Bill C-22:
New Powers, Old Problems

Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC)

About CIPPIC

The Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic (CIPPIC) is Canada's first and only public interest technology law clinic. Based at the Centre for Law, Technology and Society at the University of Ottawa's Faculty of Law, our team of legal experts and law students works together to advance the public interest on critical law and technology issues including privacy, free expression, intellectual property, telecommunications policy, and data and algorithmic governance.

Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic
University of Ottawa, Faculty of Law
57 Louis Pasteur St.
Ottawa, Ontario, K1N 6N5
Canada

Authors: Aaranya Alexander, Jennifer Turliuk, and David Fewer

For more information, visit our website at www.cippic.ca.

CIPPIC

Table of Contents

Executive Summary

Bill C-22 gives the state broad access to the digital lives of Canadians without the legal justification, standards or safeguards needed. Powerful investigative tools for serious crimes cannot come at the expense of the privacy and freedoms of innocent people.

Committee hearings and the consultation process must be extended. CIPPIC is deeply concerned about the expedited process of Bill C-22 given its broad mandate and potential implications on Canadians. Civil society has had inadequate time to meaningfully comment and contribute to the Committee's review.

The *Supporting Authorized Access to Information Act* should not proceed absent major structural revision, independent oversight safeguards, and a demonstrated evidentiary basis. The overbroad scope maintained throughout this Bill risks pulling ordinary businesses into surveillance duties and allowing access to personal data without clear limits. Metadata is more deeply revealing than the Government admits, and the Bill does not clearly define what capabilities can be compelled or how they interact with constitutional protections. Secret orders and limited review leave Canadians unaware of when their information is accessed and unable to monitor how these powers expand.

The use of surveillance tools in any security context must be necessary, targeted, and proportionate. Lawful access legislation must stem from concrete gaps in existing capabilities. The government must be on the same page with the industry, judiciary, and on privacy interests associated with certain data.

The substantive recommendations follow these general themes:

- **Higher legal thresholds:** Access to sensitive data requires meaningful justification corresponding to a concrete threat of wrongdoing, even in exigent circumstances and national security situations.
- **Stronger oversight and transparency:** Surveillance powers are exceptional. They must be limited ex-ante and monitored ex-post to identify patterns of overreach and create new safeguards. Law enforcement must seek independent authorization and conduct reporting. Providers must have appropriate recourse to contest actions.
- **Narrower scope and clearer definitions**: Law enforcement powers must be sufficiently targeted and tied to legitimate investigative needs. They cannot have free discretion to subject ordinary companies to burdensome regulations at unilateral definitions of urgency, user safety and technical vulnerability. Users and companies must be fully informed on what regulations they may be subject to.

Summary of Recommendations

CONFIRMATION OF SERVICE DEMAND

1.1 Raise the threshold to "reasonable grounds to believe."

1.2 Remove the officer's unilateral power to impose non-disclosure; require a court order.

1.3 Require record-keeping and annual public reporting.

SUBSCRIBER INFORMATION PRODUCTION ORDER

2.1 Raise the threshold to "reasonable grounds to believe."

2.2 Narrow "subscriber information" to basic identifying data only.

2.3 Require judges to specify subscriber information categories to be produced.

2.4 Limit use to serious offences or require a necessity finding.

2.5 Require record-keeping and annual public reporting.

TRACKING AND TRANSMISSION DATA WARRANTS

3.1 Define "similar thing" and "similar means of telecommunication" narrowly.

3.2 Require police to return to court to expand surveillance capability.

3.3 Require *ex post* reporting to the issuing judge or justice.

FOREIGN ENTITIES PRODUCTION ORDER

4.1 Add transparency and scope controls to the foreign request mechanism.

PUBLICLY AVAILABLE INFORMATION

5.1 Define "available to the public" narrowly (ex. purchase & unlawful access).

5.2 Narrow the immunity provision.

5.3 Require record-keeping of voluntary disclosures and public information.

ABSENCE OF JUSTIFICATION & PROCEDURAL CONTROVERSY

6.1 The *SAAIA* should not proceed as tabled.

6.2 Extend Committee hearings to meaningfully address all concerns.

6.3 Require a systematic evidentiary record from the government.

CORE PROVIDER OBLIGATIONS

7.1 Limit core provider obligations to specific lawful access authorities

7.2 Require mandatory consultation on technical feasibility with industry & OPC.

7.3 Document the balancing and consultation process.

7.4 Clarify the scope & procedure for invoking a systemic-vulnerability exception.

SERIOUSNESS OF METADATA & SURVEILLANCE IMPLICATIONS

8.1	Remove *s. 5(d)* to eliminate all metadata-retention regulations.
8.2	Replace the retention power with targeted preservation orders.
8.3	Identify the substantive data & technical capacities that create investigative barriers. Clarify technical terminology with all actors.
8.4	Build knowledge to effectively use existing digital evidence and procedures.

MINISTERIAL ORDERS

9.1	Remove ministerial orders or require judicial authorization.
9.2	Narrow "electronic service provider", with exclusions and threshold on users.
9.3	Define a high threshold for a ministerial order (e.g. exigent circumstances, national security)
9.4	Clarify the scope and procedure for the systemic-vulnerability exception.
9.5	Require secrecy to be justified order-by-order, with a sunset clause.

OBLIGATION TO ASSIST

10.1	Define the scope of assistance, testing duration, & frequency limits.
10.2	Require written necessity, proportionality & exhaustion of alternatives.
10.3	Appoint an independent technical assessor for oversight.
10.4	Require record-keeping and annual reporting.
10.5	Create an express right to challenge an assistance request.

CONFIDENTIALITY & PROHIBITION ON DISCLOSURE

11.1	Require independent judicial approval for all secrecy orders.
11.2	Impose a 1-year sunset on confidentiality; renewal requiring new approval.
11.3	Create a safe harbour for aggregate transparency reporting.
11.4	Remove authority to amend limits and safeguards on disclosure & oversight.
11.5	Preserve the right to consult security-cleared independent legal counsel.

ENFORCEMENT: COMPLIANCE, AUDIT & INSPECTION ORDERS

12.1	Narrow the scope of warrantless entry, require judicial authorization based on "reasonable grounds to believe a provider is or is likely to contravene the Act.
12.2	Add rules for sealing and destruction of personal information retrieved by enforcement actions, with exceptions authorized by a judge.
12.3	Create independent review mechanisms for all enforcement actions.
12.4	Strengthen documentation and assessment of all enforcement actions in the annual reporting procedure.

Introduction

Bill C-22 creates a new lawful access architecture.[1] "Lawful access" refers to legal powers that let police and security agencies obtain digital evidence from telecommunications and online service providers. The debates over lawful access focus on:

- **New Powers:** state access to basic subscriber-identifying information, preserved data, metadata, communications content, and intercept capabilities;
- **Deputizing Private Actors:** obligations imposed on telecommunications and online service providers to facilitate that access, including by preserving data, producing records, or building access capabilities; and
- **Oversight and Accountability:** the constitutional safeguards that should govern these powers, including judicial authorization, proper grounds, transparency, and limits on what service providers must collect, build, retain, or disclose.

Civil society organizations, cybersecurity experts, academics, and industry groups raise four broad concerns about Bill C-22:

- **Privacy and *Charter* rights:** The Bill lowers thresholds for subscriber information and creates suspicion-less metadata retention that may expose users' movements, associations, identities, and service use.
- **Encryption and cybersecurity:** The Bill may require technical capabilities that weaken encryption, create systemic vulnerabilities, or turn lawful access infrastructure into a target for criminals and foreign adversaries.
- **Secrecy and accountability:** The Bill relies on confidential ministerial orders, broad non-disclosure duties, and delayed review, leaving too little public transparency or real-time independent oversight.
- **Overbreadth and cost:** The Bill may capture a wide range of electronic service providers, impose expensive technical and retention duties, and shift surveillance costs and security risks onto providers and users.

Part 1 of the Bill expands legal powers to obtain data. Part 2 creates technical and operational obligations so providers can make that access possible. Part 3 requires Parliament to review the scheme later. Modern digital investigations present real operational challenges for law enforcement, including encryption, evolving communications technologies and device-switching. Addressing these challenges requires structuring new law enforcement powers in a manner consistent with constitutional safeguards, accountability, cybersecurity, and proportionality.

---

[1] Bill C-22, *An Act Respecting Lawful Access*, 2025, 45th Parl, 1st Sess 2026, https://www.parl.ca/Content/Bills/451/Government/C-22/C-22_1/C-22_1.PDF. [*Lawful Access Act*]

Bill C-22 Part 1: Timely Access to Data and Information

1) Confirmation of Service Demand

Bill C-22, s.5 (proposed Criminal Code, s. 487.0121)

Background

The current law requires law enforcement to obtain subscriber information from telecommunications service providers through a judicially authorized production order. That process requires police to satisfy the "reasonable grounds to believe" standard before compelling disclosure of personal information.

The proposed *s. 487.0121* of the *Criminal Code* would allow law enforcement to require a telecommunications service provider to confirm whether it provides, or has provided, services to a specific subscriber, client, account number, or other identifier. The change does two things: it removes prior judicial authorization and lowers the threshold from "reasonable grounds to believe" to "reasonable grounds to suspect."

