RE: Senate Standing Committee on National Security, Defence and Veterans Affairs' study of Bill C-22, *An Act respecting lawful access*.

Executive Summary

1. Chamber of Progress is pleased to participate in the Senate Standing Committee on National Security, Defence and Veterans Affairs' (SECD) study of Bill C-22, *An Act respecting lawful access* ("Bill C-22" hereafter).

2. We share the Government of Canada's goal of protecting the public from cybercrime and national security threats. However, we are concerned that Bill C-22 in its current form would undermine Canadians' privacy and make them more vulnerable to cyber attacks.

3. We offer four constructive recommendations to Part 2 of the bill, the *Supporting Authorized Access to Information Act* ("Part 2" hereafter), to better align the legislation's lawful access objectives with the need to protect the privacy and security of Canadians:

   Recommendation 1: To preserve consumer security, explicitly prohibit mandates that could compromise encryption and broaden the definition of "systemic vulnerability" to protect consumer devices and operating systems.

   Recommendation 2: To protect consumers from the cybersecurity risks of mass data collection, remove the metadata retention mandate and rely on the existing preservation demand framework in the *Criminal Code*.

   Recommendation 3: To promote consumer trust, amend sections 14 and 15 so that non-disclosure orders are subject to judicial approval and permit transparency reporting by electronic service providers.

   Recommendation 4: Ensure that any interception is narrow and targeted to minimize exploitable vulnerabilities by requiring a targeted judicial warrant for surveillance capabilities and strictly limiting who qualifies as a 'core provider'.

Introduction

4. Chamber of Progress is a tech industry association promoting technology's progressive future, ensuring that all consumers benefit from technological leaps and that the industry operates responsibly and fairly.[1]

5. We share the Government of Canada's goal of protecting the public from cybercrime; however, we are deeply concerned that Bill C-22 in its current form will ultimately make Canadian consumers more vulnerable to bad actors.

6. As currently drafted, Part 2 introduces severe risks to the daily privacy and cybersecurity of Canadians by allowing the government to compromise encryption protections, mandate new surveillance infrastructure and metadata retention schedules, and prevent disclosing the existence of ministerial orders.

7. The recommendations below aim to strike a vital balance: ensuring law enforcement has targeted investigative tools, without treating every Canadian as a suspect or fundamentally weakening the digital infrastructure and encrypted communications we all rely on.

Recommendation 1: To preserve consumer security, explicitly prohibit mandates that could weaken end-to-end encryption and broaden the definition of "systemic vulnerability" to protect consumer devices and operating systems.

8. End-to-end encryption is the critical security protocol that protects consumers' private messages, banking details, and personal data from cybercriminals.[2] As the Canadian Chamber of Commerce noted in a recent report, "robust encryption and cyber security measures are cornerstones of Canada's economy, government operations and personal privacy in the digital age."[3]

9. The House Standing Committee on Public Safety and National Security (SECU) introduced two important amendments to Part 2 regarding encryption. First, it updated the definition of "systemic vulnerability" by shifting the risk from a

[1] Chamber of Progress. https://progresschamber.ca/
[2] Internet Society. "What Is Encryption?" Internet Society. https://www.internetsociety.org/issues/encryption/what-is/
[3] Canadian Chamber of Commerce. "Why Strong Encryption Is Essential." June 2025. https://chamber.ca/wp-content/uploads/2025/06/WhyStrongEncryptionIsEssential_June2025.pdf

"substantial risk" to a "credible risk" grounded in international technical standards, while excluding risks relating solely to information about individuals subject to a warrant, order, or other statutory authority to access information. Second, it added subsection 2(4), which explicitly protects electronic service providers from being compelled to decrypt data if they do not hold the decryption keys. While these amendments are a positive step towards protecting strong encryption, several issues remain to ensure that consumers' privacy and security are protected.

