THE CANADIAN BAR ASSOCIATION
L'ASSOCIATION DU BARREAU CANADIEN

Bill C-22 *(Lawful Access Act, 2026)*

CANADIAN BAR ASSOCIATION
CRIMINAL JUSTICE, PRIVACY AND ACCESS TO INFORMATION LAW SECTIONS AND ANTI-CORRUPTION TEAM

May 2026

66 Slater St., Suite 1200, Ottawa, ON, Canada K1P 5H1
tel/tél. 613 237-2925 • **tf/sans frais** 1-800 267-8860 • **fax/téléc**. 613 237-0185 • cba.org • info@cba.org

PREFACE

The Canadian Bar Association is a national association representing 40,000 jurists, including lawyers, notaries, law teachers and students across Canada. The Association's primary objectives include improvement in the law and in the administration of justice.

This submission was prepared by the CBA Criminal Justice, Privacy and Access to Information Law Sections and Anti-Corruption Team, with assistance from the Advocacy Department at the CBA office. The submission has been reviewed by the Policy Committee and approved as a public statement of the CBA Criminal Justice, Privacy and Access to Information Law Sections and Anti-Corruption Team.

TABLE OF CONTENTS

Bill C-22 *(Lawful Access Act, 2026)*

Bill C-22 *(Lawful Access Act, 2026)*

I. EXECUTIVE SUMMARY

The Canadian Bar Association (CBA) Sections appreciate the opportunity to comment on Bill C-22 (*Lawful Access Act, 2026*). We also appreciate the good faith shown by the Ministers who shelved the previous iteration (part 14 and Part 15 of Bill C-2, the *Strong Borders Act*), for further stakeholders' consultations. The process improved the Bill, but the CBA has significant concerns.

The Bill creates new law enforcement and national security authorities in Part 1 and requires electronic service providers to create new capabilities in Part 2. Part 1 was authored by the Department of Justice and Part 2 was authored by the Department of Public Safety. While both are under the banner of "lawful access", they are distinct enough that separate bills would improve debate and discussion.

With respect to Part 1, "Timely Access to Data and Information", we are concerned about the balance between the threshold for obtaining subscriber information in light of the scope of data that is included in the definition (services and devices).. With respect to Part 2, which creates a new "Supporting Authorized Access to Information Act", our concerns are manifold.

The Government claims Canada is the only "Five Eyes" country without a "lawful access" law, which is only partly true. With respect to Part 1 of the Bill, Canada has long had modern tools for law enforcement and Canadian Security Intelligence Service to intercept communications, search premises and computers, and compel customer information from service providers. Canada lacks a comprehensive framework requiring service providers to be "intercept ready". Other countries' actions, especially those intrusive into personal privacy, are insufficient justification. Three of the Five Eyes countries do not have constitutionally protected rights to privacy or freedom from unreasonable search and seizure. The United Kingdom, Australia and New Zealand lack constitutional guardrails, allowing more latitude to enact intrusive surveillance laws. For Canada, s. 8 of the *Charter* must be front of mind.

II. GENERAL CONCERNS

The CBA opposes legislative practices that diminish debate and stakeholder engagement. In Resolutions 13-04-M[1] and 25-03-A[2], it urged limiting omnibus legislation to minor technical amendments. Bill C-22 instead enacts two different regimes under "lawful access": Part 1's changes to the *Criminal Code*[3] [hereinafter "the *Code*"] and Canadian Security Intelligence Service Act [hereinafter "the *CSIS Act*"][4] and Part 2's broad new framework. These should be separated to allow proper attention from the public and Parliamentarians.

The government must avoid deferring core definitions and obligations to future regulations. Legislation expanding government powers must be clear to ensure legal predictability and prevent function creep.

III. LAWFUL ACCESS OVERVIEW

Bill C-22 proposes to amend existing lawful access powers in the *Code* and the *CSIS Act,* requiring service providers to enable lawful access requests. Before discussing specific provisions, the CBA Sections will highlight overarching concerns.

A. Absence of evidence of necessity

Bill C-22 expands lawful access powers while reducing judicial oversight, materially impacting individual rights and freedoms and imposing costs on the private sector. Such changes require strong evidence of necessity and a proportionate impact on rights. The government has not provided evidence that these changes are necessary.