This is an improvement over Bill C-2[2], which would have let police compel subscriber-identifying information directly, without prior judicial authorization. Bill C-22 narrows that power to a yes-or-no confirmation that helps police identify the correct provider before seeking a court order.

Justification

The government claims that this is a process issue: that it is too slow and inefficient to obtain a warrant for simple confirmation of service demands.[3] A confirmation of service demand allows law enforcement to identify the correct provider before applying for a production order.[4] It avoids the wasted time and resources of seeking a production order from a provider that does not serve the person, account, or identifier in question.

The Problem

The "reasonable grounds to suspect" threshold is too low for a warrantless demand. This creates two problems.

---

[2] Bill C-2, *An Act respecting certain measures relating to the security of the border between Canada and the United States and respecting other related security measures,* 45th Parl, 1st Sess, 2025, https://www.parl.ca/DocumentViewer/en/45-1/bill/C-2/first-reading

[3] Canada, *House of Commons Debate*s, 45th Parl, 1st Sess, Vol 152, No 106 (20 April 2026), https://www.ourcommons.ca/Content/House/451/Debates/106/HAN106-E.PDF at p. 7164. [House of Commons, *Hansard* 20 April]

[4] House of Commons, *Hansard* 20 April at p. 7170.

- **Privacy:** Confirmation of service for discrete individuals carries a privacy risk which may be in violation of the *Charter* right to be free from search and seizure, and recognized rights to privacy and online anonymity. The demand could allow law enforcement to, without judicial authorization:
    - establish links between any person and private services;
    - identify services used by a person in the past; and
    - map relationships among subscribers, accounts, identifiers, and providers.

  The Bill recognizes that confirmation itself may reveal personal information that has implications for a person's privacy: it prohibits a demand where confirmation would reveal privileged or medical information in *s. 487.0121(3)*.

- **Oversight and accountability:** The demand lacks the main safeguard that normally governs compelled access to private information: prior authorization by a judge. The service provider may seek review, but that is an after-the-fact, recipient-driven safeguard. It does not require law enforcement to justify the demand before an independent decision-maker prior to issuing it.

  The affected person may also never know that the demand was made, as *s. 487.0121(5)* allows the requesting officer to attach non-disclosure conditions to the demand. That weakens accountability because the person whose service relationship has been confirmed cannot challenge the demand, contest the grounds, or know how often the power is used.

Recommendations

1.1 Raise the threshold from "reasonable grounds to suspect" to "reasonable grounds to believe" for a warrantless demand to confirm service (*s. 487.0121(1)*).

Rationale: The higher threshold preserves the practical value of the confirmation of service demand without widening warrantless access to private information. The demand helps law enforcement identify the correct provider before applying for a production order.

Production orders already use the "reasonable grounds to believe" standard for access to personal data held by telecommunications companies. Applying the same standard to a confirmation of service demand would not prevent law enforcement from efficiently identifying the right provider. It would simply prevent the state from using a lower threshold to obtain privacy-revealing confirmations without judicial authorization.

1.2 Remove the requesting officer's power to impose non-disclosure directly (*s. 487.0121(6)*). If secrecy is needed to avoid jeopardizing the investigation, police should seek a court order.

Rationale: The officer who seeks the information should not also control its secrecy, else the investigator decides both access and concealment. A judge adds an independent check, forces police to justify secrecy on the facts, and keeps non-disclosure tied to necessity rather than convenience. Any restriction on speech, notice, or transparency should come from a court.

1.3 Require record-keeping: require every demand to be logged with the issuing agency, its statutory basis, the identifier searched, the provider served, the response received, and whether a gag order was sought or granted.

Require annual public aggregate reporting: number of demands issued, number granted voluntarily, number refused, number challenged, number varied or revoked, number with gag orders, average response time, and breakdown by offence category.

Rationale: Transparency is the best guarantee of accountability. It makes hidden powers measurable. Record-keeping creates an audit trail for supervisors, courts, review bodies, Parliament, and the public. Aggregate reporting protects investigations while exposing patterns: overuse, mission creep, regional inconsistency, excessive secrecy, or high refusal and challenge rates. It also lets Parliament test whether the power has remained a narrow tool for identifying the right service provider or has become a routine workaround for judicially authorized production orders.

2) Subscriber Information Production Order

Bill C-22, s.6 (proposed Criminal Code, s. 487.0142)

Background

Current law permits police to obtain subscriber information through a general production order. That route requires judicial authorization and the "reasonable grounds to believe" standard. Bill C-22 creates a dedicated subscriber information production order. It still requires a judge or justice, but it lowers the threshold to "reasonable grounds to suspect." The existing general production order has already given police a workable route to link an IP address, phone number, or account identifier to a subscriber. The government has not shown why subscriber-identifying information now requires a lower standard.

The proposed order would compel a person who provides services to the public to produce all subscriber information that relates to specified information, including transmission data. Subscriber information includes identifying information, account identifiers, service types, service periods, and information identifying devices, equipment, or things used in relation to the service. The order applies beyond telecommunications providers. It can reach any person or entity who provides services to the public, including medical clinics, hotels, banks, grocery stores, cloud providers, online platforms, and device ecosystems.

Justification

The government treats subscriber information as a lower-sensitivity category because it does not include the contents of communications. It also argues that a dedicated order gives police a faster and clearer route to identify the person or account connected to an online identifier.[5] That justification overstates the distinction between content and subscriber information. Subscriber information can still expose sensitive facts about identity, location, associations, services used, devices owned, and relationships between accounts.

The Problems

The order combines a low threshold with a broad definition. It also creates an all-or-nothing production model: the order produces "all the subscriber information" that relates to the information specified on application, not only the subset needed to identify the subscriber.

---

[5] Canada, *House of Commons Debates*, 45th Parl, 1st Sess, Vol 152, No 103 (15 April 2026), https://www.ourcommons.ca/Content/House/451/Debates/103/HAN103-E.PDF at 6968. [House of Commons, *Hansard* 15 April]

- **Privacy:** Subscriber information can reveal more than a name and address. It can expose service types, service periods, account identifiers, device identifiers, and relationships between people, devices, accounts, and services. In practice, it could reveal a patient's medical service or device, a customer's cable package, a person's iCloud account relationships, the identifiers for phones, tablets, laptops, AirTags or Alexa devices and service histories that go well beyond basic identification.
- **Threshold:** The lower "reasonable grounds to suspect" standard gives police access to identity-linked information before they can meet the ordinary production order threshold. The order applies to any offence under the *Criminal Code* or any other federal Act, not only serious crimes. A low threshold may be more defensible for a narrow identity check but is much harder to justify when the order can compel broad service, device, and account information.
- **Scope:** The phrase "all the subscriber information" begs overcollection. It may give police more than they need to link an IP address, phone number, or account identifier to a named person. The Bill's own tracking and transmission data provisions show a narrower solution: where subscriber information relates to transmission data, the Bill refers only to paragraph (a)[6] identifying information.[7] That model undercuts the need for this order to reach service types, service periods, account ecosystems, and device inventories.
- **Oversight and accountability:** Judicial authorization helps, but it does not solve the breadth problem if the statute gives the judge an all-or-nothing choice. The judge should have to specify the categories of subscriber information that police may obtain, and the application should explain why each category is necessary for the investigation. The order should also require minimization, logging, and reporting so Parliament can see how often police use the new, lower threshold tool and what kinds of information it produces.

Recommendations

2.1 Raise the threshold to "reasonable grounds to believe" in *s. 487.0142(1)*.

Rationale: Subscriber information now sits at the centre of modern privacy. It links people to online activity, devices, services, locations, and associations. The state should not obtain that information on the lowest threshold in criminal law. Accordingly, subscriber

[6] From the definition of "subscriber information": (a) information that may be used to identify the subscriber or client, including their name, pseudonym, address, telephone number and email address, in *Lawful Access Act* at s. 4(2).
[7] *Lawful Access Act* at s. 20, creating s. 492.2(1.1) of the *Criminal Code*.

information should remain subject to the standard of a general production order. A "reasonable grounds to believe" standard preserves access where police or CSIS can justify it and aligns such orders with the privacy interests the courts already recognize in subscriber-identifying information. The existing general production order already gives authorities effective and accessible means to obtain subscriber information. The privacy risk grows in the intelligence context because affected persons may receive no subsequent criminal process in which they can challenge the intrusion.

2.2 Narrow the definition of "subscriber information" in *s. 4(2)* of Bill C-22 to the basic identifying information needed to connect a specific identifier to a person or account.

Rationale: Police do not need every service type, device identifier, or account relationship to identify the subscriber behind an IP address or similar identifier. A narrower order would give police the routing and identification function they need while avoiding unnecessary disclosure of private services, use of cloud ecosystems, devices, or services. This narrower model would also reduce the risk that a subscriber information order becomes a shortcut to information that carries a higher privacy interest than basic identification.

2.3 Require judges to specify the categories of subscriber information that may be produced. At minimum, the order should default to name, address, contact information, and the specific account or identifier at issue. It should exclude service types, service periods, and device, equipment, or thing identifiers unless the judge expressly finds that the additional category meets the higher standard and is necessary for the investigation.

