November 19, 2026

The Honourable Marty Deacon
Chair, Standing Senate Committee on National Security, Defence and Veterans Affairs
The Senate of Canada
2 Rideau Street
Ottawa, Ontario K1A 0A4

Email: secd@sen.parl.gc.ca

Dear Senator Deacon:

Apple appreciates the opportunity to submit written comments on Bill C-22, "An Act respecting lawful access" ("Bill"), as passed by the House of Commons on June 18, 2026. As a provider of hardware, software, and services used by people across the globe, Apple has extensive experience with lawful access frameworks.

We appreciate the efforts that have been made to improve the Bill. At the same time, we remain concerned that certain provisions, as currently drafted, would weaken encryption and put Canadian individuals, businesses, and government institutions at much greater risk of harm from malicious actors.

Simply put, Bill C-22 could be used by the Government of Canada to require companies to weaken end-to-end encryption or build backdoors into their new encrypted products — something Apple will never do.

As explained below, we urge the Standing Committee on National Security, Defence and Veterans Affairs ("Committee") to adopt targeted amendments that would protect the data security and privacy of Canadians while preserving the Bill's public safety objectives.

Background

Apple shares the government's commitment to the safety and security of Canadians. At Apple, our goal has been and always will be to create technology that empowers and enriches people's lives while helping them stay safe. Apple is committed to enhancing the privacy, security, and safety of our users all around the world.

Our work to protect our users has never been more important because the pervasive threats they face in the modern digital world continue to grow in complexity and frequency – and include AI and other evolving technologies that provide hackers with new tools to exploit cybersecurity weaknesses. Canadians rely on their devices and technology services to securely store and process highly sensitive information, including their health data, the location of their family members, highly personal messages, photos, and financial information. Our users trust Apple devices and services to keep their data safe, secure, and private. And that is why we are constantly innovating and introducing new features to protect them.

Overview

One of the most effective security technologies available today is end-to-end encryption. Encryption shields everyday citizens from identity theft, fraud, unlawful surveillance, and data breaches. It also serves as an invaluable protection for journalists and human rights activists who are constantly targeted by malicious actors. Encryption also protects the data and communications of Canadian businesses, government officials, and other people and entities that use our products and services – ultimately

broadly benefiting the economic prosperity and national security of Canada. The value of encryption is a key reason for the technology community's broad consensus in support of its continued use.

It is false to suggest that exceptions can be made and that access to end-to-end encrypted data could be created just for those sworn to uphold the public good. Any process that weakens the mathematical models that protect user data for anyone will, by extension, weaken the protections for everyone. In other words, when you build a backdoor into an encrypted device, anyone can walk through it.

Unfortunately, we have seen recent examples of this. In February 2025, malicious actors targeted Canadian telecom and other networks to steal customer data, monitor communications, and conduct broad espionage.[1] Unlike typical cyberattacks seeking primarily to steal customer data, this attack "focused on controlling communications infrastructure that billions rely on every day."[2] And the attack reportedly exploited precisely the kind of government-mandated "lawful access" backdoors that Bill C-22 could effectively create.[3]

Today, Apple cooperates with law enforcement agencies, including those in Canada, by providing the data we can access responsive to lawful requests. We have a dedicated law enforcement team that works tirelessly to respond to such requests in accordance with the law, including immediate contact for emergency requests. We recognize, and share, the government's commitment to the safety and security of all Canadians.

However, Bill C-22, as passed by the House, would undermine our ability to offer users the privacy and security they expect of Apple products. Accordingly, we urge the Committee to adopt the following targeted amendments:

- **Strengthen statutory protections for encryption.** Include a clear statutory statement that no provider may be required—by statute, regulation, order, or other directive—to weaken, bypass, or undermine end-to-end encryption, including through mandates to create backdoors, decryption capabilities, or systemic access mechanisms, or to refrain from the *future* use of encryption.

- **Clarify and narrow the definition of "systemic vulnerability."** Replacing "substantial risk" with "credible risk" is an improvement, but the revised definition remains unclear and still contains a carve-out for government access. Define "systemic vulnerability" as "a vulnerability in an information system, system security procedures, internal controls, or implementation thereof that has been, or could be, exploited or triggered by any threat source, including, but not limited to, any weakness, capability, design requirement, or other modification to a network, system, device, service, process, or security architecture that uses encryption, which is the cryptographic transformation of data from plaintext into a form of ciphertext that conceals the data's original meaning to prevent it from being known or used, or similar protections."