In briefings on Bill C-2 and Bill C-22, officials cited the elapsed time, technological advances, the expansion of digital service providers, the outdated Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications, and Canada's lack of enhanced lawful access legislation compared with other Five Eyes countries. The government has not cited investigations that are actually hindered by current provisions or technical limits that prevent service providers from satisfying lawful access orders. Both the *CSIS Act*[5] and the *Code*[6] provide for "assistance

---

1 CBA Resolution 13-04-M, Omnibus Bills, online.

2 CBA Resolution 25-03-A, Debate and Consultation in Multipart Legislation, online.

3 Criminal Code, RSC 1985, c C-46 [the *Code*].

4 *Canadian Security Intelligence Service Act*, RSC 1985, c C-23 [*CSIS Act*].

5 *CSIS* Canadian Security Intelligence Service Act, RSC 1985, c C-23, s 22.3;

6 Criminal Code, RSC 1985, c C-46, s 487.02.

orders", with judicial oversight for technical capabilities. Without evidence of necessity, these changes should not be implemented.

B. Expanding the scope of lawful access powers

Bill C-22 significantly expands lawful access: more parties could demand access, more information could be compelled, technical capacity requirements are broadened, and more entities would be subject to them, while judicial discretion is reduced. This expansion lacks adequate consultation with key stakeholders on its impact, feasibility and proportionality. We note that the consultations between Bill C-2 and Bill C-22 focused on "fixing" Bill C-2 rather than on necessity and proportionality.

C. Lack of safeguards

Part 1 of Bill C-22 reduces judicial oversight. Confirmation of Service Demand powers do not require prior judicial authorization, and officers may impose a non-disclosure for up to a year. Where judicial oversight exists, the threshold is low (i.e., reasonable grounds to suspect). Part 2 requires service providers to support state surveillance with minimal safeguards, no effective proportionality test, limited appeal, and non-disclosure, and allows orders without compensation, shifting costs from Law Enforcement Agencies (LEAs) to the private sector, effectively deputizing businesses as state agents.

Involving the Intelligence Commissioner in the approval of Ministerial Orders in Part 2 is an improvement over Bill C-2, but the combination of expanded powers, limited transparency, and limited safeguards creates serious risks to individual rights and freedoms.

D. *Charter* compliance

The CBA Sections believe Parts 1 and 2 of Bill C-22 risk violating the s. 8 *Charter* protection against unreasonable search and seizure. In particular, the scope of "subscriber information" may include information that s. 8 of the *Charter* would require a showing of more than reasonable suspicion. In addition, the provisions in Part 1 related to voluntary disclosures appear misaligned with the Supreme Court rulings in *R. v. Spencer* and *R. v. Bykovets*.[7]

[7] *R. v. Spencer*, 2014 SCC 43, [2014] 2 S.C.R. 212; *R. v. Bykovets*, 2024 SCC 6

IV. PART 1 - TIMELY ACCESS TO DATA AND INFORMATION

A. New Confirmation of Service Demand

Part 1 introduces s. 487.0121 of the *Code*, allowing a "peace officer or public officer", without judicial authorization, to demand that a telecommunications service provider confirm "whether or not they provide or have provided telecommunication services to any subscriber or client, or to any account or identifier, specified in the demand."

Insufficient Minimum Timeframe to Comply with Confirmation of Service Demand

The new section 487.0121(5) mandates a 24-hour time response time. The CBA suggests increasing this to 48 or 72 hours, except where there are "exigent circumstances", as 24 hours might be unrealistic for smaller providers.

Timeframe for Non-Disclosure

The new section 487.0121(5) also permits officers to prohibit disclosure of the demand for a period of up to a year.[8] The CBA is of the view that this is excessive and recommends reducing it to 90 days, with a court approval required for extensions. Because confirmation of service can precede the production order, the non-disclosure powers related to it should also be tightly time-limited.

Revocation or Variation of Demand

Bill C-22 introduces s. 487.0121(11) of the *Code*, allowing a judge to revoke or vary a demand. The CBA Sections submit that a judge should be able to revoke a demand if, in the totality of the circumstances, the demand is an unreasonable invasion of the privacy of the person(s) involved, where the issuing officer cannot meet the threshold, or where compliance would cause non-Canadian residents to violate foreign law.

