ACT Association for Competitive Technology

June 3, 2026

Standing Committee on Public Safety and National Security (SECU)
Sixth Floor, 131 Queen Street
House of Commons
Ottawa ON K1A 0A6
Canada

RE: Bill C-22, *An Act respecting lawful access*

Dear Chair Duclos and Members of the Standing Committee on Public Safety and National Security,

On behalf of the Association for Competitive Technology (ACT), I am writing to respectfully share concerns regarding Bill C-22, An Act respecting lawful access.[1]

ACT represents small business innovators and startups in the software development and high-tech space located in Canada and around the world.[2] As the world embraces mobile technologies, our members create the innovative products and services that drive the global digital economy by improving workplace productivity, accelerating academic achievement, and helping people lead more efficient and healthier lives. Today, the domestic app economy is worth more than $6.1 trillion.[3]

We appreciate Minister Anandasangaree's May 27, 2026, public commitment that the government will propose amendments to clarify that Bill C-22 does not undermine encryption. However, as currently drafted, Bill C-22 would impose sweeping technical obligations on electronic service providers that would undermine the encryption protections Canadians rely on every day to secure their personal, health, and financial information. While we share your goal of keeping Canadians safe, we are concerned that the bill, as written, could ultimately weaken critical privacy and cybersecurity safeguards and impose substantial compliance and operational burdens on small businesses. We urge the Committee to amend the bill to include explicit protections for strong end-to-end encryption and ensure Canada's small businesses and developers can take advantage of effective safeguards to protect their customers.

Encryption safeguards sensitive personal information from unauthorized access and misuse. In practice, consumers depend on it every time they send a message, make a payment, or use a health or financial app. For developers, the protections end-to-end

[1] "Bill C-22." *SECU - Bill C-22, An Act Respecting Lawful Access*, www.ourcommons.ca/Committees/en/SECU/StudyActivity?studyActivityId=13454852. Accessed 28 May 2026.
[2] ACT | The App Association, *About*, *available at* http://actonline.org/about.
[3] ACT | The App Association, *State of the U.S. App Economy: 2023*, https://actonline.org/wp-content/uploads/APP-Economy-Report-FINAL-1.pdf.

encryption provides are equally foundational and enable them to build secure, trustworthy products, protect their customers, and compete in global markets where consumers expect strong privacy and security protections.

Part 2 of Bill C-22, the Supporting Authorized Access to Information Act, would empower the Governor in Council to require core providers to develop and maintain the operational and technical capabilities necessary to obtain private information, as well as install and maintain devices and equipment that allow authorized persons to access such information. Together, these requirements effectively mandate the installation of a backdoor into encrypted systems. The bill also empowers the Minister of Public Safety and Emergency Preparedness to issue orders imposing equivalent obligations on any electronic service provider, significantly expanding the bill's reach in practice. While the bill does include an exception where providers do not have to comply if doing so would introduce a systemic vulnerability into the system, the definition of systemic vulnerability depends on whether the vulnerability would create a substantial risk. The vagueness of this phrase leaves significant room for interpretation and likely will not mitigate actual or perceived obligations to weaken encryption.

As cybersecurity experts have long recognized, requirements that mandate exceptional access or otherwise require providers to bypass or weaken encrypted systems create vulnerabilities that malicious actors can and will exploit. In late 2024, Salt Typhoon, a hacking group affiliated with the Chinese government, infiltrated U.S. telecommunications networks through lawful access infrastructure.[4] During the cyberattack, hackers exploited the vulnerabilities that had been installed to facilitate law enforcement investigations and accessed U.S. policymakers' private data and communications.[5] Incidents such as the Salt Typhoon attack illustrate how any mechanism designed to provide access for one purpose, such as lawful surveillance, will become a target for adversaries and offer bad actors an opportunity to access and misuse consumers' data. As testimony before the Committee has already established, any capability that permits exceptional access to end-to-end encrypted communications is itself a systemic vulnerability, regardless of how narrowly the access process is defined.

ACT also notes that strong encryption is also a foundational technical safeguard underpinning the "appropriate security safeguards" that the Personal Information Protection and Electronic Documents Act (PIPEDA) requires organizations to maintain over personal information. Bill C-22 would erode that safeguard in direct tension with existing privacy obligations under Canadian law.

Finally, ACT believes that the cross-border implications of Bill C-22 also warrant the Committee's attention. Most digital services used by Canadians—and upon which Canadian small business developers build—are offered by providers that serve

[4] Krouse, Sarah, et al. "China-Linked Hackers Breach U.S. Internet Providers in New 'Salt Typhoon' Cyberattack." *The Wall Street Journal*, The Wall Street Journal, 26 Sept. 2024, www.wsj.com/politics/national-security/china-cyberattack-internet-providers-260bd835.

[5] Nakashima, Ellen, and Josh Dawsey. "Chinese Hackers Collected Audio of Calls by U.S. Political Officials - The Washington Post." *The Washington Post*, The Washington Post, 27 Oct. 2024, www.washingtonpost.com/national-security/2024/10/27/chinese-hackers-cellphones-trump/.

customers in the United States and globally. A Canadian mandate that weakens encryption undermines the contemplated U.S.–Canada executive agreement under the U.S. Clarifying Lawful Overseas Use of Data (CLOUD) Act, which is based on the expectation that participating partners maintain robust privacy and cybersecurity protections.

Practically, vague or overly broad lawful access mandates create significant uncertainty that forces small businesses and app developers to delay or abandon new projects, or to lose access to the cutting-edge security tools they have integrated into their own products and services. As opposed to their larger counterparts, small businesses don't have large legal and compliance teams. Interpreting complex, evolving compliance obligations requires diverting limited resources away from hiring, growth, and innovation. Faced with this uncertainty, many small businesses may choose to pull out of the Canadian market entirely, limit the services they offer to Canadian users, or avoid building products that involve the collection or transmission of personal information. The result would be a Canadian market with fewer choices, weaker security tools, and fewer protections for consumers.

Given these ramifications, ACT respectfully urges policymakers to amend Bill C-22 to include clear, explicit protections for strong encryption. As drafted, the bill's requirements risk being interpreted or applied through regulation and ministerial orders to require providers to weaken, bypass, or compromise encryption and other core security features. The bill should be revised to:

- Expressly state that no regulation or order made under the Supporting Authorized Access to Information Act shall require an electronic service provider to introduce, retain, or refrain from removing any vulnerability, backdoor, or exceptional-access capability in any product, service, device, or system used to secure information in transit or at rest, or to weaken any form of encryption, including end-to-end encryption;
- Strengthen its definition of "systemic vulnerability" to expressly include any capability designed to provide access to end-to-end encrypted content, and move away from a subjective "substantial risk" threshold;
- Include a transparency provision permitting providers to publicly disclose the existence and aggregate use of orders issued under the Act, consistent with practices in other Five Eyes jurisdictions; and
- Narrow the definition of "subscriber information" to a closed list of discrete identifiers, as proposed by the Privacy Commissioner of Canada in his May 26, 2026, testimony.

We appreciate your consideration of the above views and welcome any opportunity to provide additional commentary as the legislative process advances.

Sincerely,

Morgan Reed
President
Association for Competitive Technology