---

[1] *Cyber threat bulletin: People's Republic of China cyber threat activity*, Government of Canada (June 19, 2025), https://www.cyber.gc.ca/en/guidance/cyber-threat-bulletin-prc-cyber-actors-target-telecommunications-companies-global-cyberespionage-campaign.

[2] Meghal Donde, *Salt Typhoon Across the Internet*, Global Cyber Alliance (Dec. 9, 2025), https://globalcyberalliance.org/new-report-salt-typhoon-across-the-internet/.

[3] Marie Woolf, *Lawful-access bill could threaten encryption, deter investment*, The Globe and Mail (May 1, 2026), https://www.theglobeandmail.com/politics/article-lawful-access-bill-could-threaten-encryption-deter-investment-chamber/.

- **Prohibit government-mandated installation or use of surveillance equipment.** Expressly prohibit the government from requiring any provider to install, operate, or maintain government-owned or government-controlled surveillance or other equipment in providers' networks, systems, or devices.

- **Narrow secrecy provisions to what is necessary and allow limited disclosures.** Limit secrecy provisions to circumstances that are necessary and proportionate to protect national security or ongoing investigations. Allow providers to consult legal counsel and technical experts, and to make protected disclosures to competent foreign authorities and to courts in Canada and foreign jurisdictions under seal.

- **Limit future regulatory expansion.** Define fundamental obligations in the statute rather than deferring them to future regulations. Establish statutory limits on the regulations the Governor in Council may make, especially those affecting cybersecurity, encryption, and service provider obligations.

- **Strengthen protections for timely and complete judicial review.** Ensure that judicial review of any government action meets due process requirements and is available to providers before compliance is required. Stay all compliance obligations pending completion of that review.

- **Clarify that providers are not required to produce data stored outside Canada.** Expressly provide that no warrant, order, directive, regulation, or other mandate may require the disclosure or production of data located outside Canada, to avoid conflicts with foreign law and inconsistent legal obligations for providers operating in multiple jurisdictions.

- **Narrow inspection powers and include other appropriate safeguards.** Remove or narrow warrantless entry provisions. Protect proprietary and confidential business information obtained through compliance with the Bill.

- **Clearly define and narrow the scope of covered providers and services.** Specify which providers, products, and services are subject to the Bill. Establish a clear definition of, and statutory limits on, the entities that may be designated as "core providers."

These recommendations are discussed in greater detail below.

Strengthen Statutory Protections for Encryption

As currently drafted, Bill C-22 could be used to require service providers to build backdoors into encrypted systems. While Apple recognizes the government's goal of protecting Canadians, this approach could undermine cybersecurity and increase the risk of exploitation by malicious actors. Undermining encryption—even for law enforcement purposes—inevitably introduces risks to individuals, businesses, and governments, and threatens both national security and the economy. As Apple has explained in its public submissions to the UK Parliament regarding proposed amendments to the Investigatory Powers Act, encryption is "critical to shielding everyday citizens from unlawful surveillance, identity theft, fraud, and data breaches."[4]

[4] *Written Evidence Submitted by Apple to the Investigatory Powers Public Bill Committee*, UK Parliament (Mar. 2024), https://publications.parliament.uk/pa/cm5804/cmpublic/investigatorypowersamendment/memo/ipab10.htm.



We appreciate the addition of section 2(4), which provides that the Bill is not to be construed as compelling a provider to decrypt information encrypted by its users, unless the provider supplied the encryption and has the information necessary to decrypt it. However, that provision addresses information that is already encrypted. It does not clearly prohibit forward-looking requirements that could weaken encryption, such as requiring providers to modify services that currently use end-to-end encryption, to restrict the future use of encryption, or to create new access capabilities. Instead, we recommend including the following:

> *Notwithstanding any other provision of this Act, a core provider, electronic service provider, or any employee, contractor, or agent thereof, shall not be required to: (a) take any action that would create or introduce any vulnerability in any network, system, device, service, or other process, or refrain from taking an action to fix an identified vulnerability; (b) refrain from the prospective use of encryption or other technology, process, or procedure that enhances data security; or (c) use or install any hardware, software, or firmware controlled or developed by the government or any third party on its behalf. Nothing in the Act is intended, or may be used, to limit or otherwise prevent the use of any type of encryption or other technology, process, or procedure that enhances data security within Canada.*

Clarify and Narrow the Definition of "Systemic Vulnerability"

