

Bill C-22, *An Act respecting lawful access*

Brief to the Standing Senate Committee on National Security, Defence and Veterans Affairs

International Civil Liberties Monitoring Group

Submitted Nov. 4, 2026

About the International Civil Liberties Monitoring Group
The International Civil Liberties Monitoring Group is a coalition of Canadian organizations founded in 2002 following the adoption of Canada's first-ever Anti-terrorism Act. Our mandate is to monitor and defend against the impacts of Canada's national security and anti-terrorism laws on civil liberties in Canada and internationally. The coalition's 45 member organizations cover a broad range of sectors, including faith-based, labour, human rights, environmental, legal and humanitarian groups. More at http://iclmg.ca.

Introduction

Over the past two decades, successive federal governments have attempted to weaken privacy protections under the name of 'lawful access.' However, each time, privacy experts, human rights and civil liberties advocates, and the general public have refused to trade the important protections that privacy laws afford us in exchange for promises of "security" built on nebulous justifications that these powers are necessary for law enforcement. Our coalition has contributed consistently to these conversations, through op-eds, briefs, consultation submissions and committee appearances.[1]

There has also been a pattern, including regarding Bill C-22, of law enforcement arguing that new investigatory powers are necessary to address novel challenges whereas evidence shows that tools and powers that would allow them to adequately address these problems already exist. As described by the Citizen Lab, while law enforcement may present these issues as a blockage, in reality they are experiencing investigatory friction: difficulties exist, but investigations can still be carried out effectively.[2] Furthermore, as detailed by Professor Michael Geist, the government has once again failed to present convincing evidence or scenarios to justify the reforms they are seeking in this legislation.[3]

Position on Bill C-22

Our coalition is deeply concerned that, if enacted, Bill C-22 will significantly expand state surveillance and seriously threaten privacy rights, with concurrent impacts on free expression, freedom of association, and equality rights.

---

[1] See, for example: https://iclmg.ca/atf-consultation/, https://iclmg.ca/opc-biometrics-consultation/, https://iclmg.ca/wp-content/uploads/2016/12/Nat-Sec-Consultation-ICLMGs-Answers-EN.pdf, https://iclmg.ca/issues/bill-c-59-the-national-security-act-of-2017/bill-c-59s-mass-surveillance-and-cyber-powers/

[2] Parsons, Christopher. "Canada's New and Irresponsible Encryption Policy," The Citizen Lab, 21 August 2019. Online: https://citizenlab.ca/research/canadas-new-and-irresponsible-encryption-policy-how-the-government-of-canadas-new-policy-threatens-charter-rights-cybersecurity-economic-growth-and-foreign-policy/

[3] Geist, Michael. "The Government Tries to Make the Case for Bill C-22: Why Its Own Use Cases Reveal Disproportionate Overreach," michaelgeist.ca, 21 May 2026. Online: https://www.michaelgeist.ca/2026/05/the-government-tries-to-make-the-case-for-bill-c-22-why-its-own-use-cases-reveal-disproportionate-overreach/

This legislation presents one of the greatest threats to privacy in Canada of the past two decades. Its provisions will weaken the rules governing police access to personal information, all while facilitating a vast expansion of government surveillance, and create a treasure trove of data that will be catnip to hackers. It is one more case in the decades-long trend of Canadian governments using national security as an excuse to erode civil liberties and human rights.

We acknowledge that the House of Commons adopted several amendments meant to address the concerns we and others have raised, but for the reasons explained below believe that they have failed to address the underlying problems with Bill C-22.

Recommendation 1: Based on the concerns below, Bill C-22 should not proceed to Royal Assent and should instead be withdrawn, reconsidered and subjected to further consultation. In the alternative, outstanding concerns with Part 1 of the Bill should be addressed through targeted amendments, while Part 2 should be removed altogether.

Part 1: Timely Access to Data and Information

a. "Information Demands" vs "Confirmation of Service"

Part 1 of Bill C-22, *Timely Access to Data and Information*, proposes a new "Confirmation of Service Demand." It would be restricted to telecommunication service providers (TSP) and consist of a yes/no answer about whether a TSP holds an account associated with an individual's name, email, phone number, etc.

While narrow in scope, "Confirmation of Service Demands" would still set the alarming precedent of allowing law enforcement and intelligence officers to request information without a warrant based only on the suspicion – rather than the belief – that the information would be of use in investigating a crime. This sets a worrisome precedent and risks the further broadening of warrantless demands as it gains acceptance.

