September 30, 2025

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 Ali Ehsassi
Committee Member Rhonda Kirkland
Committee Member Dane Lloyd
Committee Member Jacques Ramsay

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

Re: BSA Comments on Bill C-2's Law Enforcement Access Provisions

The Business Software Alliance (BSA)[1] welcomes the opportunity to provide feedback on provisions in Bill C-2 that create 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 are enterprise software and technology companies that create business-to-business products and services 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.

We are concerned with Parts 14 and 15 of Bill C-2, because these provisions create expansive new 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.

I. Promote Strong Encryption and Protect Against Systemic Vulnerabilities

We strongly encourage you to ensure Bill C-2 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 15 entirely. Part 15 gives the Governor in Council authority to draft regulations that will give government agencies broad powers to require technical assistance from "core" electronic service providers. These technology companies must provide "capabilities related to extracting and organizing information" including "providing access to such information." (Part 15.5(2).) The bill also requires a much broader set of companies and persons to "assist" law enforcement, including requiring assistance by persons located in places that are searched. (Part 15.19(5).)

The breadth of these powers creates significant concerns. These new authorities may prevent electronic service providers from providing privacy-protective services, including encrypted services that securely handle users' data. Although several provisions in Part 15 state that providers are not required to introduce or ignore a systemic vulnerability, that limitation is not carried throughout each power created in Part 15. For example, the obligation to assist in Part 15.14 and the duty to assist in Part 15.19(5) do not clearly state that these powers cannot be used to require companies to introduce or ignore systemic vulnerabilities.

We strongly recommend removing Part 15 to avoid undermining the widespread use of strong encryption. Just last year, 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."[2] 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.

The concerns raised by Part 15 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. We urge you not to take this approach.

[2] *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.

Recommendations:

- Part 15 should be removed from the bill.

- If Part 15 is retained, it should be significantly revised to ensure new powers created by this part cannot be used to require companies to introduce or ignore systemic vulnerabilities. We strongly recommend at least four 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 provision that applies to all powers in Part 15, including the assistance obligations in Part 15.14 and in Part 15.19(5).
        - That language should state: No electronic service provider is required to comply with any order or request made pursuant to Part 15, or any regulations issued under Part 15, 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.

    - **Second: Define systemic vulnerabilities**. Systemic vulnerability should be defined by statute 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 considerations concerning core providers.** The Governor in Counsel should be subject to statutory considerations in making determinations under Part 15 Section 5, which addresses obligations on core providers. Specifically, the bill should add the following:

        - *Factors***.** Before making regulations respecting the obligations of core providers, the Governor in Council must consider:
            - operational impacts on affected core providers;
            - impact on the public safety of Canadians;
            - financial impacts on affected core providers;
            - impact on the delivery of services and systems to consumers; and
            - any other factor that the Governor in Council considers to be relevant.

    - **Fourth: Require warrants for searches of data centers.** Part 15 Section 19 gives Canadian 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 is housed in data centers. This provision should be revised to require a judicial warrant to enter a data center or other location.

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 14 or Part 15, 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 obtain information from the owner of the information, not the technology provider, when possible. 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 Part 14's 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 at the owner of the data they seek when possible, rather than seeking out data that belongs to a business by issuing legal process 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 Part 14's 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 prohibiting companies from disclosing information about the legal process they receive.

We strongly recommend revising Part 14 to ensure that non-disclosure orders 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. For example, a provider may receive a legal order to produce information relating to an investigation that it knows has been made public in another country. In that circumstance, the provider may want to comply with the underlying legal order but challenge the non-disclosure order, which may not be needed if the facts of the investigation are public. The provider should have a clear way to raise such a challenge, without challenging the underlying legal demand.

Finally, we recommend adding a new provision to Part 14 to create a statutory reporting framework. The government should be required to publish aggregated statistics about the amount of each type of legal process it issues each year and the amount of non-disclosure orders issued. Statutory reporting frameworks can promote transparency about the use of new powers and enable greater understanding by both policymakers and the public about how these authorities are used.

Recommendations:

The bill should be amended to ensure:

- Non-disclosure orders are only issued by judges. Part 14 currently requires judges to issue non-disclosure orders in some circumstances, but not for non-disclosure orders that accompany information demands. 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 by Technology Providers 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 14 authorizes judges to request transmission data or subscriber information from a foreign entity, 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 14 Section 2.4 appears to grant the Canadian government the authority to conduct remote searches of cloud-based data — regardless of where that data is located or which foreign laws may apply to it.

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.[3] If Bill C-2 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 14's amendments to Criminal Code Section 487(2.4), which governs warrants for examining computer data. This provision should remove language allowing a search to include computer data "available to" a computer system. In addition, amendments to Criminal Code Section 487(2.7) 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 14 creating a mechanism to challenge any order issued under Part 14 that creates a conflict of laws, on the basis of international comity principles. That provision could also set out factors for the court to consider in assessing potential conflicts of laws.

- Revise Part 14's amendments to Criminal Code Section 487.0193 to clearly allow foreign entities to seek judicial review of an order issued under Section 487.018. The revised language should expressly state that such challenges may be based on principles of international comity and may set out factors for the 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

[3] *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).