Rationale: The judge should not face an all-or-nothing order. Judicial authorization only protects privacy if the judge can tailor the production to the investigative need. Requiring the order to specify categories of data would reduce overbreadth and force police to explain why each category matters.

2.4 Limit use of the order to serious offences or require an additional necessity finding where police seek anything beyond basic identifying information.

Rationale: A lower-threshold production order should not apply with equal force to serious crimes and minor federal regulatory offences. If Parliament keeps a dedicated subscriber information order, it should either restrict the power to serious offences or require police to show why ordinary production order powers will not meet the investigative need.

2.5 Require record-keeping and annual public reporting. Each order should be logged with the issuing agency, statutory basis, offence category, identifier searched,

provider served, categories ordered, response received, review application, and whether a non-disclosure order was sought or granted. Public reporting should disclose aggregate numbers, categories, providers by class, offence categories, and review outcomes.

Rationale: The new order lowers a long-standing threshold for a high-volume investigative tool. Record-keeping and public reporting would not compromise investigations, but would allow Parliament, courts, providers, and the public to see whether the power remains confined to identification or expands into mapping of services, devices, and account ecosystems.

3) Tracking and Transmission Data Warrants

Bill C-22, s.19 and s. 20 (proposed Criminal Code, s. 492.1(2.1), s. 492.2(1.1))

Background

Current law allows police to seek judicial warrants for tracking data and transmission data. Bill C-22 expands what those warrants provide. A tracking warrant could authorize police to collect tracking data for a known thing that a person uses, carries, or wears, and also for an unknown "similar thing", if the judge or justice has reasonable grounds to suspect that the person will use, carry, or wear it. The Bill makes a parallel change for transmission data, allowing a warrant to cover an unknown means of telecommunication of a similar type.

Justification

The government's rationale is continuity. A target may switch devices or communications methods during an investigation. A warrant limited to the device or method known at the time of application may lose value as soon as the target changes tools.[8]

The Problems

- **Privacy:** Tracking data and transmission data can reveal movements, routines, contacts, and associations.
- **Vagueness:** The word "similar" does not clearly define the outer boundary of the warrant.
- **Judicial control:** Loose warrant language risks turning authority over one known thing or communications method into rolling authority over unknown future substitutes.

Recommendations

3.1 Amend *ss. 19* and *20* to define "similar thing" and "similar means of telecommunication" narrowly. The warrant should identify the class of thing or communications method covered, the factual basis for believing the person will use it, the permitted period of collection, and any limits needed to protect third-party privacy.

3.2 Require police to return to court where the new thing or communications method materially expands the surveillance authorized by the original warrant.

[8] Government of Canada, "Charter Statement -- Bill C-22: An Act respecting lawful access", (24 April 2026), https://www.justice.gc.ca/eng/csj-sjc/pl/charter-charte/c22_2.html.

3.3 Require post-execution reporting to the issuing judge or justice. The report should identify each unknown thing or communications method monitored under the warrant, the basis for treating it as similar, the dates of collection, and any third-party information captured.

Rationale: These amendments preserve the legitimate investigative goal. Police should not have to restart the warrant process every time a target moves to a clearly connected substitute. But Parliament should not let a warrant for one known device or communications method become open-ended authority to follow a person across future tools. A narrow definition, mandatory warrant terms, a return-to-court trigger, and post-execution reporting would preserve judicial control while still allowing investigators to respond to device-switching and communications method switching.

4) Foreign Entities Production Order

Bill C-22, s. 7 (proposed Criminal Code, s. 487.0181(1))

Background

Bill C-22 creates a new judicial authorization that allows a peace officer or public officer to ask a foreign service provider to produce transmission data or subscriber information. A judge or justice must first find reasonable grounds to suspect that an offence has been or will be committed and that the requested data or information is in the foreign entity's possession or control and will assist the investigation. The request must be sent within 30 days.

Justification

This provision offers a useful solution to cross-border information access problems because it gives foreign providers evidence of Canadian judicial authorization.[9]

The Problem

The provision features many of the same shortcomings of the other lawful access powers of Bill C-22:

- **Low threshold:** The request may seek subscriber information or transmission data on reasonable grounds to suspect. Subscriber information can include service types and device identifiers, not just a name and address, and may carry a meaningful privacy interest.
- **Limited transparency:** The Bill does not require public reporting on how often officers use this power, which categories of data they request, which foreign jurisdictions receive requests, how often providers comply, or how often requests rely on foreign law or treaty-related requirements.
- **Scope control:** Because the request may include information required by the foreign provider, foreign state, or an international arrangement, the Bill should make clear that those additions cannot expand the substance of what the Canadian authorization permits.
- **Cross-border architecture remains under-explained:** The government has offered little in the way of explanation for how this power will relate to the US *CLOUD Act* and the Council of Europe's *Second Additional Protocol to the Convention on Cybercrime*.

[9] Department of Justice Canada, "Proposed changes to laws on timely access to information (Bill C-22 - Part 1): 4. Cooperation requests with international partners", (24 March 2026), https://www.justice.gc.ca/eng/csj-sjc/pl/c22/#s4.

Recommendations

4.1 Retain the foreign request mechanism in *s. 7*, but add transparency and scope controls:

i) Require requests for subscriber information that go beyond basic identifying information to state reasonable grounds to believe, consistent with the broader subscriber information recommendation.

ii) Require the request to state clearly that it is a request, not a Canadian production order enforceable against the foreign provider.

iii) Require the request to stay within the specific data categories authorized by the Canadian judge or justice.

iv) Require officers to record the provider, foreign state, offence category, data sought, legal basis, whether the request included information required by foreign law or an international arrangement, and the response received.

v) Require annual public aggregate reporting on foreign production requests, including request volume, data categories, country categories, provider categories, compliance rates, and refusals.

Rationale: This approach gives Parliament and the public a way to see how the foreign request mechanism operates. These recommendations ask for modest safeguards so a useful cross-border request mechanism does not become an unreported and poorly understood access channel.

5) Publicly Available Information

Bill C-22, s. 11 (proposed Criminal Code, s. 487.0195)

Background

Bill C-22 states that peace or public officers do not need a warrant, production order, or confirmation of service demand to receive, obtain, and act on information that is "available to the public."

Justification

Police need clarity that they do not need a warrant to observe or use genuinely public information, such as information posted openly on a public website, public registry, or public-facing social media page.[10]

Problems

Digital information can be accessible in practice while remaining private in substance. Information may be hacked, leaked, scraped, purchased, brokered, or assembled from commercial surveillance markets. Location data, device identifiers, service records, IP-linked information, private messages, emails, photos, and chat logs can reveal intimate details about identity, movements, associations, and private life. Bill C-22 should not allow the state to treat that information as accessible without a warrant merely because someone can obtain it. To do so risks laundering privacy-invasive data through accessibility. Voluntary disclosure does not eliminate privacy interests.

The immunity provision may encourage disclosure in legally uncertain cases. If disclosure is clearly lawful, immunity adds little. If disclosure is doubtful, immunity may push recipients toward cooperation rather than careful review of privacy consideration. The provision may thus weaken privacy promises made to users. Service providers, platforms, businesses, or other custodians may tell users that information will be disclosed only when legally required. An overly broad statutory immunity for voluntary disclosure may undermine those assurances.

Recommendations

5.1 Define "available to the public" narrowly to include only information that a person intentionally makes available to the general public, without circumvention, breach of confidence, unlawful access, scraping, brokerage, or commercial purchase. The definition should expressly exclude:

[10] Department of Justice Canada, "Proposed changes to laws on timely access to information (Bill C-22 - Part 1): 2. Clarifications", (24 March 2026), https://www.justice.gc.ca/eng/csj-sjc/pl/c22/#s2_1.

i) location data, device identifiers, service-use data, and other information that can reveal movements, associations, identity, or patterns of life;

ii) hacked or leaked data; and

iii) scraped, brokered, and commercially purchased personal data.

Rationale: Personal information should not become accessible without a warrant because someone else exposed it, aggregated it, or sold it.

5.2 Narrow the immunity provision in the proposed *s. 487.0195(2)* of the *Criminal Code*.

Rationale: Immunity should not encourage custodians of personal information to disclose in legally uncertain circumstances. The provision should protect good faith acts in emergencies or legally required disclosures, prohibit routine voluntary cooperation that bypasses judicial authorization.

5.3 Require record-keeping of voluntary disclosures and reliance on public information.

Rationale: Officers should record what was received or obtained, the source, the basis for treating it as voluntary or publicly available, and whether the information included personal data. This ensures accountability without blocking legitimate investigations.

Bill C-22 Part 2: *Supporting Authorized Access to Information Act (SAAIA)*

6) Absence of Justification and Procedural Controversy

Background

The *SAAIA* is an interceptability mandate that obligates electronic service providers (ESPs) to build surveillance infrastructure and capabilities into their systems. ESPs include any entities that provide services which incorporate use of digital information, thus including most Canadian businesses. A category of ESPs called "core providers" will need to follow regulations to help with lawful access orders. These regulations may mandate the retention of metadata – the information surrounding content - like who a customer called and texted, their location, their time and duration of use, and other features.