> **Recommendation 1:** That the committee fully examine the impact of precedent-setting warrantless Confirmation of Service Demands
> **Recommendation 2:** That clauses 5 and 31 of Bill C-22 be amended to require annual public reporting by law enforcement and CSIS and/or the federal government on the use of Confirmation of Service Demands

b. Production orders for subscriber information

Clause 6 of Bill C-22 will create a new "production order" power allowing police to obtain personal information (known as "subscriber information") about the clients of any entity that provides a service to the public based on the very low threshold of "reasonable grounds to suspect" that an offence has been or will be committed, and that information will assist in the investigation of said offence. Instead, the appropriate threshold would be the higher standard

of “reasonable grounds to believe,” which better reflects the sensitive nature of the information in question, and reflects the standard currently used in other similar orders.

These concerns arise from four aspects of the legislation:

First, the information captured by the definition of “subscriber information” goes beyond basic information regarding clients/subscriber and includes potentially highly revealing details not just about the client, but about the services they accessed, the timeframe, and the devices used. This includes:

a. information that may be used to identify the subscriber or client, including their name, pseudonym, address, telephone number and email address;
b. identifiers assigned to the subscriber or client by the person, including account numbers; and
c. information relating to the services provided to the subscriber or client, including
    i. the types of services provided,
    ii. the period during which the services were provided, and
    iii. information that identifies the devices, equipment or things used by the subscriber or client in relation to the services.

Not only is such information very revealing of an individual’s personal life, but the list is also not exclusive of other data. For example, birth dates and physical attributes could also be used to identify an individual; identifiers held by one service provider could be used to reveal information found in another database; types of services provided and dates of service could reveal travel plans, medical history or financial holdings.

Second, this new production order would apply to any service provider, a much broader category of entities than “telecommunications service providers,” as is the case for Confirmation of Service Demands. Instead, “service providers” could include anyone from a health care practitioner to a car rental agency to an email or internet service provider to a financial institution.

Third, this new production order is much broader than existing production orders that require the threshold of “reasonable grounds to suspect”. For example, s. 487.018(1) of the Criminal Code establishes a production order power for financial data. Such a request is restricted to financial institutions only, and establishes a closed list of data that can be requested (as opposed to the open-ended list included in the proposed definition of “subscriber information”). While similar to “subscriber information,” this production order cannot be used to request “any” identifying information, nor all the kinds of services that were provided, nor the devices that an individual used.

Finally, clause 7 of Bill C-22 would allow law enforcement to seek judicial authorization for a “request” to foreign TSPs for either transmission data or subscriber data, also based on “reasonable grounds to suspect.” This new power will have the effect of significantly increasing the pool of personally revealing information which Canadian law enforcement can access on

the basis of a low threshold, and foreign jurisdictions may have weaker data collection and retention rules, further endangering privacy interests.

> **Recommendation 3:** That clauses 6 and 7 of Bill C-22 be amended by replacing "reasonable grounds to suspect" with "reasonable grounds to believe"

Other concerns remain with Part 1. In particular, we support the concerns raised by the Ligue des droits et libertés in its brief regarding the voluntary provision of information as well as the use of publicly available information,[4] and those raised by the CCLA and the Citizen Lab in their brief regarding amendments to the Mutual Legal Assistance regime.[5]

Part 2: *Supporting Authorized Access to Information Act* (*SAAIA*)

Of greatest concern in Bill C-22 is the proposed creation, in Part 2 of Bill C-22, of the *Supporting Authorized Access to Information Act* (*SAAIA*).

Through both public regulations and secret orders, the *SAAIA* would allow the government to require the broadly defined category of "electronic service providers" (ESPs) to make wide-ranging and drastic modifications to their systems to facilitate access for law enforcement and intelligence agencies, as well as retain sensitive personal data about users for up to six months, without adequate safeguards to protect against security vulnerabilities that such orders will create. These vulnerabilities will create substantial risks to the security of information online, including by rendering encryption nearly meaningless. The new regime would also lack adequate accountability or transparency provisions.

The provisions of the *SAAIA* present one of the most significant expansions of state surveillance apparatus of the past 20 years. If enacted, it will threaten not just privacy rights, but associated freedoms such as free expression, freedom of association, and equality rights. It also serves to further entrench the broader ecosystem of secret orders, decision-making and investigations that is a hallmark of Canada's national security and anti-terrorism regime, and which continues to result in police and intelligence service overreach, unjustified surveillance and investigations of racialized and Indigenous communities, and the violation of Canada's domestic and international human rights and civil liberties obligations.