B. New Production Order for "Subscriber Information"

Part 1 of the Bill creates a "production order for subscriber information," requiring judicial authorization based on mere suspicion that (a) an offence has been or will be committed under the *Code* or any other Act of Parliament; and (b) the subscriber information is in the person's possession or control and will assist in the investigation of the offence. "Reasonable grounds to suspect" is the lowest threshold in our legal system.

---

8 Section 158 of the Bill

Unlike General Production Orders, which specify data being sought, this order compels "all the subscriber information" in the recipient's possession. The definition "subscriber information" in Bill C-2 goes beyond general production orders connecting an identifier with a suspect, touching the "biographical core" protected by s. 8 of the *Charter*,[9] revealing "intimate details of the lifestyle and personal choices of the individual".[10]

The definition of "subscriber information", as presently worded in the proposed amendment to s. 487.011 of the *Code*, raises concerns that the information captured under this definition may go to the "biographical core". Orders may target any type of service provider such as hotels, health clinics, where the "types of services provided" and devices used (e.g. medical devices, networking equipment) can reveal highly personal and sensitive information.

The CBA Sections submit the definition of "subscriber information", as set out in s. 4 of the Bill, should be limited to information that identifies the subscriber or the client. If "devices" remain in the definition, it should be limited to devices that primarily facilitate communication. Any information beyond that, based on mere suspicion, risks violating s. 8 of the *Charter*.

C. New Judicial Authorization for Requests of Transmission Data or Subscriber Information from a Foreign Entity

Proposed new s. 487.0181 of the *Code* authorizes a "request" (not an order) directed at a "foreign entity that provides telecommunications service to the public." The request is approved by a judge on an application by a peace officer or a public officer. The threshold for issuing such a request mirrors the low threshold for the new subscriber production order (reasonable suspicion).

Subject to the same concerns expressed with respect to the new production order for subscriber information (threshold and scope), we are of the view that this section creatively attempts to address the uncertainty of serving Canadian production orders on entities domiciled wholly outside of Canada, relying on the voluntary cooperation of foreign entities, but it raises similar concerns about a low threshold and privacy.

---

9 *R. v. Plant*, 1993 CanLII 70 (SCC), at pg. 293:. "to protect a biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state".

10 *R. v. Bykovets*, *supra,* 2024 SCC 6, at para. 51, citing *R. v. Plant*, 1993 CanLII 70 (SCC), at pg. 293; *R. v. Spencer*, *supra*, at para. 27

D. Insufficient timeframes to seek review of orders

Bill C-22 shortens the window of opportunity for recipients of a production order or information demand to apply to the Court to have it varied or revoked. The amended s. 487.0193 of the *Code* applies to all production orders and reduces the review timeframe to ten business days after receiving the order (from previously generally 30). This timeframe is too short, particularly because decisions to challenge a production order require internal escalation, and many service providers may lack on-call legal counsel. It also limits engagement with the issuing officer or prosecutor to avoid a court application. This change should be removed from the Bill. The ability of a recipient to seek review of a production order should only expire with the deadline imposed by the judge to produce the materials. If advance notice to the officer is retained, email notice should suffice and pause the timeframe to allow time for filing application materials.

E. Voluntary disclosure and immunity

A significant concern of the CBA Sections is that no information demand is necessary for a peace officer or public officer to "ask" for information if the person is lawfully in possession of the information. The proposed legislation then goes on to provide that: "no production order or warrant, or information demand made under s. 487.0121, is necessary for a peace officer or public officer to receive any information from a person who is lawfully in possession of it and to act on the information if the person provides it voluntarily or is required by law, including a law of a foreign state, to provide it."[11]

While the CBA Sections appreciate that the stated intent of the proposed new s. 487.0195(3) may be to clarify that police may act on passive, unsolicited receipt of "tips" (e.g. from the National Center for Missing and Exploited Children or Crime Stoppers), it also creates a framework for routine, informal voluntary requests that may reach the "biographical core". The purported grant of immunity effectively destroys the privacy interests inherent in the requested information. It is also unclear how voluntary provision of information may be requested, and it may be easy for a company to confuse a "demand" with a "request" for voluntary provision of the material, which creates a muddy framework. Essentially, this bypasses judicial control in circumstances where a compelling privacy interest may exist.

This section should be narrowed to provide that police may collect and use information that is (a) provided to law enforcement or government on a person's or an organization's own initiative,

---

11 Section 164 of the Bill: the new s. 487.0195(3) of the *Code*

without being asked, or (b) information that is reported to the police or other authority pursuant to a legal obligation (such as mandatory reporting of child sexual abuse and exploitation material).