10. The bill states that companies do not have to comply if an order introduces a "systemic vulnerability" that would create a "credible risk" of unauthorized access to secure information based on "recognized international technical standards." However, the definition of "systemic vulnerability" in subsection 2(1), which informs the protections under subsections 5(5), 7(5), and 24(2.1), remains narrowly focused on "electronic services."

11. This drafting may unintentionally leave a gap in protection. Physical devices and operating systems are "equipment" or "hardware," not protected "electronic services." As a result, consumer devices, operating systems, and firmware may fall outside the bill's protections. That could allow the government to compel technology companies to bypass or weaken device-level encryption, which would create exploitable vulnerabilities for all users of the technology.[4]

12. While this provision has been meaningfully improved since Bill C-22 was first introduced, its amendment also brought a new exception for security risks associated with individuals who are subject to a court-authorized warrant, order, or other statutory authority. Unfortunately, it is simply not possible to restrict the risk of unauthorized access to one person.[5]

13. Moreover, subsection 2(4) leaves managed-key cloud services exposed and does not prohibit product redesigns. While subsection 2(4) protects providers from certain decryption obligations, it leaves a potential gap for cloud hosting, SaaS, and managed IT providers that both supply encryption and possess the information necessary to

[4] Joe Mullin and Cindy Cohn. "Salt Typhoon Hack Shows There's No Security Backdoor That's Only for the Good Guys." Electronic Frontier Foundation, Oct. 2024. https://www.eff.org/deeplinks/2024/10/salt-typhoon-hack-shows-theres-no-security-backdoor-thats-only-good-guys

[5] Michael Geist. "Is Compromise on Encryption Possible? Why Bill C-22's 'Minor Opening' Leaves the Central Question Unanswered." Michael Geist, Sep. 30, 2026. https://www.michaelgeist.ca/2026/09/is-compromise-on-encryption-possible-why-bill-c-22s-minor-opening-leaves-the-central-question-unanswered/

decrypt their customers' data. Furthermore, it fails to explicitly prohibit secret orders under section 7 that force companies to alter software, reconfigure products, or build pre-encryption interception tools.

14. Chamber of Progress respectfully submits that Parliament close these remaining loopholes by broadening subsection 2(1) to protect devices and operating systems, striking the flawed warrant carve-out, and amending subsection 2(4) to explicitly prohibit mandated product redesigns or weakened security architectures.

Amendment i)
Proposed additions underlined; deletions in strike-through

systemic vulnerability means a vulnerability in the electronic protections of an electronic service, device, equipment, or operating system 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, including any requirement to weaken, bypass, or circumvent end-to-end encryption ~~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~~. (vulnérabilité systémique)

Amendment ii)

Decryption
2(4) No obligations under this Act are to be construed as compelling an electronic service provider to; (a) decrypt, or to ensure that an authorized person is able to decrypt, any information that is encrypted by a person to whom the electronic service provider provides services, or; (b) alter, redesign, or reconfigure any product, service, software, hardware, operating system, or security architecture to weaken, circumvent, or disable encryption ~~unless the encryption was provided by the electronic service provider and the provider possesses the information necessary to decrypt the information~~.

Recommendation 2: To protect consumers from the cybersecurity risks of mass data collection, remove the metadata retention mandate and rely on the existing preservation demand framework in the *Criminal Code*.

15. Section 5(2)(d) of Part 2 grants the government the power to force entities designated as “core providers” to retain categories of metadata – such as sensitive location data and communication logs – on all users for up to a maximum period of time.

16. Chamber of Progress welcomes SECU's amendment to reduce the maximum retention period from 12 to six months and to require that categories of retained metadata be deemed essential for specified investigative purposes. Nevertheless, these safeguards do not eliminate the privacy and cybersecurity risks associated with requiring providers to retain sensitive information they would otherwise delete.

17. If imposed, such a requirement would cut against data privacy and minimization best practices and create new compliance burdens that would disproportionately impact smaller firms designated as “core providers,” such as new entrant sovereign data centres or artificial intelligence start-ups, which are currently being encouraged through government policy.