ESPs, even if not core providers, may be subject to secret Ministerial orders to maintain lawful access capability. A service provider does not have to comply with the order if it would introduce a "systemic vulnerability" - one that creates "a substantial risk that secure information could be accessed by a person who does not have any right or authority to do so". This safeguard is not adequately described and may not extend to fully protect devices or encryption.

The *SAAIA* also includes a new "reasonable assistance" obligation for internet service providers to assist police with lawful actions and a suite of audit and enforcement provisions.

Law enforcement is currently able to get special wiretap orders. With the *SAAIA*, they could mandate the capability to plug directly into ESPs' systems to give effect to intercept orders, creating a 'back door'. There is a risk that external bad actors may try to exploit this back door, like Chinese hacker group "Salt Typhoon" breaching US lawful access infrastructure, resulting in interception of call records.[11] This level of risk may override the benefits the government expects.

The vague systemic vulnerability safeguard has also driven companies (e.g. Meta, Signal, NordVPN) to signal they would withdraw from providing service in Canada. This is due to

[11] M. Geist, "Could Bill C-22 Make Canadians Less Safe? The Systemic Vulnerability Gap in Canada's New Surveillance Law", (8 April 2026), https://www.michaelgeist.ca/2026/04/could-bill-c-22-make-canadians-less-safe-the-systemic-vulnerability-gap-in-canadas-new-surveillance-law/.

the potential requirements to decrypt user data and rearrange their infrastructure to enable surveillance.

Moreover, the new ministerial order power grants access to any digital service used by Canadians without full independent approval or disclosure. The breadth of these new powers has even been likened to the potential creation of a surveillance state.

Justification

Several bills have been introduced in Canada to this end, most recently Bill C-2, but have died on the vine due to pushback because of overbreadth.

The government's main justifications for the *SAAIA* are:

- **Allies:** Canada's status as the only G7 and Five Eyes country without legislation requiring ESPs to develop and maintain lawful access capabilities.[12]
- **Ensuring capabilities:** Inconsistent capabilities and data retention across providers makes it difficult to execute warrants and production orders. The core provider regulations and ministerial orders are considered targeted approaches over imposing mandates on entire sectors of enterprises.[13]
- **Major & modern cybercrimes:** The government claims that threat actors exploit digital ecosystems in Canada and are evolving with rapid technological changes, faster than the capabilities of law enforcement. Crimes like online sexual abuse, terrorism, or foreign interference warrant stronger capabilities to generate leads and investigate threats with data. These crimes will only get more complex, and investigations must not be halted based on unavailability of certain data.[14]

The Problem:

This *SAAIA* enlists private service providers as agents to facilitate the construction of a communications environment tailored for surveillance. At a time when liberal democracies are already struggling to live up to their own values, the *SAAIA* moves Canada in the wrong direction: toward broader state surveillance capacity, deeper secrecy, and weaker democratic control. A significant expansion of state power requires evidence, necessity, and proportionality; the government's attempt to provide these has been unconvincing. A

---

[12] Government of Canada, "Lawful access" (Updated 25 May 2026), https://www.canada.ca/en/services/policing/police/crime-and-crime-prevention/lawful-access.html. [Government of Canada, "Lawful access"]

[13] Government of Canada, "Backgrounder – Supporting Authorized Access to Information Act (Bill C-22 – Part 2)" (Modified 12 March 2026) https://www.canada.ca/en/public-safety-canada/news/2026/03/backgrounder--securing-access-to-information-in-bill-c-22.html. [Government of Canada, "Backgrounder"]

[14] Government of Canada, "Backgrounder".

freedom-loving democracy cannot accept surveillance capacity of this magnitude without robust checks, strict limits, and meaningful accountability. The Bill lacks these, too.

- **Moving too quickly, with inadequate consultation:** Bill C-22 is being reviewed at a pace inconsistent with the complexity and significance of its provisions. The *SAAIA* creates a new standalone regulatory framework for obligations that have not yet been defined. It delegates foundational policy choices to the executive, and affects the security and privacy of virtually every Canadian who uses a digital service. The Committee has heard from a limited number of witnesses in a compressed timeframe.

  Few civil society actors have had the opportunity to be present and submit analyses before the Committee. National Security and Intelligence Review Agency (NSIRA), Signal, Apple, the Canadian Chamber of Commerce, the Cybersecurity Advisors Network, and the chairs of the US House Judiciary and Foreign Affairs Committees have all raised concerns. In contrast, the government was only questioned for an hour in the first hearing.
- **Lack of evidence:** The government has put forward mainly anecdotes and few statistics to indicate that the full expansion of procedural powers in Part 2 is required.[15] The National Security and Intelligence Committee of Parliamentarians' 2025 review of lawful access needs found that there are real challenges associated with modernization and existing lawful access procedures. However, the government fails to demonstrate how the breadth of access is required to address these issues, when they have historically found workarounds. There is no systematic evidentiary record showing that the existing framework failed to provide law enforcement with the access it needed.
- **Powers are too broad:** The breadth of the *SAAIA* is disproportionate to any need the government has identified. For example, the ESP definition captures most businesses in Canada, whose primary services may not be digital. The ministerial order powers extend the full regulatory regime to any ESP at the Minister's discretion. The metadata retention requirement applies to all users regardless of suspicion.

[15] National Security and Intelligence Committee of Parliamentarians, *Special Report on the Lawful Access to Communications by Security and Intelligence Organizations,* (revised version tabled on 15 September 2025) https://www.canada.ca/en/national-security-intelligence-committee-parliamentarians/services/press-release-sr-2025-09-15.html at para 168. [NSICOP, *Special Report on Lawful Access*]

Legislation that impinges on the constitutional rights of every Canadian - not just criminal suspects, but all users of digital services - requires evidence of failure in existing mechanisms, and a proportionate response tailored to identified gaps. Taken together, these provisions do not represent a carefully calibrated response to law enforcement issues. The *SAAIA* is surveillance infrastructure whose scope will be determined after the fact, by regulation and ministerial order, largely in secret.

Recommendations

6.1 The *Supporting Authorized Access to Information Act*, should not proceed as tabled. It requires major structural revision, independent oversight safeguards, and a demonstrated evidentiary basis.

Rationale: The *SAAIA* does not address proven gaps. It instead replaces a judicially controlled, case-specific framework with surveillance infrastructure affecting every Canadian who uses a digital service. If the government wishes to return with a more targeted proposal, it should first produce the evidentiary record that would justify it.

In the alternative, the following recommendations apply:

6.2 Extend committee hearings to ensure that the full range of affected stakeholders have an opportunity to appear and that their concerns are addressed on the merits before the Bill proceeds.

Rationale: The government's dismissal of concerns from corporations and technical experts as misreadings of the Bill threatens repeating the *Online News Act*'s failure, when government supporters confidently told Committee that Meta and Google were bluffing and would come to the table when legislated to do so. They did not. The concerns about Bill C-22 are substantive, specific, and consistent across a wide range of independent expert voices. They deserve full engagement.

6.3 Require the government to produce a systematic evidentiary record demonstrating that existing assistance order mechanisms have failed in identified cases, before Part 2 proceeds in any form.

Rationale: The government should not entrench a surveillance architecture affecting every Canadian based on thin evidence. If the existing production order mechanism works, the case for replacing it with a scheme of obligations has not been made.

7) Core Provider Obligations

Supporting Authorized Access to Information Act, s. 5-6

Background

Law enforcement can issue judicially authorized preservation orders to have service providers retain a suspect's personal data, metadata or keep their accounts open for up to four months.[16] Those preservation orders use the "reasonable grounds to suspect" threshold, but accessing the preserved information requires a judicially authorized production order based on the "reasonable grounds to believe" threshold.[17] Providers can set their own policies on what data to collect from users, how to store it, and how long they want to preserve it absent from a court order. Providers often encrypt user data using proprietary methods.

Section 5 of the *SAAIA* introduces a scheme of mandatory regulations that require core providers to build and maintain lawful access capabilities. The regulatory scope permits the mandated incorporation of law enforcement monitoring devices into provider networks, building new capacities to collect user data, complying with cybersecurity requirements, and maintaining user metadata for up to 1 year. The regulations could eliminate the need for a preservation order, although metadata and surveilled information would only be accessible to law enforcement with an authorized production order.

The specific requirements and core providers are defined with regulations passed by the designated Governor in Council and Federal Cabinet. The Governor in Council must balance several interests listed in *s. 5(3)*: the administration of justice, feasibility of compliance, impact on users, privacy and cybersecurity among others. According to *s. 5(5),* a core provider can be exempt from a regulation if the obligation would introduce a "systemic vulnerability" to their system.

