May 8, 2026

Chair Jean-Yves Duclos
Vice Chair Frank Caputo
Vice Chair Claude DeBellefeuille
Committee Member Sima Acan
Committee Member Chak Au
Committee Member Marianne Dandurand
Committee Member Anthony Housefather
Committee Member Rhonda Kirkland
Committee Member Dane Lloyd
Committee Member Marcus Powlowski
Committee Member Jacques Ramsay
Committee Member Amandeep Sodhi

Sent via email

Re: BSA Comments on Bill C-22, the Lawful Access Act 2026

The Business Software Alliance (BSA)[1] welcomes the opportunity to provide feedback about our concerns with Bill C-22, which creates new authorities for Canadian law enforcement agencies to access information held by technology companies.

BSA is the leading advocate for the global software industry. Our members create business-to-business technologies to help their customers innovate and grow. For example, BSA members provide tools including cloud storage services, customer relationship management software, human resource management programs, identity management services, cybersecurity, and collaboration software. Many BSA members have significant operations in both Canada and the US, with operations, investments, and employees in both countries.

BSA raised concerns last fall with Bill C-2, the predecessor of Bill C-22.[2] We remain concerned with Bill C-22, which continues to create expansive powers for law enforcement agencies to obtain information from technology companies. We strongly recommend the bill be amended to:

- Promote strong encryption and protect against systemic vulnerabilities;
- Ensure high standards for law enforcement demands issued to technology companies;
- Impose clear limits on any non-disclosure orders; and
- Specifically allow comity challenges and ensure respect for international laws.

[1] BSA's members include: Adobe, Alteryx, Asana, Atlassian, Autodesk, Avalara, Bentley Systems, Box, Cisco, Cohere, Cohesity, Dassault Systemes, Databricks, Docusign, Dropbox, Elastic, EY, Graphisoft, HubSpot, IBM, Informatica, Kyndryl, MathWorks, Microsoft, Notion, Okta, OpenAI, Oracle, PagerDuty, Palo Alto Networks, PTC, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Trend Micro, TriNet, Workday, Zendesk, and Zoom Communications Inc.

[2] *See* Business Software Alliance, Letter of Sept. 30, 2025, *available at* https://www.bsa.org/policy-filings/bsa-letter-canadian-parliaments-standing-committee-public-safety-national-security-law-enforcement-access-provisions-canada-bill-c-2.

I. Promote Strong Encryption and Protect Against Systemic Vulnerabilities

We strongly encourage you to ensure Bill C-22 does not weaken the security or privacy of products and services offered in Canada by forcing companies to adopt or ignore systemic vulnerabilities.

We recommend removing Part 2 entirely, because it raises the same concerns that BSA previously raised about Part 15 of Bill C-2. This bill continues to give the Governor in Council authority to draft regulations to give government agencies broad powers to require technical assistance from "core" electronic service providers. These companies must provide "capabilities related to extracting and organizing information" including "providing access to such information." (Part 2, Sec. 5(2)(a).) The bill also requires a much broader set of companies and persons to "assist" law enforcement, including by obligating electronic service providers to provide certain assistance (Part 2, Sec. 14) and by requiring assistance by persons located in places that are searched (Part 2, Sec. 20(5).)

The breadth of these powers creates significant concerns, despite several changes introduced in Bill C-22 that were lacking in Bill C-2. These include defining "systemic vulnerabilities" and adding statutory factors for the Governor in Council to take into account when making regulations for core providers.

Bill C-22 continues to create expansive powers — and may prevent electronic service providers from providing privacy-protective services, including encrypted services that securely handle users' data. Although several provisions in Part 2 state that providers are not required to introduce or ignore a systemic vulnerability, that limitation is not carried throughout each power created in Part 2. For example, neither a specific obligation for electronic providers to provide assistance (created in Part 2 Sec. 14) or a broader obligation for others to assist (created by Part 2 Sec. 20(5)) contain clear exceptions to ensure these powers cannot be used to require companies to introduce or ignore systemic vulnerabilities. The bill should also establish a clear mechanism for challenging orders that raise such security concerns.

Less than two years ago, Canada recognized the benefits of strong encryption when it joined three other countries in urging companies to protect against international cybersecurity threats by increasing their use of encryption, including to ensure that "traffic is end-to-end encrypted to the maximum extent possible."[3] Strong encryption:

- Protects consumers' information and ensures they control where their information is sent, even if a device is lost or stolen.
- Defends against massive data breaches, by safeguarding companies' digital records and protecting financial payment information and other online transactions.
- Prevents hackers from accessing sensitive information such as health records, or from wreaking havoc with transportation and electrical grids.
- Protects privacy, improves security, and promotes anonymity.
- Secures data, networks, and devices — including critical infrastructure, identity information, 5G networks, and IoT devices.

[3] *See* Enhanced Visibility and Hardening Guidance for Communications Infrastructure, Dec. 3, 2024, jointly published by government agencies of the United States, Canada, Australia, and New Zealand, *available at* https://media.defense.gov/2024/Dec/03/2003596322/-1/-1/0/JOINT-GUIDANCE-ENHANCED-VISIBILITY-HARDENING-GUIDE-FOR-COMMS-INFRASTRUCTURE.PDF.