We also appreciate the inclusion of a "systemic vulnerability" exception in sections 2(1), 5(5), and 7(5) of the Bill. However, the definition of "systemic vulnerability" contains overly broad and insufficiently defined terms, increasing the risk that the government could override necessary security protections in providers' networks. As drafted, the Bill defines a "systemic vulnerability" as:

> [A] vulnerability in the electronic protections of an electronic service that creates a credible risk, based on recognized international technical standards, that secure information could be accessed by a person who does not have any right or authority to do so, other than a risk that relates only to information related to persons with respect to whom a warrant, order or other authority to access information conferred under the *Criminal Code* or the *Canadian Security Intelligence Service Act* – or any similar authority conferred under another Act of Parliament – applies.

Replacing "substantial risk" with "credible risk" is an improvement, but the revised definition remains unclear. The Bill does not define the term "credible risk," nor does it specify which "recognized international technical standards" apply.

In addition, the definition's language regarding access to secure information by a person without "any right or authority to do so" is circular. The Bill excludes risks relating only to information concerning persons subject to "a warrant, order or other authority to access information" under specified federal statutes. This exception is overly broad and vague, creating significant uncertainty regarding the scope of protections against systemic vulnerabilities. It leaves open the possibility that a government actor could, through regulations or orders issued pursuant to the Bill or through authorities conferred under other federal statutes, authorize its own access to encrypted communications, thus excluding its own actions from the definition of systemic vulnerability. Efforts to clarify this provision have so far been inadequate. This uncertainty provides no assurance that the data security and privacy of Canadians will continue to be protected if the Bill is enacted without clarifying the definition of systemic vulnerability and without expressly prohibiting any governmental efforts that would undermine encryption. It is difficult to imagine that Parliament intends to allow the government to circumvent, through its own regulations or orders, the very protection against systemic vulnerabilities that the proposed Act is designed to guarantee.

Moreover, Bill C-22 allows for the definition of "systemic vulnerability" to be amended by regulation under section 47(1)(c) without parliamentary debate, which could enable future governments, for whatever reason, to narrow or otherwise alter the exception. In effect, this is a clear loophole that provides no meaningful assurance that the Bill will protect Canada's cybersecurity.

Instead, we recommend defining "systemic vulnerability" in the statute itself as "a vulnerability in an information system, system security procedures, internal controls, or implementation thereof that has been, or could be, exploited or triggered by any threat source, including, but not limited to, any weakness, capability, design requirement, or other modification to a network, system, device, service, process, or security architecture that uses encryption, which is the cryptographic transformation of data from plaintext into a form of ciphertext that conceals the data's original meaning to prevent it from being known or used, or similar protections."

Prohibit Government-Mandated Installation or Use of Surveillance Equipment

As drafted, sections 13(1)-(4) require electronic service providers ("ESPs") to provide "all reasonable assistance" upon request by the Minister "to a person or class of persons specified in the request to permit the assessment or testing of any device, equipment or other thing that may enable an authorized person to access information." This language could be interpreted to empower the government to require Apple to install government-controlled equipment in its networks or on its devices. The Bill adds, "[f]or greater certainty, the assessment or testing must not have the effect of granting access to personal information." This provision, however, either standing alone or in context, does not clearly prohibit the government from requiring a provider to use government-owned or -controlled equipment to accomplish the assessment or testing. This provision poses unacceptable risks to user and network security, privacy, and operations.

Moreover, under section 5(2)-(3), core providers, such as Apple, would be subject to currently unknown regulations promulgated in the future by the Governor in Council that are intended to facilitate government surveillance. Again, such regulations could require Apple to install government equipment in its networks. In formulating such regulations, the Governor in Council is required to "take into account," among other things, "the potential impact of the regulation on privacy protection and cybersecurity." By no means does this prohibit the issuance of regulations that could require Apple to install government equipment in its networks, or, indeed, undermine encryption.

The Bill should expressly prohibit the government from ordering or requiring providers to install or use in their networks, or on their devices, surveillance or other equipment that the government owns or controls.

Narrow Secrecy Provisions to What Is Necessary and Allow Limited Disclosures

We understand that there may be legitimate reasons to maintain the confidentiality of sensitive investigations in certain circumstances. However, transparency and government accountability are also important considerations, especially with respect to surveillance activities that impact data security and privacy.