F. "Public" Information

The new s. 487.0195(4) of the *Code* suggests that police or public officers may use information that is "available to the public", assuming no privacy expectation. Law enforcement in the U.S. have bypassed the Bill of Rights by purchasing geolocation information from data brokers and participants in the online advertising ecosystem. One might characterize this information as being "available to the public", and police should not be able bypass the *Charter* by using data brokers.[12] In addition, the dark web is replete with "leak sites" where hackers disclose and sell information that has been unlawfully purloined from third parties. This illegally sourced information would be "available to the public." This section should be limited to information that is already lawfully available to the public and for which an individual no longer has any reasonable expectation of privacy.

G. Exigent Circumstances

Clause 167 of the Bill would replace s. 487.11 of the *Code*, allowing law enforcement to seize subscriber information or transmission and tracking data without an order where conditions for obtaining such information and data exist under the proposed applicable provisions, but by reason of exigent circumstances would be impracticable. Any such demand should include enough information for the service provider to be satisfied that exigent circumstances exist, especially where foreign laws related to emergency requests may apply.

H. Examination of Computer Data: Retention and Destruction

Section 156 of the Bill modernizes the language of s. 487 of the *Code* to incorporate the examination of computer data. Sections 170 & 171 would exempt "computer data" from sections 489.1 ("Restitution of thing or report") and 490.81 ("Management order") of the *Code*, raising concerns that law enforcement could retain it indefinitely. The CBA Sections recommend a provision mandating the destruction of seized data after a set time (e.g. one year), unless an extension is authorized by the court. Alternatively, the CBA Sections suggest amending warrant conditions[13] to data retention timeframes, after which data must be destroyed unless extended.

---

12 Wolfie Christl, Astrid Perry, Luis Fernando Garcia, Siena Anstis, and Ron Deibert. "Uncovering Webloc: An Analysis of Penlink's Ad-based Geolocation Surveillance Tech," Citizen Lab Report No. 191, University of Toronto, April 9, 2026, online. and Lena Cohen, Hudson Hongo. "The Government Uses Targeted Advertising to Track Your Location. Here's What We Need to Do." (Electronic Frontier Foundation, March 5, 2026) online.

13 Section 156(3) of the Bill: the proposed new s. 487(2.4) of the *Code*.

While prolonged examination may be helpful to complex and long-term investigations (e.g. ongoing criminal organization offences, homicides, sexual assault "cold cases", etc.), indefinite retention and open-ended use is unacceptable. The CBA Sections note that the *Code* already includes destruction provisions of computer data in the context of "preservation demands" (see s. 487.0194 of the *Code*).

I. Amendments to the Canadian Security Intelligence Service Act

The same concerns raised about the proposed amendments to the *Code* apply, more acutely, to the complementary amendments to the *CSIS Act.*[14] In criminal law proceedings, once a person is charged, they have the ability to have a judge scrutinize the state action in the context of a trial. *Charter* remedies are available at trial when officers fail to perform their obligations with respect to intrusive state powers. By contrast, activities undertaken by the Canadian Security Intelligence Service usually remain unknown to affected individuals and rarely face ex post facto judicial oversight. Any increase in CSIS lawful access should always be subject to judicial oversight and judicial control.

V. PART 2 – SUPPORTING AUTHORIZED ACCESS TO INFORMATION ACT

A. General

The CBA Sections are concerned that Part 2 of Bill C-22, creating the *Supporting Authorized Access to Information Act* (SAAIA), has not been justified by the government as being necessary or proportional. It mandates "electronic service providers" to build backdoors for law enforcement access to data, which may attract hackers, undermining public safety.

Part 2 of Bill C-8, the *Critical Cyber Systems Protection Act* (CCSPA), allows regulators to order "designated operators" of critical systems to take "any [necessary]measure",[15] potentially including backdoor vulnerabilities, confusing compliance obligations with lawful access and cyber systems regimes.

Obligations on "core providers" and the contents of Minister Orders should be limited so that they cannot dictate (i) any changes to products or services that an ESP provides in the ordinary course of business, (ii) the collection and retention of any data beyond what the ESP requires for its own

14 *CSIS Act*, RSC 1985, c C-23.