18. Moreover, Canadian and European technology innovators warn that the potential for blanket retention of personally identifiable data creates a massive honeypot of highly sensitive information that is vulnerable to data breaches and hackers.[6] Where personal data would otherwise be deleted, it would now be retained and susceptible to unauthorized access by cyber criminals or foreign-state-backed threat actors.

19. Canadian courts have established that metadata, including IP addresses and subscriber information, is constitutionally protected under section 8 of the Charter of Rights and Freedoms, which guards against arbitrary and unreasonable search and seizure.[7] Mandating that firms store categories of Canadians' metadata for up to six months treats innocent consumers with suspicion and arguably violates constitutional privacy protections.[8] Internationally, there is support for limiting metadata retention. The Court of Justice of the European Union has repeatedly held that the indiscriminate retention of metadata violates fundamental rights.[9]

---

[6] Joint Letter: Tech Industry Concerns with Bill C-22. Sep. 24, 2026. https://progresschamber.org/resources/coalition-letter-canada-amend-bill-c-22/
[7] Robert Diab. “Metadata and Bill C-22.” https://www.robertdiab.ca/posts/metadata-c22/
[8] Ibid.
[9] European Parliament. “Mapping CJEU limits on data retention frameworks.” https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/775878/EPRS_BRI(2025)775878_EN.pdf

20. Chamber of Progress submits that Parliament amend the bill to delete the blanket retention authority in paragraph 5(2)(d) and instead rely on the existing preservation demand powers under section 487.012 of the *Criminal Code*.[10]

21. This would still provide law enforcement with the ability to preserve specific data only when authorities have a reasonable suspicion tied to a specific, active investigation, without interfering with Canadians' privacy rights at scale.

Proposed amendment to subsection 5(2) of Part 2 (deletion in strike-through):

Core providers — obligations
5 (2) The Governor in Council may make regulations relating to the obligations of core providers, respecting

[...]

~~(d) the retention of categories of metadata — including transmission data, as defined in section 487.011 of the *Criminal Code* — for reasonable periods of time not exceeding six months.~~

Recommendation 3: To promote consumer trust, amend sections 14 and 15 so that non-disclosure orders are subject to judicial approval and permit transparency reporting by electronic service providers.

22. We recognize that non-disclosure orders are necessary tools for law enforcement and national security agencies, especially in cases where public disclosure could jeopardize an ongoing investigation or pose a direct threat to national security or cybersecurity.

23. The House SECU committee took a positive step toward addressing these concerns by adding a new provision in subsection 15(1) that allows the Minister, upon request, to issue a written authorization permitting a provider to disclose information related to an order. Chamber of Progress welcomes this new discretion, as it provides a

[10] Michael Geist. "The Lawful Access Privacy Risks: Unpacking Bill C-22's Expansive Metadata Retention Requirements." https://www.michaelgeist.ca/2026/03/the-lawful-access-privacy-risks-unpacking-bill-c-22s-expansive-metadata-retention-requirements/

valuable mechanism for ministerial relief.

24. However, relying solely on executive discretion does not go far enough to resolve the underlying problem. The blanket, indefinite non-disclosure orders proposed under section 14 of Part 2 establish an overly broad "secret by default" framework. This approach prevents companies from being transparent with their users about the safety of their platforms, meaning consumers will never know if the digital services they trust have been affected by state-mandated surveillance. Over time, this lack of transparency erodes trust in our digital ecosystem and technology sector.

25. Such measures signal to the international community that data stored in or routed through Canada may be subject to state access, undermining Canada's digital sovereignty and global competitiveness at a time when we are trying to increase our digital autonomy.

26. Although section 49 provides for annual ministerial reporting, it does not expressly establish an independent right for electronic service providers to publish aggregate information about orders affecting their services.