Finally, the provisions of the *SAAIA* are largely unchanged from what was originally presented in Bill C-2. While some new safeguards were introduced in Bill C-22, these are offset by, among other things, the escalation in the order-making powers to include the retention of metadata. Moreover, amendments adopted in the House of Commons around encryption, systemic

---

[4] Ligue des droits et libertés, "Establishing a Surveillance Architecture in Canada." 29 October 2026.
[5] Cynthia Khoo, Tamir Israel, and Kate Robertson. "(Un)forced Errors: Analysis of Proposed Surveillance Law Expansion under Bill C-22,An Act respecting lawful access," *The Citizen Lab and the Canadian Civil Liberties Association*, 2 June 2026. Online at: https://ccla.org/wp-content/uploads/2026/06/2026.06.02-Bill.C22-Citizen.Lab_CCLA-Submission.pdf

vulnerabilities and metadata continue to fail to adequately address the risks posed to our privacy and security. The study in the House of Commons was also hindered by a rushed study, resulting in limited witness appearances, rushed debate, and the inability for briefs to be circulated to committee members in a timely fashion.

Given all the above, and the concerns detailed below, we believe that Part 2 of Bill C-22 should not proceed to Royal Assent, and instead be removed in favor of further study and consultation.

> **Recommendation 4:** Ensure Bill C-22 receives a full study, hearing from civil liberties, human rights, privacy, and cybersecurity experts.
> **Recommendation 5:** Withdraw Part 2 as it can't be amended in a way that upholds Charter rights.

<u>Key issues with Part 2 of Bill C-22:</u>

> **Issue 1:** The definition of electronic service providers is unacceptably broad

The *SAAIA*'s order and regulation making powers will apply to all "electronic service providers" (ESPs), which the bill defines as, "person or group that provides an electronic service to persons in Canada or carries out all or part of its business activities in Canada."

An "electronic service" is further defined as, "a service, or a feature of a service, that involves the creation, recording, storage, processing, transmission, reception, emission or making available of information in electronic, digital or any other intangible form by an electronic, digital, magnetic, optical, biometric, acoustic or other technological means, or a combination of any such means."

The *SAAIA* therefore captures not just large online platforms and telecommunications companies such as Meta, X, Amazon, Bell, and Rogers, but also local bookstores, mental health service providers, financial institutions, travel booking websites, dating sites, and more—essentially anything that allows users to create accounts, communicate, or book appointments online. Some have even questioned whether websites that simply allow commenting would also be included. Even operators of Wi-Fi networks, such as schools, libraries and cafés could be captured. This is an unacceptably broad category, and the government has failed to explain why covering such a wide range of companies is necessary.

ESPs will also include a subcategory known as "core providers"; however, core providers will only be defined by regulation once the *SAAIA* is enacted, so it is impossible to know for certain which ESPs will fall under that category.

Core providers will be subject to public regulations issued by the Governor in Council. While public disclosure is a positive, it is undercut by the Minister of Public Safety's ability to issue

secret orders to all ESPs, including core providers. The secrecy means it will not be possible to know the true scope of orders served on ESPs, core or otherwise. While safeguards exist—such as requiring the Intelligence Commissioner to approve secret orders before they take effect—as explained below, they do not go far enough.

Issue 2: Order making powers threaten privacy and security online

Both the public regulations and secret ministerial orders allowed under the *SAAIA* can be used for the same purposes

Among other things, this includes:

- the development, implementation […] and maintenance of operational and technical capabilities, including capabilities related to extracting and organizing information […] and to providing access to such information;
- the installation, use, operation […] and maintenance of any device, equipment or other thing that may enable an authorized person to access information.
- the retention of categories of metadata for up to six months.

These powers are exceptionally broad even for public regulations, let alone for secret orders. They could be used in ways that are difficult to foresee, with consequences—intended and unintended—that remain impossible to fully anticipate.

Four areas of risk are especially worrisome:

2.1 Bill C-22 will weaken online security and render encryption meaningless

First, the breadth of what ESPs can be ordered to do will weaken protections for private communications and the transmission of data online. This includes the possibility of forcing ESPs to add new access points to their networks to allow for government surveillance or data collection, which would also create openings for other actors – from foreign states to hackers – to exploit to their own ends.

Most concerning, though, is that the *SAAIA* would undermine encryption to the point that it will be meaningless. Bill C-22 would allow the government to order companies to create backdoors, bypass or weaken encryption, or decrypt encrypted data for access by law enforcement and intelligence agencies. As the Mozilla Foundation put it, "there is no safe way to create exceptional access to encrypted data that only the intended actor can use. An access mechanism created for law enforcement can also be discovered, exploited or abused by potentially bad actors."[6]

[6] S. Windwehr and T. Stampelos, "Canada's bill C-22 threatens encryption, users' privacy and the security of digital economies." *Mozilla.org*, 8 October 2026. Online at: https://blog.mozilla.org/netpolicy/2026/10/08/canadas-bill-c-22-threatens-encryption-users-privacy-and-the-security-of-digital-economies/

The government attempted to address these concerns by amending Bill C-22 during debate in the House of Commons to include a caveat to limit decryption (s.2(4)) that would prohibit the orders from forcing a service provider to create a decryption key if none existed. However, it fails to adequately address this flaw in the bill by still leaving open the possibility of either weakening encryption or creating backdoors into encrypted communications, among other encryption-busting tools.

