In response to the secret order, Apple reportedly disabled ADP for UK users in February 2025, effectively weakening encryption protections for approximately 35 million iPhone users in the UK.[9]

If a U.S. based provider is forced to redesign its system to facilitate Canadian authorized access to content that is currently inaccessible even to the provider itself, the resulting capability cannot be geographically limited. This directly threatens the privacy of U.S. persons who expect and depend upon robust encryption to protect sensitive communications, health data, financial records, and personal correspondence from unwarranted intrusion. A backdoor built to satisfy one government's demands inevitably becomes a target for adversaries, as demonstrated by the 2024 Salt Typhoon intrusion into U.S. Communications Assistance for Law Enforcement Act-compliant wiretap infrastructure.[10] The Salt Typhoon intrusion shows that once such access points exist, they do not remain exclusive to lawful authorities—they become persistent, high value targets for our foreign adversaries.[11]

Bill C-22 sets a dangerous precedent that could erode the mutual benefits of strong encryption standards. American companies operating in Canada would face a difficult choice: compromising the security of their entire user base—including U.S. citizens—or risking exclusion from the Canadian market. Either outcome harms U.S. national security and economic interests by undermining trust in American technology and inviting reciprocal demands from other nations. Over time, these pressures will fracture global cybersecurity norms and weaken our collective defenses against malicious actors who exploit inconsistent standards.

---

[6] Joseph Menn, *U.K. orders Apple to let it spy on users' encrypted accounts*, WASH. POST (Feb. 7, 2025).
[7] *Id.*
[8] *Id.*
[9] Press Release, Apple can no longer offer Advanced Data Protection in the United Kingdom to new users, Apple (Feb. 24, 2025).
[10] Cybersecurity & Infrastructure Security Agency, AA25-239A: *Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System (Salt Typhoon)* (2025), https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-239a ("Salt Typhoon," a People's Republic of China-linked cyberespionage campaign that targeted major U.S. telecommunications infrastructure) (CALEA, a federal law that requires U.S. telecommunications carriers to design systems to facilitate court-authorized electronic surveillance); *See also* Sarah Krouse, et al., *China-Linked Hackers Breach U.S. Internet Providers in New 'Salt Typhoon' Cyberattack*, WALL ST. J. (Sep. 26, 2024).
[11] *Id.*

The United States and Canada maintain a close partnership in matters of security, intelligence cooperation, and cross-border law enforcement. At present, however, we do not have an executive agreement under the CLOUD Act. We look forward to your prompt collaboration on this issue, with the goal of safeguarding the privacy and civil liberties of our citizens. The Committee on the Judiciary has jurisdiction over federal law enforcement and civil liberties pursuant to Rule X of the Rules of the House of Representatives.[12] The Committee on Foreign Affairs has jurisdiction over relations of the United States with foreign nations generally, as well as measures to foster commercial intercourse with foreign nations and to safeguard American business interests abroad pursuant to Rule X of the Rules of the House of Representatives.[13]

Thank you for your attention to this important matter.

Sincerely,

Jim Jordan
Chairman
Committee on the Judiciary

Brian Mast
Chairman
Committee on Foreign Affairs

cc: The Honorable Jamie Raskin, Ranking Member, Committee on the Judiciary

The Honorable Gregory Meeks, Ranking Member, Committee on Foreign Affairs

[12] Rules of the House of Representatives, R. X, 119th Cong. (2025).
[13] *Id*.