The lists and classifications of core providers are exempt from the *Statutory Instruments Act (SIA)*, evading a multi-step review and publication process by the Department of Justice, Parliament, and Parliamentary committees.[18]

Justification

The government argues that companies' specific data retention policies, the advancement of cybercrime complexities and outdated lawful access policies delay crucial investigations:

---

[16] *Criminal Code,* RSC 1985, c. C-46 at s. 487.013, s. 487.0131. [*Criminal Code*]
[17] For example, using the general production order in *Criminal Code*, at s. 487.014.
[18] *Statutory Instruments Act,* RSC 1985, c. S-22. [*SIA*]

- **The need for legally required capacities:** Electronic service providers may encrypt information on their users or choose not to collect or preserve it at all. They are thus unable to provide valuable information even when law enforcement has a valid production order.[19]
- **Complexity of modern cybercrime:** Criminals increasingly use encrypted, anonymous and cross-border telecommunications services, and law enforcement needs access to this information to effectively combat crimes.[20] Specifically, the government has focused on large-scale organized crimes, like human trafficking, online child sexual abuse and issues of national security. The lawful access capabilities are to benefit local law enforcement, the RCMP, and CSIS.
- **Following Allies:** The scheme aims to catch up with the Five Eyes Intelligence sharing alliance with the United Kingdom, Australia, New Zealand and United States. The government claims that each of these countries has their own lawful access schemes, and Canada lags behind.[21]

Notably, there has been no explicit justification for exemption from the *SIA*, although the exemption may be attached to the need for private operations on issues of national security.

The Problem

Unchecked executive discretion to balance the interests of national security and law enforcement over privacy and technical feasibility puts people and providers at risk.

- **Privacy and feasibility:** There is no oversight or commitment to protecting the privacy and security of valuable user data in passing regulations. The Governor in Council need only *consider* the feasibility of its regulations and its impact on privacy and cybersecurity. Further, the balancing process is not documented. Regulatory oversight through the *SIA* provides *Charter* scrutiny but does not oversee the balancing process of *s. 5(3)*. While the government claimed in Committee that core providers will be consulted in the regulatory process, this is not included in the Bill.[22]
- **Poor technical and procedural safeguards:** The systemic vulnerability safeguard offers no specificity on the procedure to trigger or justify its use. What constitutes a

[19] House of Commons, *Hansard* 15 April at 6975.
[20] House of Commons, *Hansard* 20 April at 7163-64.
[21] House of Commons, *Hansard* 20 April at 7162.
[22] S. Heigel in Canada, House of Commons, Standing Committee on Public Safety and National Security, *Recording of Proceedings*, 45th Parl, 1st Sess, No 36 (5 May 2026), https://parlvu.parl.gc.ca/Harmony/en/PowerBrowser/PowerBrowserV2?fk=13437210 at 16h 25. [*SECU Hearing*, 5 May]

systemic vulnerability is open to interpretation and conflict between the government and the core provider. The government has made it clear in Committee that providers with existing capability to decrypt (i.e. not end-to-end encrypted) can be ordered or regulated to decrypt.[23]

Recommendations

7.1 Limit core provider obligations to assistance that gives effect to a specific, lawful access authority. Amend *s. 5(2)* of the *SAAIA* to prohibit regulations that require a core provider to:

i) redesign, weaken, or alter products or services offered in the ordinary course of business;

ii) collect, generate, retain, or organize information that the provider does not need for its own business purposes, except under a specific preservation or production authority;

iii) add, remove, disable, or modify product functionality;

iv) install, operate, or maintain government-controlled or third-party monitoring equipment inside its network or systems; or

v) build or maintain standing access capabilities that are not tied to a specific judicial or statutory authorization.

Rationale: The government should be able to compel access and intercept under certain circumstances, but it does not need the means to force redesign of infrastructure, over-collect data or demand changes to product functionality without compelling justification.

7.2 Amend *s. 5(3)* of the *SAAIA* to include a mandatory consultation on scope and technical feasibility with industry actors and the Office of the Privacy Commissioner prior to the making of regulations.

Rationale: The mandatory consultation process will ensure personal privacy interests and provider technical capabilities are always considered when making core provider obligations. The government cannot claim to consult with core providers and prioritize the safety of users with no written obligation to do so.

7.3 The balancing process and consultation in *s. 5(3)* should be documented for appropriate oversight under the *Statutory Instruments Act* and the annual reporting

[23] S. Heigel in *SECU Hearing*, 5 May at 16h 06.

process. It should clearly outline the final justification and outline the countervailing perspectives from the industry and Privacy Commissioner.

Rationale: Documentation of the balancing process informs the oversight body with all perspectives on a proposed regulation for consideration of *Charter* compliance. When a regulation is pertinent to national security, the documentation will be handled confidentially under the *SIA* oversight process and by the National Security and Intelligence Review Agency (NSIRA) in their review of the annual report.

7.4 Clarify the scope and define the procedure to raise the systemic vulnerability exception.

Amend the definition of "systemic vulnerability" in *s. 2(1)* of the *SAAIA* to include any requirement that would weaken, bypass, compromise, or interfere with encryption, authentication, device security, operating system integrity, software update integrity, service integrity, or cybersecurity protections. Remove the "substantial risk" threshold or replace it with a lower standard, such as "material risk."

Create an independent process for systemic vulnerability claims. The procedure should first trigger a review of the claim by the Department of Public Safety, pause any penalties for non-compliance, and output a transparent judgement. If the exception is denied, the core provider should be able to seek a final independent review by the Federal Court.

Rationale: Clarification of safeguards essential for compliance. It also avoids unnecessary obligations on the provider and saves enforcement resources. The systemic vulnerability procedure would ensure both the provider and regulatory body are on the same page regarding what constitutes a systemic vulnerability, and how new regulations may compromise a core provider's system.

8) Seriousness of Metadata and Surveillance Implications

Supporting Authorized Access to Information Act, s. 5(2)d

Background

Current law gives law enforcement targeted tools to preserve and obtain metadata in specific investigations, including preservation orders, production orders for transmission data, production orders for tracking data, and tracking or transmission data warrants. These tools generally require investigative grounds, and police usually need judicial authorization before they can compel production or obtain access to the data.

Section 5(2)(d) of the *SAAIA* would allow Cabinet to require core providers to retain categories of metadata for periods of up to one year. That will shift metadata retention from a targeted investigative measure into a infrastructure obligation imposed before any particular suspect, device, account, or investigation has been identified.

Justification

The government claims that metadata are "basic information" with a reduced privacy interest. They recognize that "metadata", as currently defined in the Bill, has a significant scope: it includes internet transmission data, including timestamps, IP addresses and device identifiers.[24]

The government aims to use metadata to map complex networks and timelines for use in modern intelligence-led policing. They claim that the scope of metadata cannot be limited, because exclusion of key categories will result in incomplete evidence and barriers across jurisdictions and platforms.[25] The government further claims that metadata regulations will be tailored to specific types of data for certain scenarios, determined by consultation with the industry, law enforcement and intelligence agencies to ensure proportionality and necessity.[26]

The Problem

The scope of metadata is expansive, poorly understood, and underplayed as "basic information".

- **Privacy**: Aggregating metadata has a high privacy interest and is identifiable information.[27] People's activities are so unique that as little as four location points

[24] Supt. R. Burchill (RCMP) in *SECU Hearing*, 5 May at 16h 14.
[25] S. Acan in *SECU Hearing*, 5 May at 17h 46.
[26] K. Ho in *SECU Hearing*, 5 May at 16h 12.
[27] R Diab, "Is the Power to Preserve Everyone's Metadata Constitutional?", (19 March 2026), https://www.robertdiab.ca/posts/metadata-c22/.

can identify 95% of people.[28] One week of metadata from a single app is enough to build a comprehensive profile.[29] According to researchers, any dataset rich enough to be useful to law enforcement can be de-anonymized.[30] Metadata offers retrospective reconstruction of an innocent person's life, and prediction on their future. There is an expectation that it will not be preserved at the government's discretion; the government may not keep watch "just to be sure."[31]

Metadata is a proxy for content; they are often inseparable.[32] Long-term aggregates of metadata are equally revealing and more valuable than the content itself. Metadata can be easily analyzed in bulk and correlated with external events compared to parsing semantics of written and recorded content.[33] With AI, the profiling and prediction capabilities available to law enforcement would be nearly unlimited and precise to a suspect's habits or intentions.[34] An exemption on content, social media or browsing history is no safeguard, when strategic metadata extraction across multiple sources is allowed.[35]

Metadata retained by companies is extremely valuable for behavioural analytics.[36] Bulk location and app usage metadata underpin the $365 billion data broker industry, with certain (e.g. financial) companies spending millions annually for pseudonymized location trails. Metadata exposes where people go, what they do, and which services they use.

Metadata retention without qualification is not the norm in Canada nor with its allies. The EU and UK have insisted that general metadata retentions must link to

---

[28] Office of the Privacy Commissioner of Canada, *Metadata and Privacy: A Technical and Legal Overview* (October 2014), https://www.priv.gc.ca/media/1786/md_201410_e.pdf. [Office of the Privacy Commissioner of Canada, *Metadata and Privacy*]

[29] D. Tokmetzis, "How Your Innocent Smartphone Passes on Almost Your Entire Life to the Secret Service" (20 December 2013), https://www.statewatch.org/media/documents/news/2014/jul/bits-of-freedom-on-the-metadata-of-your-phone.pdf.

[30] Office of the Privacy Commissioner of Canada, *Metadata and Privacy*.

[31] R Diab, "Is the Power to Preserve Everyone's Metadata Constitutional?",(19 March 2026), https://www.robertdiab.ca/posts/metadata-c22/.