The concerns raised by Part 2 are exacerbated because the bill does not define the new powers it creates or the "core" electronic service providers subject to them — but leaves those critical elements to later regulations. That creates little room for stakeholder input, short-circuits debates on the breadth of these powers, and leaves companies with too much uncertainty about their potential obligations. In some cases, uncertainty around open-ended assistance or inspection obligations may introduce risk into product design considerations, with the potential to deter privacy-protective or security-forward architectures. Regulatory frameworks should incentivize security by design, not create uncertainty that could undermine investment in safer technologies. We urge you not to take this approach.

Recommendations:

- Part 2 should be removed from the bill.

- If Part 2 is retained, it should be significantly revised to ensure the powers it creates cannot be used to require companies to introduce or ignore systemic vulnerabilities. We strongly recommend seven key changes:

    - **First: Ensure new powers cannot require systemic vulnerabilities.** Rather than relying on provision-by-provision exceptions, as in the current text, the bill should create a clear new exception that applies to all of Part 2.

        - That language should state: No electronic service provider is required to comply with any order or request made pursuant to Part 2, or any regulations issued under Part 2, if compliance with the request or order would require the provider to introduce a systemic vulnerability in a service or prevent the provider from rectifying such a vulnerability.

        - Alternatively, if the bill continues to rely on provision-by-provision exceptions, it should create clear exceptions to the powers created by Part 2 Sec. 14 and Part 2 Sec. 20(5) that state these powers do not require introducing or ignoring systemic vulnerabilities.

    - **Second: Strengthen the definition of systemic vulnerabilities**. While we appreciate that Bill C-22 (unlike Bill C-2) defines systemic vulnerabilities, that definition should be strengthened to ensure it prohibits using powers created by the bill to undermine strong encryption. Specifically, we recommend defining systemic vulnerability as "forced decryption through technical means or any other technical change that risks the security or privacy of a user or all users of a service."

    - **Third**: **Create statutory limits for designating core providers in the Act — or require parliamentary oversight.** The bill gives significant discretion to the Governor in Council to identify classes of "core providers" that will be subject to these new powers. We recommend narrowing that authority, at least to establish clear statutory criteria and guardrails for designation, or to require meaningful parliamentary oversight and consultation before any class of core providers is identified. These safeguards are particularly important given the breadth of regulatory obligations imposed on core providers.

- **Fourth: Create limits on non-disclosure orders.** The bill creates broad powers to prohibit providers from disclosing the existence or content of any order issued under Part 2. This non-disclosure framework is overly broad and may impose a default rule of secrecy, which undermines trust and transparency about a provider's services. We recommend amending the bill to: (1) limit the issuance of any non-disclosure order to circumstances where the requesting authority can demonstrate, based on specific facts, that disclosure would jeopardize the conduct of a specific investigation; (2) limit the duration of any non-disclosure orders, subject to judicial extensions, and (3) affirmatively recognize that non-disclosure orders do not prevent a provider from issuing general reports on the existence or nature of demands in aggregate, such as transparency reporting that does not identify a specific order or investigation.

- **Fifth: Narrow the definition of "electronic service providers."** As written, the bill defines an extremely broad set of electronic service providers — wrapping in any company that "provides" a service or feature "that involves the creation, recording, storage, processing, transmission, reception, emission, or making available of information in electronic, digital, or any other intangible form" through technological means. This definition should be narrowed, including to focus on entities that provide electronic *communications*.

- **Sixth: Avoid requiring retention of metadata**. The bill would authorize regulations requiring certain providers to retain metadata, including transmission data, for "reasonable" periods of up to one year. This could force companies to adopt blanket retention policies — and keep every type of metadata about every customer they serve. Such indiscriminate retention would result in a staggering amount of data collection and is incompatible with core concepts of PIPEDA, including data minimization. Indiscriminate retention of metadata would also undermine privacy-by-design practices adopted across modern electronic services. We strongly recommend replacing this one-size-fits-all mandate with a proportional requirement to preserve metadata data on demand, limiting the obligation to retain metadata to circumstances in which it is proportionate and tied to a specific investigation.

- **Seventh: Require warrants for searches of data centers.** Part 2 Sec. 20 should be amended to require judicial authorization for entry into any place pursuant to the inspection power it creates — not just for dwelling houses. For example, the provision could provide law enforcement authorities the ability to search locations including data centers if they have "reasonable grounds to believe that anything relevant" to verifying or preventing compliance or non-compliance with the bill is located there. This standard is far too low given the amount of sensitive data that may be inspected. This provision should be revised to require a judicial warrant to enter into places pursuant to the inspection power.

II. Ensure High Standards for Accessing Information from Technology Companies

Law enforcement agencies should be required to meet high standards to obtain legal process that can require technology companies to disclose consumers' data.

At minimum, to exercise any of the new powers in Parts 1 or 2, the bill should require "reasonable grounds to believe" an offense has occurred rather than "reasonable information to suspect," which is used throughout the bill.