15 Part 2, s. 36(1)(b) of the *Critical Cyber Systems Protection Act*.

purposes, and (iii) any changes that would affect the functionality (including ordering additional functionality) for any products or services offered by the ESP.

B. Definitions and scope (s.2)

The scope of application of Bill C-2, Part 2 is based on the definition of "electronic service" and "electronic service provider". The power to require lawful access technical capacity applies to electronic service providers (ESP). The broad definitions of "Electronic Service" and "Electronic Service Provider" could include a much wider range of entities that have digital operations, including retail operations, academic institutions, health care facilities, lawyers' offices and media outlets. It would be almost impossible to find a business in Canada that does not create, store or transmit information in electronic form.

The CBA Sections are concerned that the government could impose lawful access technical capacities for all aspects of digital life. The definition of electronic service provider should be strictly limited to those who principally provide communication services to the public.

C. Core Providers and Ministerial Orders (ss.5-13)

These sections empower the government to require ESPs to develop, test, implement, operate and monitor lawful access technical capabilities to provide access to information in relation to their electronic services. Section 5 empowers the Governor-in-Council (GiC) to make regulations establishing lawful access technical capabilities for "core providers" a subset of ESP that is defined by the GiC in subsequent regulations. The CBA Sections are concerned by the absence of procedural safeguards for this new and far-reaching power. Section 5 has no obligation to consult or a proportionality test. While section 5(3) lists factors to consider, transparency about their consideration in not required.

An ESP can apply for a temporary exemption, but otherwise, there is no oversight or review process other than judicial review. Any power to impose lawful access technical capabilities should be accompanied by proportionate procedural safeguards.

Section 5 also lacks a process to compensate for costs arising from imposing lawful access technical capabilities. If an ESP lacks a particular capability, it is typically because it has no legitimate business need for it. As a result, lawful access technical capabilities required under s. 5 are capabilities and costs that will generally only be incurred to facilitate lawful access to information. This represents a transfer of investigative costs that traditionally rest with LEAs to

ESPs in the private sector. The CBA Sections are concerned about the impact on ESPs and increased lawful access activity if LEAs ignore costs of their activities.

s. 5(2)(a) – Capabilities

By requiring providers to build and maintain interceptions or data production capabilities, the Bill mandates the existence of a privileged access point within otherwise secure systems. The term broadness creates ambiguity in required technical architecture: compliance uncertainty for smaller providers, excessive regulatory discretion and complex compliance assessment.

While the government has said that Bill C-22 does not permit backdoors, a plain reading of s. 5(2)(a) and the lack of guardrails says otherwise.

s. 5(2)(b) – Devices and equipment

SAAIA should not permit the government, via regulation or Ministerial Order, to require the installation of specific equipment or devices on providers' systems. Diligent companies must have full awareness and control of any equipment or devices associated with its infrastructure. An open-ended obligation to install equipment for surveillance is unreasonable and introduces significant cybersecurity risks for ESPs.

s. 5(2)(c) – Notices to the Minister or other persons

GiC regulations and Ministerial Orders may require ESPs to give notice to the Minister or other person about capabilities and any device, equipment or other thing. The CBA is concerned that this mirrors the powers contained in the UK's lawful access law (the *Investigatory Powers Act 2016* (IPA), significantly expanded by the *Investigatory Powers (Amendment) Act 2024*.

It is entirely lawful, and should remain so, for a company to make changes to its systems that both (a) increase the security of its users' information, and (b) reduce the ability of the company to provide access to user information. Many of the most popular messaging apps in the world have introduced "end to end encryption", which increases the security of user data and means that law enforcement no longer has access to text messages from the service provider.

s. 5(2)(d) – Retention of categories of metadata

Bill C-22, unlike C-2, allows core providers and ESPs subject to ministerial orders to retain metadata for up to one year. Section 5(4) limits data retained, but metadata includes very sensitive information, such as location data. This is a dramatic expansion from Bill C-2.

In Europe, mandatory metadata retention was deemed a privacy rights intrusion when the European Court of Justice struck down the EU *Data Retention Directive* in 2014,[16] holding that the general and indiscriminate retention of all users' telecommunications metadata was a disproportionate interference with privacy and data protection rights. The Directive required member states to mandate retention for between six and twenty-four months. In the years since, the CJEU has progressively clarified that while targeted retention linked to specific threats or geographic areas can be lawful, blanket retention of all users' data remains incompatible with EU fundamental rights. This will likely be challenged as a violation of s. 8 of the *Charter*.