[32] Office of the Privacy Commissioner of Canada, *Metadata and Privacy*.

[33] American Civil Liberties Union of California, *Metadata: Piecing Together a Privacy Solution,* (February 2014), https://www.aclunorcal.org/publications/metadata-piecing-together-privacy-solution/; Office of the Privacy Commissioner of Canada, *Metadata and Privacy*.

[34] A. Vedaschi, C. Graziani, *Artificial Intelligence, Counter-Terrorism and the Rule of Law* (Edward Elgar, 2025), https://www.elgaronline.com/monobook-oa/book/9781803928340/9781803928340.xml at pp. 47-57.

[35] L. Stein, "What Your Data is Actually Worth", (10 October 2023), https://www.datapods.app/en-US/blog/consumer/what-your-data-is-actually-worth

[36] L. Stein, "What Your Data is Actually Worth".

specific serious threats, independent oversight and remedies for rights violations.[37] The US has no data retention regime and recognizes wealth of detail from metadata connection available to the government based on the ubiquity of phones.[38] In 2025, 40 US states settled with Google for $425 million USD for collecting "non-personal, pseudonymous, encrypted" tracking metadata of its users for years without consent, indicating the data's value to users and the companies.[39]

Treating metadata as routine or invaluable is false and inconsistent with the *Charter*. Determining the privacy interest associated with metadata as a fact-specific exercise. Canadian Courts have found that derivatives of communication are constitutionally protected because they convey meaning about content.[40] The Supreme Court recognized that metadata reveals interests, habits, and identity that a user divulges *unwittingly*, and thus attracts a strong privacy interest based on their reasonable expectations of its use.[41] The Court also rejected the idea that expectation of privacy diminishes simply because people know that companies already collect their metadata.[42]

- **Ineffective justification**: The 2025 investigation on lawful access by the National Security and Intelligence Committee of Parliamentarians identified that law enforcement found metadata to be burdensome to sift through.[43] There is no indication that this would change with retention of additional metadata. There is also no evidence of a pattern of cases where missing year-old metadata has resulted in breaking of the chain of evidence or being a major contributor to incomplete evidence at the Court level.[44]
- **Blanket retention:** The Bill authorizes retention at scale, without individualized suspicion. This amounts to the state-mandated creation and maintenance of a massive, year-long archive of private communications metadata for undefined and

[37] A. Vedaschi, C. Graziani, *Artificial Intelligence, Counter-Terrorism and the Rule of Law* (Edward Elgar, 2025), https://www.elgaronline.com/monobook-oa/book/9781803928340/9781803928340.xml; *Privacy International v Secretary of State for Foreign and Commonwealth Affairs*, [2019] UKSC 22; *Secretary of State for the Home Department v Watson & Others*, [2018] EWCA Civ 70; *Big Brother Watch and Others v. the United Kingdom*, (2021) 72 EHRR 17; *La Quadrature du Net et autres v Premier ministre et autre*s, C-511/18, C-512/18 et C-520/18, ECLI:EU:C:2020:791.
[38] Office of the Privacy Commissioner of Canada*, Metadata and Privacy*.
[39] CBC News, "Google ordered to pay $425 million US for privacy violations in class-action case", (3 September 2025), https://www.cbc.ca/news/business/google-class-action-privacy-1.7624738.
[40] *R v TELUS Communications Co.*, 2013 SCC 16.
[41] *R v Vu,* 2013 SCC 60.
[42] *R v Duarte,* 1990 CanLII, 150 (SCC).
[43] NSICOP, *Special Report on Lawful Access* at para 67.
[44] NSICOP, *Special Report on Lawful Access* at para 168-171.

only potential future investigative use. Blanket prospective retention of metadata raises clear constitutional concerns.

Recommendations

8.1 Remove *s. 5(2)(d)* of the *SAAIA*, thereby stopping all regulations regarding metadata retention entirely. Law enforcement must be properly educated on the effective use of metadata accessible with existing schemes.

8.2 If Parliament insists on a retention power, replace *s. 5(2)(d)* with targeted preservation only.

8.3 Identify the substantive data and technical capacities that pose barriers to the investigation process. Clarify and arrive at a mutual understanding of technical terms between law enforcement and industry (e.g. end-to-end encryption, systemic vulnerability, etc.).

8.4 Build knowledge and capacity within law enforcement agencies to work effectively with existing digital evidence and existing assistance order mechanisms before expanding their powers: how deal with metadata data, forming common understandings of technical information (e.g. encryption, privacy interests, possible future tech-crime capabilities).

Rationale: New lawful access legislation must be made based on comprehensive assessments of access barriers and full understanding of the implications of the legislation. The government should demonstrate that less intrusive alternatives have been exhausted before Parliament is asked to authorize extensive metadata retention infrastructure. This protects the privacy of Canadian electronic services users, and ensures targeted, incremental expansion as proportional with law enforcement's justified needs.

The existing production and preservation orders are comprehensive and consistent with allies' positions on lawful data retention. Law enforcement should understand how to analyze large amounts of metadata, and benefit from the existing capabilities of using it. The operational gaps - like difficulty executing tracking warrants - reflect capacity and coordination problems within law enforcement.

9) Ministerial Orders

Supporting Authorized Access to Information Act, s. 7

Background

Ministerial Orders authorized under *s. 7* of the *SAAIA* compel any ESP to comply with any core provider obligation, even if the ESP is not a core provider. The order must be approved by the Intelligence Commissioner who reviews whether the Minister's conclusions are reasonable. The order may be made and operate in secret. ESPs need not comply if the order creates a systemic vulnerability.

Justification

The government aims to have a flexible, targetable capability to compel a given ESP to suit their imminent lawful access needs.

- **Timeliness**: The Minister can act at the request of law enforcement or CSIS. Issues of national security warrant quick action to preserve data. The government claimed in Committee ex-post review or approval by the NSIRA would not suit their needs for expediency.[45]
- **Technological Advancements & National Security**: ESPs that are not core providers but are of interest to law enforcement will crop up often in rapid and evolving technological investigations.

The Problem

Ministerial orders create a secret executive route for imposing surveillance-capability obligations on providers that Parliament has not clearly limited by necessity, seriousness, proportionality, or provider type. The scope of entities who may qualify as an "ESP" is immense. Affected providers have limited procedural rights, the Privacy Commissioner has no required role, and the systemic vulnerability safeguard remains too narrow and procedurally unclear. The overbroad scope of ESPs, unclear threshold for ministerial orders, and streamlined review process skirts effective oversight for orders with different levels of security and privacy implications.

- **Privacy:** The privacy implications for users are unbounded. The wide ambit of "electronic service provider" implicates nearly every service in Canada. In the absence of an intended scope of use of Ministerial Orders, and with the wide breadth of potential core provider obligations, the order could compel immediate

[45] G. Anandasangaree in *SECU Hearing,* 5 May at 16h 25.

and secret surveillance or metadata retention of any person without their knowledge.

- **Overreach of Executive Powers**: The Minister has discretion to balance privacy, cybersecurity, and technical feasibility with national security and law enforcement needs. The Intelligence Commissioner would only rule on the order's reasonableness.
- **Poor technical and procedural safeguards:** The Minister must consider feasibility, cost, impact on users, privacy, and cybersecurity, but the Bill does not create a clear process for providers to contest those issues or pause compliance while a systemic vulnerability claim is adjudicated.

Recommendations

9.1 Remove ministerial orders under *s. 7* of the *SAAIA* or require judicial authorization.

Rationale: The government has not shown why secret executive orders without judicial authorization are necessary for all ESPs. If the power remains, it should require approval by a judge on necessity, proportionality, technical feasibility, cybersecurity risk, and privacy impact.

9.2 Narrow the definition of "electronic service provider" to exclude entities whose primary business is not the provision of communications or data services. Establish a minimum threshold based on number of Canadian users or nature of service before any obligations under the *SAAIA* apply.

Rationale: A definition broad enough to capture law firms, medical clinics, and media organizations is a general grant of authority that will be bounded only by the government's regulatory choices. Parliament must draw those boundaries, not delegate them entirely to the executive.

9.3 Define a high threshold for a ministerial order (e.g. for exigent circumstances or national security) and require necessity and proportionality. The Privacy Commissioner must be involved in assessing proportional privacy and cybersecurity implications of an order. Orders for national security investigations must be subject to order-by-order ex-post review by the NSIRA.

Rationale: A high threshold for a Ministerial order will limit overreach by executive power. A power of this kind should not be available for ordinary investigations or convenience. It should be reserved for serious cases where no less intrusive means will work. Executive decision-making on national security warrants independent scrutiny on reasonableness, proportionality, and necessity. The Intelligence Commissioner's mandate is only to

consider reasonableness. The NSIRA's review shortly after the order is made is within their mandate and consistent with all executive national security decision-making.

9.4 As with the core provider obligations, clarify the scope and define the procedure to raise the systemic vulnerability exception in Ministerial orders. Define explicitly that the forced creation of a decryption capability is clearly a systemic vulnerability.

The procedure should first trigger a review of the claim by the internal enforcement body, pause any penalties for non-compliance, and make a transparent judgement. If the exception is denied, the ESP may seek final recourse with independent review by the Federal Court.