Section 14 is problematic because it broadly restricts disclosure across multiple categories of information. For example, it prohibits disclosure of (i) information contained in an order, (ii) the fact that an ESP is or was subject to an order, and (iii) "any prescribed information."

Section 14 is broader than necessary and risks preventing providers from taking responsible steps to protect their users. The language in section 14 prohibiting ESPs from disclosing "any prescribed information" is vague and could be interpreted to prohibit an ESP from disclosing the existence of a security vulnerability to anyone, including in scenarios that could mitigate potential harm to Apple's

Canadian customers. This could create significant cybersecurity risks for providers and their users across Canada.

The Bill should be amended to clarify that providers may consult independent legal counsel and relevant technical experts when assessing compliance with any order; make protected disclosures to competent foreign authorities and to courts in Canada and foreign jurisdictions under seal; and disclose information necessary to mitigate potential harm to their users' security. We believe ESPs should be permitted to disclose security threats in appropriate and secure circumstances. Accordingly, secrecy provisions should be narrowed to protect specific investigative techniques, not to shield the entire framework from public accountability.

Limit Future Regulatory Expansion

Bill C-22 leaves significant substantive issues to future regulations, which could extend beyond the current scope of the legislation. For example, section 5(2) authorizes the Governor in Council to make regulations on an expansive set of core provider obligations, including the development of technical capabilities, the installation of devices or equipment that may enable access, and the retention of metadata for up to six months. Given the impact on cybersecurity, encryption, and providers' rights and obligations, Parliament should establish safeguards and limits in the statute, rather than defer them to future regulations.

Establish a Statutory Right to Meaningful and Timely Judicial Review

We welcome the provision for judicial review in the Federal Court under section 17. However, the proposed Act should more clearly ensure that ESPs have the ability to seek thorough and timely judicial review of any order or action before being required to comply. The Bill should be amended to specify: (1) providers may challenge regulations, ministerial orders, or any other government action before being required to comply with such measures; (2) providers may appeal such judicial determinations; and (3) courts may review all aspects of a regulation, ministerial order, or other government action.

Clarify That Providers Are Not Required to Produce Data Stored Outside Canada

The Bill does not clearly limit the government's ability to compel access to data stored outside Canada. This uncertainty could create conflicts with foreign law and leave providers operating in multiple jurisdictions facing inconsistent legal obligations. The Bill should expressly provide that no warrant, order, directive, regulation, or other mandate may require the disclosure or production of data located outside Canada.

Narrow Inspection Powers and Include Other Appropriate Safeguards

Section 20(7) would allow the government to enter private property without a warrant, and there are no provisions in Bill C-22, as drafted, ensuring that proprietary or confidential business information obtained in the course of that inspection would be protected. Accordingly, we urge the Committee to remove section 20(7), which would allow persons to enter private property without a warrant, and to impose clear limits on the disclosure of proprietary and confidential business information obtained pursuant to any order.

Clearly Define and Narrow the Scope of Covered Providers and Services

We understand that the government believes it needs to modernize lawful access for the digital age. However, Bill C-22's definition of ESP in section 2(1) as any person that provides an "electronic service" to persons in Canada or carries on any part of its business activities in Canada is extraordinarily broad. As drafted, the definition could encompass not only traditional telecommunications common carriers

and service providers, but also a wide range of companies offering any interconnected digital product or service used by Canadians.

The breadth of this definition is further compounded by the fact that the schedule of "core providers" subject to the regulatory obligations under section 5 is entirely blank as currently drafted. Instead, the classes of core providers are to be defined through Governor in Council regulation under section 5(1), with no statutory limits on the categories that may be added after the Bill passes.

Parliament should clearly define the scope of covered providers, and the products and services they offer Canadians, so future requests for Canadians' data are narrowly tailored to the specific investigative need rather than imposed as blanket obligations on broad classes of providers that weaken the privacy protections afforded all Canadians.

Conclusion

While we share the government's commitment to ensuring that law enforcement has robust tools to protect Canadians, we respectfully submit that these tools must not come at the expense of the security and privacy protections on which Canadians depend to protect their fundamental rights, their economic prosperity, or the security of the nation.

Apple has worked, and will continue to work, tirelessly to protect our users, including by strengthening security protections to address the pervasive and evolving threats to users' data, while continuing our commitment to respond to lawful requests. We appreciate the opportunity to submit our views regarding this legislation. We hope that our concerns will be addressed through amendments to the Bill, and we remain available to consult with the government and Parliament at any time to discuss these issues further.