D. Ministerial orders

Section 7 empowers the Minister of Public Safety and Emergency Preparedness to issue Ministerial Orders imposing obligations on ESPs, similar to the GiC regulations, with some procedural safeguards. These include considering the impact on justice administration, the feasibility for ESPs, and the impact on service users. Intelligence Commissioner approval is required, but affected ESPs have no right to make representations, and there is no transparency about the factors considered. This lack of criteria and meaningful and proportionate procedural safeguards is a significant concern for the CBA Sections.

Currently, the police and CSIS can apply to a judge for an "assistance order" requiring service provider assistance for a warrant, potentially with a non-disclosure order. These orders are tailored to the particular warrant, the provider and the nature of the assistance required. The judge would consider the impact of the *Charter* in the issuance of the assistance order. A judge under both the *Code* and the *CSIS Act* is able to have an amicus appointed to consider the impact of the order on third parties. Assistance orders are, by definition, subject to judicial supervision and control. This is effectively being replaced by Ministerial Orders with no judicial oversight.

The CBA notes that there is no evidence that assistance orders under the *Code* or *CSIS Act* are inadequate and recommends that Ministerial Orders should be removed from the Bill.

E. Systemic Vulnerability (ss. 5(3) and 7(4))

Both GiC regulations and Ministerial Orders state a provider can bypass a provision if complying would "introduce a systemic vulnerability in electronic protections related to that service or prevent the provider from rectifying such a vulnerability." Despite government claims not to undermine encryption, similar laws in other jurisdictions have been used to undermine

16 EU Data Retention Directive, online.

encryption, as reportedly occurred with Apple under the UK regime.[17] This should not be permitted in Canada.

The definition of systemic vulnerability in the Bill is insufficient to meaningfully constrain risk. The current definition only addresses unauthorized third-party access, not data integrity, availability, or limits vulnerabilities related to a device, software or operating system. "Systemic vulnerabilities" should make it clear that an obligation to undermine or circumvent encryption is prohibited, and it should be clear that vulnerabilities are not just related to unauthorized access, and not just related to "services". Specifically, the CBA proposes the following definition of "systemic vulnerability":

> ***systemic vulnerability*** means a vulnerability in electronic protections that creates a substantial risk to the confidentiality, integrity, or availability of information, services or systems.

And amend paragraphs 5(5) and 7(5) to clearly carve out encryption:

> (5) A [core provider/ electronic service provider] is not required to comply with a provision of [a regulation made under subsection (2)/an order], with respect to an electronic service, if compliance with that provision would require the provider to introduce a systemic vulnerability related to that service, or prevent the provider from rectifying such a vulnerability, or require the provider to remove, circumvent or undermine the encryption of information.

F. Government should accept the risk that it is proposing to create

By mandating backdoors and expanded data retention, SAAIA would create valuable targets for malicious actors. The *Communications Assistance to Law Enforcement Act* in the U.S. required similar backdoors, exploited by foreign hackers to obtain U.S. data.[18] Canada faces the same risk if it imposes similar requirements.

Retaining metadata conflicts Canadian privacy laws, which limits retention to necessary and reasonable business purposes. Metadata under SAAIA lacks business purpose, risking privacy laws and best practices violations and attracting cyber criminals.

Overall, the regime should specify the factors, eligible costs, and guidance for calculating compensation. Many ESP capital expenditures under Part 2 will serve no business purpose and will be solely for lawful access. If these costs benefit society, they should be covered by

---

17 The Guardian, UK government resumes row with Apple by demanding access to British users' data, (1 October 2025) online.

18 Wall Street Journal, "U.S. Wiretap Systems Targeted in China-Linked Hack: AT&T and Verizon are among the broadband providers that were breached" (5 October 2024) online.

government revenues rather than imposed on certain ESPs. In addition, SAAIA should compensate to ESPs and affected individuals for losses associated to compliance, including data breaches from government-mandated backdoors.

G. Obligation to Assist

Section 14 grants numerous national security individuals the authority to request information from ESPs. Allowing anyone – civilian or otherwise – within agencies such as the RCMP and CSIS to request information under Part 2 is excessive. The scope and the types of information that can be requested under such a disclosure obligation should be narrowed.