Rationale: Clarification of safeguards essential for compliance. It also avoids unnecessary obligations on the provider and saves enforcement resources. The systemic vulnerability procedure would ensure both the provider and regulatory body are on the same page regarding what constitutes a systemic vulnerability, and how new regulations may compromise a core provider's system.

9.5 Require secrecy to be justified order by order, with a sunset clause.

Rationale: Secrecy should not be the default. The Minister should have to justify confidentiality based on specific facts, and any secrecy obligation should expire unless renewed by an independent decision-maker. Public aggregate transparency reporting should follow.

10) Obligation to Assist

Supporting Authorized Access to Information Act, s.14

Background

Section 14 of the *SAAIA* requires electronic service providers to provide "all reasonable assistance" to specified government personnel for the purpose of assessing or testing any device or equipment that may enable authorized access to information. The only substantive limit is that the testing must not have the effect of granting access to personal information.

Currently, reasonable assistance requirements are part of judicially authorized warrants. When police or CSIS obtain a production order, wiretap order, or tracking order, they can ask the judge to issue an assistance order directing the service provider to give all reasonable assistance to give effect to it. These assistance orders are appropriately tailored to the specific case, signed off by a judge, and subject to judicial review. There has been little evidence identifying problems with this existing mechanism that would justify the creation of a new ministerial request untethered by any judicial authorization.

Section 14 differs structurally from the compelled disclosure and assistance obligations in Part 1. The production orders and confirmation of service demand each define the category of information sought, require statutory grounds before the obligation is triggered, and provide for judicial review. Section 14 does none of these things. The obligation is triggered by a written ministerial request alone.

Justification

The government's case appears to rest on capability gaps. The government has provided three scenarios of how Bill C-22 would help investigations, each which reference ESP assistance.[46] The first is a missing 16-year-old girl who made an emergency call after 10 days missing; the provider could confirm the call and the tower used but could not provide the last known location of the phone before it was disconnected. The second and third are about CSIS obtaining a warrant to track a suspect's cell phone, only to find that the telecommunications provider lacked the capability to track the device in real time.

The Problem

The existence of potential capability gaps supports some form of capability assessment. They do not justify an open-ended assistance obligation triggered by ministerial request alone.

[46] Government of Canada, "Lawful access".

The undefined scope of "reasonable assistance" creates three problems:

- **Scope:** The Bill fails to define permissible categories of testing, technical depth, duration, frequency, or the systems that may be touched.
- **Privacy and security:** The prohibition on granting access to personal information during testing is narrow – it addresses the immediate output of a test but not the cumulative knowledge about system vulnerabilities that testing may generate. There is no requirement that testing be the least intrusive means of achieving its purpose, and no limit on how often the same provider may be subjected to it.
- **Oversight and accountability:** The assistance obligation is self-policed by the requesting party. There is no independent technical assessor, few documentation requirements, no limit on duration, and no obligation to record what was tested, what was learned, or what capabilities were confirmed. There is no defined ability to contest the request. If it is not an order, can they refuse it? If the testing introduces a vulnerability to their system, can they get an exemption? This should be made clear in the Bill.

Recommendations

10.1 Define the permissible scope of assistance. Prohibit testing that requires the provider to: weaken encryption, introduce or preserve a vulnerability, alter the ordinary functionality of a product or service, or collect or retain data beyond what the provider requires for its own business purposes.

Rationale: An obligation that is this technically consequential should not have its scope determined solely by the executive. Regulations that define permissible categories of assistance, maximum testing durations, frequency limits, and documentation requirements would constrain the obligation without defeating its purpose. Parliamentary approval of this scope, rather than mere tabling, ensures democratic deliberation over obligations that can affect the security of communications for millions of Canadians.

10.2 Require a written ministerial finding of necessity, proportionality, technical feasibility, and absence of less intrusive alternatives before a *s. 14* request is issued, with approval by the Intelligence Commissioner before testing begins.

Rationale: Production orders always require statutory grounds and judicial authorization before a provider is compelled to produce information. There is no principled reason that the obligation to assist in building and testing access capabilities – a more structurally invasive requirement – should be triggered by ministerial request without any prior independent finding. The written necessity and proportionality determination would align

s.14 with the standards for state access to digital information and would give the Intelligence Commissioner meaningful material to review.

10.3 Appoint an independent technical assessor to oversee testing conducted under *s. 14*.

Rationale: The prohibition on accessing personal information during testing is currently self-policed by the requesting agency - the party with the strongest interest in expansive access. An independent technical assessor would verify that testing remains within authorized parameters, document what was assessed and what was learned, and report findings to the Intelligence Commissioner and the Minister. Involving them as an independent check on the testing of private providers' systems is consistent with that mandate and would provide genuine rather than nominal oversight.

10.4 Require record-keeping and annual reporting on assistance requests, as an amendment to *s. 49(2)(d)*.

Rationale: Every request under *s. 14* should be logged with the Department of Public Safety, along with its the statutory basis, the provider subject to the request, the nature and duration of testing, and the independent assessor's findings. Public aggregate reporting on the number of requests made, number of providers subject to testing, number of requests contested, and breakdown by category of capability assessed would protect operational details while making the regime measurable. Accountability allows Parliament, oversight bodies, and the public to assess whether the assistance obligation has remained a narrow and targeted tool or has expanded into routine surveillance infrastructure assessment.

10.5 Create an express right to challenge a *s. 14* request.

Rationale: Section 14 does not create a mechanism for an ESP to challenge a request. The Bill should state whether the ESP may seek review, whether compliance is suspended during review, whether penalties are unavailable while review is pending, and whether the systemic vulnerability safeguard applies to requests for reasonable assistance.

11) Confidentiality and Prohibition of Disclosure

Supporting Authorized Access to Information Act, s.15-18

Background

The Confidentiality section of the *SAAIA* allows secret orders to ESPs to implement a capability for access to information. Users may continue to rely on a service without knowing that the state has required changes to the technical or operational architecture on which their privacy and security depend. For example, an order could turn an Amazon Alexa device into a listening device or track any cell phone.[47] While the government has said they do not plan to undermine decryption, the words of the Bill do not prohibit it, with no transparency requirements for Canadians.[48]

Currently, when police or CSIS obtain a judicial order requiring a service provider to provide assistance, that order can be accompanied by a non-disclosure order where a judge finds there are reasonable grounds to believe disclosure would jeopardize the police investigation (see e.g. *Criminal Code* s. 487.0191). Bill C-22 replaces that judicially controlled model with automatic ministerial confidentiality that attaches without any independent determination of necessity.

Section 15's confidentiality provisions are remarkably broad. It prohibits electronic service providers and anyone acting on their behalf from disclosing informational details such as the contents of a ministerial order; the information the Minister relied on in making it; the fact that the provider is subject to it; information exchanged during the representations process; inspection details; and information submitted during periodic review. There is no sunset, no necessity threshold, and no judicial authorization required before the gag attaches. Providers must stay silent indefinitely unless the *Act* or the *Canada Evidence Act* permits otherwise. This prevents meaningful public accountability and makes it very difficult for providers to seek legal advice or warn users in any general way about government surveillance capabilities built into their services.

This goes further than the confirmation of service demand regime in Part 1, which requires the requesting officer to have reasonable grounds to believe disclosure would jeopardize the investigation before imposing non-disclosure, and limits that condition to one year. Part 2 has no comparable constraint.

---

[47] D. Fraser, "My testimony on Bill C-22, the Lawful Access Act of 2026, to the House of Commons Standing Committee on Public Safety and National Security" (7 May 2026), https://blog.privacylawyer.ca/2026/05/my-opening-statement-on-bill-c-22.html.

[48] D. Fraser, "My testimony on Bill C-22, the Lawful Access Act of 2026, to the House of Commons Standing Committee on Public Safety and National Security".

Justification

The government has justified mandatory confidentiality on the basis that ministerial orders must remain secret to avoid tipping off threat actors, pointing to Intelligence Commissioner approval as the primary safeguard.[49]

The Problem

The confidentiality regime creates several compounding problems.

- **Privacy and rule of law:** A provider subject to a ministerial order cannot tell its user base that government-mandated access capabilities have been built into their service. Users of the service therefore cannot make informed choices about what communications they entrust to that provider. This information asymmetry is created without any independent determination that secrecy is necessary in the particular case. The Supreme Court of Canada has recognized that Canadians hold significant privacy interests in their digital communications and the services through which they are conducted, including a reasonable expectation that those services operate as they appear to.[50] Where the government secretly mandates that a provider alter its security architecture to enable access, users have a misaligned expectation of privacy – they believe they are protected when they are not. A search or seizure conducted through infrastructure the user did not know had been compromised engages *s. 8* of the *Charter*.
- **Oversight and accountability:** The confidentiality obligation in Part 2 attaches automatically and does not require prior judicial authorization. The provider cannot contest the order or warn its users and faces significant procedural obstacles to seeking relief. The Intelligence Commissioner's mandate concerns national security rather than individual privacy, meaning the body providing pre-approval is unsuited to assess the privacy interests most directly engaged.
- **No independent oversight:** There is no independent oversight on what information is prohibited from disclosure, and secrecy is not considered on a case-by-case basis. The minister who issues the order controls its secrecy.
- **Ability to amend without disclosure:** The Governor in Council should not be able to amend the procedural requirements about disclosure and should not have the power to remove oversight mechanisms.