27. Therefore, additional action is required to ensure companies can be transparent with consumers. Chamber of Progress respectfully submits that Parliament amend section 15 so that non-disclosure is not automatic or perpetual. Secrecy should only be imposed where a judge is satisfied that public disclosure would jeopardize an ongoing investigation, national security, or cybersecurity, and the statute should explicitly permit providers to publish aggregate transparency reports.

Amendment i)

Proposed amendment to section 14 (additions underlined):

Prohibition on disclosure
14 An electronic service provider and any person acting on its behalf must not disclose any of the following information except as permitted under this Act or the *Canada Evidence Act*, <u>provided that a judge has made an order prohibiting disclosure under subsection 15(5)</u>:

Amendment ii)

Proposed amendment to section 15 (additions underlined):

Judicial order
(5) On application by the Minister or a requesting authority, a judge may make an order prohibiting the disclosure of the information referred to in section 14 if the judge is satisfied that public disclosure would jeopardize an ongoing investigation, national security, or cybersecurity.

Aggregate transparency reporting
(6) Nothing in this section prevents an electronic service provider from publishing aggregate transparency reports containing statistical information about the orders they are subject to, provided the reports do not compromise an individual investigation, national security, or cybersecurity.

Recommendation 4: Ensure any interception is narrow and targeted to minimize exploitable vulnerabilities by requiring a targeted judicial warrant for surveillance capabilities and strictly limiting who qualifies as a 'core provider'.

28. Sections 5(2) and 7 give the government the authority to force service providers to build, install and maintain surveillance systems and interception capabilities directly into their networks. While we share the government's goal of protecting Canadians from cybercrime and national security threats, forcing new access points into our digital infrastructure introduces severe structural risks to our sensitive data and communications.

29. Any backdoor that is inserted into our networks creates new vulnerabilities that can be exploited by unauthorized third parties, such as foreign adversaries or cyber criminals.[11] These risks are not hypothetical. The recent "Salt Typhoon" cyberattacks in the U.S. offer a cautionary tale for Canada; state-sponsored hackers were able to successfully breach major networks and extract consumer data by exploiting the

[11] Joe Mullin and Cindy Cohn. "Salt Typhoon Hack Shows There's No Security Backdoor That's Only for the Good Guys." Electronic Frontier Foundation, Oct. 2024. https://www.eff.org/deeplinks/2024/10/salt-typhoon-hack-shows-theres-no-security-backdoor-thats-only-good-guys

same type of lawful access interception infrastructure that Bill C-22 will enable.[12] More recently, hackers breached an FBI surveillance system, exposing sensitive investigation data and triggering a major incident.[13]

30. Alongside these cybersecurity risks, there is growing concern about extraterritorial access to Canadians' data, via legal instruments such as the U.S. CLOUD Act.[14] Inserting interception capabilities will exacerbate these concerns by creating new opportunities for unauthorized access, effectively undermining Canada's digital sovereignty. As we build sovereign AI compute and data centre infrastructure to ensure our global competitiveness, we cannot afford to create new vulnerabilities for foreign adversaries to exploit.

31. Although ministerial orders under section 7 are subject to approval by the Intelligence Commissioner, Chamber of Progress believes that surveillance capabilities should also be subject to targeted judicial authorization tied to a specific investigation. This safeguard would help prevent blanket surveillance by ensuring that surveillance capabilities are tied to specific investigations, individualized suspicion, and independent judicial oversight.

32. Furthermore, lawmakers should narrow who qualifies as a "core provider" to ensure the government cannot secretly mandate surveillance equipment inside everyday consumer devices, such as smart home appliances or vehicles, without parliamentary oversight.