H. Judicial Review

Sections 16 and 17 lack accountability and rule of law. Section 16 minimizes ESPs' right to challenge orders by imposing a 15-day advance notice of application for judicial review to be attached to a formal letter to the Minister. Section 16 lacks a clear right to challenge the government.

I. Mandatory confidentiality

The confidentiality outlined in s. 15 of SAAIA are overbroad and unjustified. Every ESP under a Ministerial Order is prohibited from disclosing to anyone order's existence. Companies should be transparent about their products, unless there is a clear law enforcement or national security imperative.

Experience in the UK shows a similar law to secretly require Apple to remove encryption on certain of its core/key products. US companies should be able to seek the US government's assistance in resolving problematic orders. The Minister should justify, on a per-order basis, the need for secrecy associated with these orders, and any confidentiality requirements should sunset. These orders should be subject to judicial review, where the Minister would have the onus of satisfying the court that the secrecy order is reasonably necessary in order to protect public safety or national security. Non-Canadian companies, particularly from a "Five Eyes" country, should disclose orders to their home jurisdiction counterpart.

Section 18 suggests further confidentiality rules that could limit information sharing, potentially affecting ESP's security clearance programs. The anticipated government overreach in these sections is unreasonable and suggests excessive regulatory control. Judicial review should not be so blocked and advance notice along with section 17, which adds ambiguity to limit disclosure of access requests, should be removed.

J. Inspection powers

Sections 19-21 echo the intrusive investigative powers of the CCSPA (Bill C-8) affording Minister and designated persons with powers of entry - from "examining anything" on-site to removing "any document, record or cyber system, or a portion of it" for the purpose of reviewing or copying it.[19]

These powers – and sections – enable warrantless investigations for ESPs, allowing examination and copying of documents, with an obligation to assist. A threshold of reasonable and probable grounds should be required before entry, balancing the broad powers and lack of liability during investigations. Inspections should (a) require notice to the ESPs, (b) be carried out during ordinary business hours, (c) inspectors should have to satisfy the ESP's reasonable security and operational requirements and (d) they should be carried out in a manner designed to minimize impacts on the ESP's operations.

K. Audits (s.21)

To verify SAAIA compliance, designated person may order internal audit by ESPs. The ESP must comply without independent review or oversight and no assurance of confidentiality for the resulting report, including any personal information it contains. The CBA Sections believe that further procedural safeguards are required for this audit power, including an independent review of the Audit order and handling of information.

VI. PRIOR CBA RECOMMENDATIONS

A. Codify Purpose Limitation and Data Minimization Principles

The CBA Sections recommend any use of information collected by law enforcement or national security authorities be limited to specific, statutorily defined purposes connected with the purposes for which was collected, with explicit prohibitions on secondary use beyond the initial authorization. For example, computer data retained by the government pursuant to Part 1 of the Bill should not be used for any other purpose except to advance the investigation for which the data was initially seized. Data collection and retention must be proportional and necessary to a legitimate governmental objective[20].

---

19 See, for example, CCSPA, ss. 49-50.

20 Reference: OBA Submission on Privacy Guidance on facial Recognition for Police Agencies (15 October 2021)

B. Ensure Cross-Statute Consistency with Privacy Laws

The new Act should not override privacy rights or accountability mechanisms in other statutes. The CBA Sections recommend legislative language affirming that existing privacy protections under federal and provincial legislation remain fully applicable[21].

C. Mandate Independent Oversight and Reporting

The CBA supports annual public reporting obligations to Parliament and an oversight mechanism such as the Privacy Commissioner, the National Security and Intelligence Review agency, or another designated tribunal, to audit compliance, review complaints, and investigate overreach or misuse.

D. Require Transparent Regulation-Making Process

The Act delegates significant authority to future regulations; therefore, the CBA Sections recommend public and stakeholder consultation, particularly from privacy, legal, and civil liberties organizations.

VII. CONCLUSION

Bill C-22 has significant implications that affect Canadians' privacy, safety and cybersecurity interests. The recommendations put forward by the CBA are intended to be a good faith contribution to Parliament's important deliberations in crafting laws that are effective, understandable and consistent with the *Charter*.

---

21 CBA Resolution 15-04-M: Independent Oversight of Canada Border Services Agency (February 21-22, 2015); CBA Submission on Security of Canada Information Sharing Act (SCISA) (January 2017)