[49] Government of Canada, "Backgrounder"
[50] *R v Spencer*, 2014 SCC 43.

Recommendations

11.1 Ministerial orders and confidentiality requirements should not take effect unless an independent decision-maker approves them on a case-by-case basis. That review should include Federal Court approval for any prohibition on disclosure and meaningful review by the Privacy Commissioner of Canada for orders that affect user privacy, security architecture, or the confidentiality of provider obligations.

Rationale: Restrictions on a provider's ability to speak, notify, or disclose information are extraordinary powers used in exceptional circumstances. The officer or Minister who compels technical capabilities should not also unilaterally control their secrecy, and secrecy cannot be routine administrative practice. The Federal Court adds an independent check, forces the executive to justify secrecy on the specific facts, and ensures non-disclosure is tied to demonstrated necessity rather than administrative convenience. The Privacy Commissioner is best placed to assess how confidentiality orders affect individual autonomy over personal information since secrecy prevents people from making meaningful choices about the services they use and the treatment of their information.

11.2 Impose a 1-year limit on confidentiality obligations, after which extension or renewal requires a fresh justification and approval by a Federal Court judge.

Rationale: The current prohibition has no expiry. Secret orders of indefinite duration serve government convenience, not investigative necessity. Operational sensitivity that genuinely justifies secrecy at the time an order is made should not persist for years. A 12-month default, renewable only with fresh demonstration of continued necessity, would match the non-disclosure limits in the confirmation of service demand, and would ensure that secrecy does not outlast its justification.

11.3 Create a safe harbour for aggregate transparency reporting, with data securely recorded and reported at a later date for Parliamentary and public review. Add the secrecy orders to the annual reporting process by the Minister (*s. 49(2)* of the SAAIA), and allow providers to report the numbers in aggregate to the public.

Rationale: Providers should be permitted to publish annual statistics on the number of orders received, broad categories of obligations imposed, and whether orders were contested without needing to identify specific orders or investigations. Amending the reporting approach preserves operational secrecy while giving Parliament, and the public the minimum information needed to assess whether the regime is proportionate.

11.4 Remove the Governor in Council's authority to amend procedural limitations on disclosure and oversight mechanisms by regulation under *s. 18(b)*.

Rationale: Oversight mechanisms that can be quietly removed by executive action without Parliamentary approval are not genuine safeguards. The procedural protections in the confidentiality regime should be entrenched in the statute and amendable only through Parliament.

11.5 Explicitly preserve the right to consult security-cleared independent legal counsel without that consultation constituting a prohibited disclosure.

Rationale: The current wording of s. 15 is broad enough to potentially capture disclosure to legal counsel, creating uncertainty about whether a provider subject to a ministerial order can obtain meaningful legal advice about the scope of its obligations or its rights under the SAAIA. A carve-out explicitly permitting disclosure to security-cleared counsel under confidentiality conditions would eliminate that ambiguity, protect investigations, and preserve a basic due process guarantee without waiting for a court to resolve the question at a provider's expense.

12) Enforcement: Compliance, Audit and Inspection Orders

Supporting Authorized Access to Information Act, s. 19-27.

Background

In addition to monetary penalties, the Minister and a delegated enforcement team can verify and enforce compliance with the act by (1) conducting inspections, (2) ordering the ESP to conduct an internal audit of their services, or (3) issuing compliance orders. Only compliance orders can be reviewed by the Minister upon request by the provider.

The threshold for an inspection is whether there are reasonable grounds to believe that an activity regulated by the *SAAIA* is conducted in that location. No warrant is required, and the annual report of the Minister's activities only vaguely requires "information relating to compliance orders and enforcement actions taken".

Justification

The government has not put forward any specific justification for the vague reporting requirements, reduced thresholds for enforcement activities, and lack of review mechanisms. The enforcement scheme is consistent with the broad intention of streamlining law enforcement activities by minimizing external processes.

The Problem

The enforcement procedure creates a new warrantless access and inspection power over ESP premises and electronic data, and new powers for audit and compliance orders, without opportunity for independent review. The threshold does not require suspected non-compliance: a designated person may enter private property because *SAAIA* regulated activity occurs there. Once inside, the inspector may examine, copy, and remove documents and electronic data. Providers have no means to contest orders with an independent body.

- **Privacy**: The user data managed by providers has a high expectation of privacy. Inspections of private property under the *Charter* must be reasonable. Providers could be subject to inspection without any evidence that non-compliance is occurring or may occur. The broad scope of orders ultimately allows inspection on any property merely related to electronic data collected by the ESPs.
- **Circumvents safeguards**: Providers have the right to refuse compliance with the *SAAIA*'s orders and regulations based on systemic vulnerabilities to their system. Without consideration of these safeguards in the enforcement threshold, there is a risk of surprise inspection and seizure of data for compliant providers.

- **Overreach of Executive Powers**: Enforcement decisions and reviews of appeals are subject to the discretion of the Department of Public Safety, a non-neutral party. Ministerial orders have mandatory compliance, and inspection authorities are appointed by the Minister. Providers have no option to have their orders reviewed by an alternative, objective party.

Recommendations

12.1 Narrow the inspection power in *s. 20* and require judicial authorization for intrusive inspections. The section should distinguish between routine regulatory inspections and intrusive inspections. Warrantless entry should be limited to routine compliance activity that does not involve access to customer information, retained metadata, confidential security architecture, or provider computer systems. Any inspection that may involve those categories should require prior judicial authorization, based on reasonable grounds to believe that the provider is contravening, or is likely to contravene, the *Act*.

Rationale: A threshold based on plausibility of non-compliance preserves the privacy of the provider and protects personal information and metadata that should only be accessible by warrant. Classes of inspections are consistent with the *Charter* and ensure the target of inspection is specific. Judicial authorization limits any overreach of Ministerial power.

12.2 Add strict minimization, sealing, use, and destruction rules for inspections and audits. The *SAAIA* should prohibit designated persons from accessing, copying, retaining, removing, or using customer personal information unless a judge specifically authorizes that access as necessary and proportionate. Any personal information incidentally obtained during an inspection or audit should be sealed, segregated, and destroyed unless a court authorizes its retention.

Rationale: ESPs hold sensitive customer information, including data that can reveal identity, location, communications patterns, and service use. A compliance inspection should not become a pathway into customer data. Minimization rules would keep enforcement focused on provider compliance, not user surveillance.

12.3 Create an independent review mechanism for compliance orders, audit orders, intrusive inspections, and administrative penalties. The *SAAIA* should provide both internal review and independent review by the Federal Court.

Rationale: A provider should not have to comply with a contested order while a good-faith challenge is pending where the challenge raises privacy, cybersecurity, systemic vulnerability, technical feasibility, legality, or proportionality concerns. A multi-stage appeal mechanism ensures procedural fairness and reasonable decision-making with regards to enforcement orders. An internal appeal process by the Minister (as in *s. 26-27* for compliance orders) is fair as a first step. Judicial review should be accessible as a final recourse to limit overreach given by the broad powers of the Minister. Independent review is needed before enforcement powers compel conduct that may expose personal information, weaken security, or require disputed technical changes.

12.4 Strengthen annual reporting. The annual reporting procedure in *s. 49(2)c* of the *SAAIA* must include a comprehensive assessment of all enforcement actions. All compliance, audit and inspection orders must be recorded, including: any electronic information and evidence accessed, copied, gathered, or destroyed from providers during enforcement actions, the ultimate compliance or non-compliance of the provider, and impact of the enforcement actions.

Rationale: Enforcement mechanisms should be used rarely and justifiably. Ineffective and unjust enforcement procedures must be identified and limited in the interest of the effectiveness of the *SAAIA*, as well as Canadians' and providers' rights to privacy. Public reporting supports democratic accountability. Parliament and the public need enough information to assess whether enforcement powers are rare, justified, effective, and proportionate.

Conclusion

The digital infrastructure on which Canadians depend for work, healthcare, communication, and civic participation is the infrastructure this Bill envisions as a surveillance platform. CIPPIC acknowledges that targeted, judicially controlled access powers can be justified, but those powers must be earned through evidence, constrained by clear statutory limits, and kept accountable through independent oversight and public transparency.

Bill C-22 does not meet that standard. Part 1 lowers thresholds without demonstrating that existing tools are inadequate. Part 2 creates a standing surveillance infrastructure, the ultimate scope of which will be determined after the fact, largely in secret, with thin democratic accountability. The process by which it has been reviewed has not permitted the scrutiny that a Bill of this consequence requires.

Nowhere is evidence-based policy-making more crucial to Canadians than in the enactment of powers that impinge on civil liberties.

The Committee has an opportunity to insist on a better approach: extend hearings, require an evidentiary record, and amend the Bill to ensure that any lawful access regime it authorizes is narrowly targeted, technically sound, independently reviewable, and consistent with the *Charter*.

CIPPIC remains available to assist the Committee in that work.