33. As currently drafted, the bill defines "electronic service provider" so broadly that it captures almost any business that creates, processes, or stores digital information. Because of this expansive scope, the manufacturers could be required to turn everyday household items – like smart TVs, smart refrigerators, or smart speakers –

---

[12]Sarah Krouse, Dustin Volz, Aruna Viswanatha, and Robert McMillan. “U.S. Wiretap Systems Targeted in China-Linked Hack.” The Wall Street Journal. https://www.wsj.com/tech/cybersecurity/u-s-wiretap-systems-targeted-in-china-linked-hack-327fc63b

[13] John Sakellariadis. “FBI Hack Surveillance System Major Incident.” Politico, Apr. 1, 2026. https://www.politico.com/news/2026/04/01/fbi-hack-surveillance-system-major-incident-00854237

[14] Anja Karadeglia. “Data Stored in Canada Can Be Subject to Foreign Courts, Government Paper Warns.” BayToday. https://www.baytoday.ca/national-news/data-stored-in-canada-can-be-subject-to-foreign-courts-government-paper-warns-11436428

into active listening devices. Similarly, tech companies could be forced to track the real-time location of every smartphone, smartwatch, and vehicle.

34. To impose reasonable limits on the surveillance capabilities proposed in Part 2, we submit the following three amendments:

Amendment i)

Proposed amendment to subsection 5(1) of Part 2 (changes underlined):

Core providers — classes
5 (1) The Governor in Council may, by regulation, amend the schedule by adding, amending or deleting a class of electronic service providers, provided that the class of electronic service providers is primarily engaged in the provision of telecommunications services to the public and does not include the provision of consumer devices, operating systems, smart home appliances, or vehicles.

Amendment ii)

Proposed amendment to subsection 5(4) of Part 2 (changes underlined):

Restrictions
(4) Paragraph (2)(d) does not authorize the making of regulations that require core providers to retain information that would reveal

(a) the content — that is to say the substance, meaning or purpose — of information transmitted in the course of an electronic service;

(b) a person's web browsing history; or

(c) a person's social media activities.

Targeted warrant required

(4.2) Paragraph (2)(b) does not authorize the making of regulations that require core providers to build, install, or deploy any interception capability or equipment unless an authorized person has obtained a targeted warrant from a judge authorizing its deployment in relation to a specific, active investigation.

Amendment iii)

Proposed amendment to section 7 of Part 2 (changes underlined):

Order
7 (1) Subject to section 8, the Minister may make an order with respect to an electronic service provider and the order may contain any provision that may be contained in a regulation made under subsection 5(2), whether or not the provider is a core provider. The order must specify a period, not exceeding two years, during which it is valid.

[...]

Targeted warrant required

(1.2) The Minister must not make an order under subsection (1) requiring an electronic service provider to build, install, or deploy any interception capability or equipment unless an authorized person has obtained a targeted warrant from a judge authorizing its deployment in relation to a specific, active investigation.

Conclusion

35. Chamber of Progress thanks the Senate Standing Committee on National Security, Defence and Veterans Affairs for the opportunity to participate in its study of Bill C-22.

36. To reiterate, Chamber of Progress offers four constructive recommendations to Part 2 to better align its goal of modernizing law enforcement tools with the need to protect privacy and security for Canadians:

    Recommendation 1: To preserve consumer security, explicitly prohibit mandates that could weaken end-to-end encryption and broaden the definition of "systemic vulnerability" to protect consumer devices and operating systems.

    Recommendation 2: To protect consumers from the cybersecurity risks of mass data collection, remove the metadata retention mandate and rely on the existing preservation demand framework in the *Criminal Code*.

Recommendation 3: To promote consumer trust, amend sections 14 and 15 so that non-disclosure orders are subject to judicial approval and permit transparency reporting by electronic service providers.

Recommendation 4: Ensure any interception is narrow and targeted to minimize exploitable vulnerabilities by requiring a targeted judicial warrant for surveillance capabilities and strictly limiting who qualifies as a 'core provider'.

37. We believe that these targeted recommendations will successfully balance the need to modernize Canada's cybercrime investigation tools with protecting Canadian consumers from unintended privacy risks and cybersecurity vulnerabilities.

38. We respectfully request the opportunity to appear before the SECD committee to discuss these recommendations further during the committee's study of the bill.