Protection of our private information and communications online is fundamental to be able to exercise all related rights and civil liberties in an ecosystem that has become essential to our everyday activities. Bill C-22 poses a clear threat to these protections.

2.2 Mandatory retention of metadata violates privacy rights

The *SAAIA* would also allow the government to order ESPs to retain users' metadata for up to six months. While this is a reduction from the original requirement to retain metadata for up to a year, it remains an unacceptable risk to privacy rights by forcing the retention of private data without judicial authorization, requiring ESPs to increase the scope of the data that they collect regarding users, and creating a trove of personal information that would be a target for exploitation by companies, foreign governments, bad actors and even Canadian law enforcement and intelligence agencies themselves.

Requiring private companies to retain information about users for eventual use by the government amounts to the deputization of private corporations into government data collection. Metadata may not contain the contents of communications, but it is still highly revealing of our private lives: who we talk to, where we travel, when we engage in activities. It can also expose entire networks of association by linking who speaks to whom, for how long, who travels to the same places at the same times, and so on. This can lead to the creation of problematic, often biased, hypotheses that can (and have) lead to profiling and harassment.

Requiring retention of such personal data therefore engages section 8 of the *Charter of Rights and Freedoms*, protecting against unreasonable search and seizure. As Prof. Michael Geist has pointed out, the result would be "a surveillance map of virtually every Canadian."[7] Under no circumstances should this degree of personal information be ordered retained without judicial authorization. Even then, authorization to retain metadata for six months should be treated as an exceptional circumstance requiring a high burden of proof.

Beyond *Charter* implications, mandatory metadata retention also has significant implications for data security. Such a pool of data would be a treasure trove for hackers, foreign entities, and other malign actors. It would also be ripe for abuse by individuals at the companies collecting the data or by law enforcement with access—as evidenced by multiple documented cases of officers misusing existing databases to track former intimate partners or women they find attractive.

[7] Op. cit. 3

2.3 Secret Ministerial orders undermine accountability, place rights and security at risk

As noted above, the *SAAIA* grants the Minister of Public Safety the ability to issue secret orders to all ESPs, including core providers.

While the *SAAIA* originally excluded any disclosure of these orders, including their content and whether or not an order had been issued, amendments in the House of Commons would now allow the Minister to include, "provisions respecting the disclosure of information contained in [an order] and the disclosure of the fact that the electronic service provider is subject to [an order]." (s.7(1.1))

However, this still leaves too much discretion with the Minister to decide when and how disclosure is allowed. There are no factors guiding what the Minister must consider or grounds on which information should be kept secret. Even with such guidelines in place, the discretionary power of the Minister would remain too broad. This is particularly true given that it would likely be the most controversial orders, or orders that pose the greatest risk to privacy or cybersecurity, that would not be disclosed.

Issue 3: How these powers could be used and associated risks

The powers granted to law enforcement and intelligence agencies under the *SAAIA* are exceptionally broad, particularly for Ministerial orders issued in secret. They could be used in ways that are difficult to foresee, with consequences—intended and unintended—that remain impossible to fully anticipate. Risks that we can envision today, though, include:

- Rapid expansion of state surveillance powers. We have seen in the past how new surveillance powers, especially those exercised in secret, expand over time, resulting in unlawful surveillance and rights violations;
- Backdoors and surveillance systems, once in place, are not limited to use by Canadian law enforcement and intelligence agencies, or Canada's allies:
    - They can also be accessed and exploited by any foreign law enforcement or intelligence agencies.
    - They can be open to attacks, hacks, leaks or misuse.
    - A crucial example is that of the "Salt Typhoon" attack in 2023-24 that exploited backdoors and access points to facilitate US national security intercept capabilities

Finally, the full scope of how this information could be used by law enforcement and intelligence agencies, both domestic and foreign, has not been made apparent by the government's examples. The scenarios provided by the government have included tracking phones used by alleged terrorists, to be able to safely trace and rescue kidnapped children or to address anonymous individuals engaged in the sexual exploitation of minors. However, the potential use goes much further than that:

- Data on location and communications would present even more opportunities for the tracking and surveillance of Indigenous land defenders or other activists, as recently revealed by the CBC. Governments could use this to target any subsection of the population they deem to be a threat to their policies (regardless of actual threats of violence)
- This data could also be used for US-style tracking of immigrants and refugees, as well as naturalized and racialized citizens, in order to facilitate detention and deportations
- The collection and organizing of metadata, about Canadians and about foreign individuals, would be a boon for CSIS' dataset collection powers, already criticized by the National Security and Intelligence Review Agency for operating in novel, unaccountable ways after their adoption in 2019.
- Access by foreign law enforcement, including from the United States, for investigations and prosecutions that threaten entire communities—such as individuals seeking abortion or other reproductive healthcare, or gender-affirming care (including US citizens lawfully accessing such care in Canada).

Issue 4: Inadequate safeguards and unjustified secrecy

While the *SAAIA* has built in safeguards, they are woefully inadequate.

4.1 Systemic vulnerabilities

A key protection that the government has pointed to is the provision of the *SAAIA* that a core provider would not be required to comply with a regulation, and an ESP would not be required to comply with an order, if compliance would result in a provider introducing a systemic vulnerability, or prevent a provider from rectifying a systemic vulnerability, in its service.

However, the definition of a systemic vulnerability in section 2(1) of the *SAAIA* is deeply flawed and raises several substantial concerns. Most alarmingly is that it does not prevent the introduction of vulnerabilities; it only prevents vulnerabilities that would present a "credible risk" of being accessed by unauthorized individuals and only in instances where the information is not related to information regarding persons who are subject to a warrant to other authority to access information. This relies on the premise, though, that such vulnerabilities can be limited to access by authorized individuals. The government states that the threshold will be a "credible risk" that information could be accessed by an unauthorized individual, but this is a highly subjective standard, and leaves open the real possibility that the temptation to create vulnerabilities useful for national security or law enforcement will result in the gradual erosion of that threshold. It is also unclear which "international technical standards" the determination will be based on, providing little reassurance that it will ensure a strong and consistent standard. Finally, as demonstrated by the Salt Typhoon cyberattacks and by recent examples of AI testing for and breaching cybersecurity weaknesses, measuring the future risk of unauthorized access created by vulnerabilities is incredibly difficult—if not impossible.

4.2 Reporting requirements do not replace effective oversight

As described earlier, the scope of secrecy and non-disclosure orders is unacceptable. Secret ministerial orders can cover the full range of ESP system modifications—from the most innocuous to the most significant; predictably, it will be the most sensitive and controversial orders that are issued in secret. The Minister of Public Safety will be empowered to determine whether any disclosure of the contents of an order would be possible, including not just the contents be the very existence of an order. While the Intelligence Commissioner will review orders for their reasonableness, it is not clear thar this would include the Minister's grounds for non-disclosure. Given the scope of the order powers in questions, this degree of secrecy, and discretionary decision making, is unacceptable.

The scope and impact of secret orders merit judicial review, not solely review by the Intelligence Commissioner. While the Intelligence Commissioner is a retired judge operating at arm's length, the position is only as strong as the individual appointed. Given that the appointment is made by the government, it remains susceptible in the future to politicization or resource cuts. Moreover, the deliberations take place in secret, with strict limits on public reporting. Given the significant powers granted to the government under the *SAAIA*, the OIC is not the adequate forum for approving ministerial orders; only judicial oversight would provide the necessary certainty—if secret orders are to be accepted at all.

Nor are these concerns allayed by public reporting requirements, information sharing with the National Security and Intelligence Review Agency or the required review three years after the enactment of the *SAAIA* regime. While reporting and review are necessary for any such regime, they can only address concerns after an order has been made, and do not impose a safeguard before an order is carried out.

Conclusion

In response to Bill C-2, hundreds of civil society organizations spoke out how the bill's new surveillance powers posed a serious attack on fundamental rights in Canada. While Bill C-22 makes modest efforts to address these concerns, it continues to pose not just a risk to privacy rights, but a wide range of associated rights that depend on access to private communications free from undue government surveillance and interference. Bill C-22 also unjustifiably creates cybersecurity risks that will further threaten the private information not just of people in Canada, but all individuals whose data is held by ESPS subject to the new regulations and secret orders regime created in the *SAAIA*. Over the past several months, privacy experts and civil liberties advocates in Canada have been joined by international experts, technology companies and law makers in echoing the need for the government to change course on Bill C-22.

Given these concerns, our coalition is calling on Senators to reject Bill C-22 and to vote against it. Barring that, significant amendments must be made to Part 1, and Part 2 must be withdrawn.