In addition, the bill should be revised in two ways to ensure privacy protections for data held by technology providers:

- First, the bill should require law enforcement agencies to first obtain information from the owner of the information, not the technology service provider, if doing so would not comprise the investigation. For example, when seeking the information of a business, law enforcement agencies should direct legal process to the business, rather than to the business's technology provider. Because the business owns and controls its information, it is in the best position to understand what information is responsive to a law enforcement request and whether any special circumstances, such as legal privileges, may apply to the information sought.

- Second, when law enforcement agencies obtain information in exigent circumstances, they should later obtain a post hac warrant. This will ensure that exceptions in the bill for access in exigent circumstances do not undermine the legal process required to obtain information in the normal course.

Recommendations:

- Create a higher standard for new legal demands. At minimum, require "reasonable grounds to believe" rather than "reasonable grounds to suspect."

- Revise amendments to Criminal Code Section 487.0181(2), which governs certain legal requests to technology providers. These changes should ensure that law enforcement authorities direct requests to the owner of the data they seek when possible, rather than seeking a business's data by issuing an order to the business's technology provider. Specifically, a new factor should be added to this provision stating: "(c) if the subscriber is an entity, seeking the information directly from the entity would be detrimental to the investigation."

- Revise amendments to Criminal Code Section 487.11, which governs legal process in exigent circumstances. This language should add a requirement to obtain a warrant as soon as practical when obtaining data under exigent circumstances. Specifically, a new subsection should state: "(c) the peace officer or public officer must obtain a warrant as soon as practical but no later than 48 hours after obtaining any data under this section."

III. Impose Clear Limits on Non-Disclosure Orders

There should be strict limits on any orders that prohibit companies from disclosing information about legal process they receive.

Both Part 1 and Part 2 create expansive powers to issue secret government demands. In addition to the recommendations discussed above for Part 2, Part 1 should also be revised to limit such secrecy.

At the outset, any nondisclosure orders should only issue with judicial approval — even when the underlying legal order does not require judicial approval. In addition, the bill should create a

specific mechanism to challenge non-disclosure orders; those challenges should be in addition to (and separate from) any opportunity to challenge the underlying order. This ensures companies can comply with valid orders but challenge overbroad secrecy demands. Finally, we recommend creating a statutory reporting framework in Part 1. Statutory reporting frameworks can promote transparency about the use of new powers and enable greater understanding by both policymakers and the public about how new authorities are used.

Recommendations:

The bill should be amended to ensure:

- Non-disclosure orders are only issued by judges. Part 1 currently requires judges to issue non-disclosure orders in some circumstances, but not for non-disclosure orders that accompany information demands issued under Criminal Code Section 487.0121. Non-disclosure orders should only be issued by judges — even if the underlying legal demand does not require judicial authorization.

- A new mechanism is created to provide a clear method for providers to challenge non-disclosure orders, separate from any challenges to the underlying legal demand.

- A statutory reporting framework is created to require public authorities to publish aggregated information about the quantity of each type of legal process they issue each year, including the quantity of any associated non-disclosure orders.

IV. Allow Comity Challenges and Ensure Respect for International Laws

The bill creates new powers for the Canadian government to issue legal demands to global companies. In particular, Part 1 authorizes judges to request transmission data or subscriber information from foreign entities, subject to certain conditions. However, the bill does not clearly provide companies the ability to raise legal challenges to these orders based on conflicting laws. Further, Part 1 Sec. 2 appears to grant the Canadian government the authority to remotely search cloud-based data (by targeting "computer data contained in or available to the computer system") regardless of which country that data is located in or which foreign laws may apply.

We strongly recommend allowing companies to raise challenges to legal process when they face a conflict of laws. These challenges can be based on principles of international comity. For example, in the United States the statute governing law enforcement demands to technology companies creates specific opportunities to raise comity challenges, which take into account the interests of the government seeking to require disclosure and the interest of the government in preventing a disclosure, as well as the location and nationality of the individual whose information is sought.[4] If Bill C-22 gives Canadian law enforcement broad authorities to issue legal demands to global companies, it should also provide a clear way to resolve conflicts of laws created by the exercise of those powers.

Recommendation:

- Revise Part 1's amendments to Criminal Code Section 487(2.1), which governs warrants for examining computer data. This provision should remove language allowing a search

[4] *See* 18 U.S.C. 2703(h) (creating comity challenges in certain circumstances) and 18 U.S.C. 2703 rule of construction (recognizing common law comity challenges in other circumstances).

to include computer data “available to” a computer system. In addition, amendments to Criminal Code Section 487(2.6) should remove language referring to a computer system “through which the computer data is available.” These changes can help to avoid remote extraterritorial searches that may conflict with foreign laws.

- Add a new provision to Part 1 creating a mechanism to challenge any order that creates a conflict of laws, on the basis of international comity principles. That provision could also set out factors for a court to consider in assessing potential conflicts of laws.

- Revise the bill to increase the time for technology providers to respond to and object to orders, to give providers more time to engage with government authorities about legal process without requiring them to file legal action.

* * *

Thank you again for the opportunity to provide our views. We welcome an opportunity to further discuss these issues.

Sincerely,

Kate Goodloe
Managing Director, Policy
Business Software Alliance