Bill C-22, An Act respecting lawful access

Brief to the Standing Committee on Public Safety and National Security (SECU)

International Civil Liberties Monitoring Group

Submitted May 24, 2026

Introduction

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.

Over the past two decades, we have observed with alarm the rapid expansion of government surveillance tools and networks, often with inadequate safeguards, and concurrent erosion of privacy protections. This includes the collection and retention of traveler data such as Advance Passenger Information / Passenger Name Record Data, granting the Canadian Security Establishment expansive surveillance powers, the use by law enforcement (from local police to the RCMP) of invasive tools like IMSI catchers and facial recognition tools (such as ClearviewAI), millions poured into new surveillance drones and towers to monitor Canada's borders, enabling CSIS to collect entire datasets of non-threat related information, and more. Recent reporting has further revealed the long history of law enforcement and intelligence agencies have surveilled Indigenous and environmental movements without justification.[1]

Our coalition has contributed consistently to these conversations, through op-eds, briefs, consultation submissions and committee appearances.[2]

Time after time, federal governments of all stripes have attempted to weaken privacy protections under the name of 'lawful access,' which others have aptly called "zombie legislation" that keeps returning from the grave. This includes the ill-fated Bill C-30, proposals in the 2016 National Security Green Paper consultation, the 2023 Consultation on the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA), and ultimately, Bill C-2, the now-shelved *Strong Borders Act*. Each time, governments have sought to significantly erode privacy protections under the guise of providing police and CSIS with powers to fight illicit activity – whether it be terrorism, money laundering/terrorist financing or online exploitation. However, each time it has become clear that people across Canada refuse to trade the important protections that privacy laws afford, in exchange for promises of "security" built on nebulous justifications that these powers are necessary for law enforcement. There has also been a pattern, including regarding Bill C-22, that while police and law enforcement argue new investigatory powers are necessary to address novel challenges, evidence demonstrates that tools and powers already exist that would allow them to adequately address these problems. As the Citizen Lab has described it, while law enforcement may present these issues as a

[1] Fenlon, Brodie. "How the RCMP spied on Indigenous organizations — and how we broke the story," *CBC News*, 24 March 2026. Online: https://www.cbc.ca/news/editorsblog/cbc-news-indigenous-rcmp-surveillance-9.7133525

[2] See, for example: https://iclmg.ca/atf-consultation/, https://iclmg.ca/opc-biometrics-consultation/, https://iclmg.ca/mr-paulson-we-have-enough-power-to-fight-cybercrime/, 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/

blockage, in reality they are experiencing investigatory friction: difficulties exist, but investigations can still be carried out effectively.[3]

Even in its recent report on lawful access—which is relatively supportive of new lawful access laws—the National Security and Intelligence Committee of Parliamentarians found that law enforcement and intelligence agencies lack evidence to demonstrate the need for such new powers and have been largely effective without the tools they claim are so urgently needed.[4]

Position on Bill C-22

Our coalition is deeply concerned that, if enacted, Bill C-22 will supercharge state surveillance and seriously threaten privacy rights, with concurrent impacts on free expression, freedom of association, and equality rights. Such an expansion of state surveillance also undermines Canada's adherence to international human rights and civil liberties obligations, including article 2 (equality), article 12 (privacy), article 19 (expression) and article 20 (association) of the Universal Declaration of Human Rights,[5] and article 2.1 (equality), article 17 (privacy), article 19 (expression) and article 22 (association) of the International Covenant on Civil and Political Rights.[6]

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. As detailed above, this is another clear case of the decades-long trend of governments using national security as an excuse to erode civil liberties and human rights.

Bill C-22 is more limited in scope than its predecessor, Bill C-2, focusing solely on lawful access, and includes some modifications that attempt to respond to previous criticisms. However, not only do these changes not go far enough, but the government has added a new data retention provision to Bill C-22 that raises significant additional privacy concerns.

Furthermore, as detailed by Professor Michael Geist in a recent article, the government has once again failed to present convincing evidence or scenarios to justify the legislative reforms they are seeking in this legislation.[7]

---

[3] 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/

[4] National Security and Intelligence Committee of Parliamentarians. "Special Report on the Lawful Access to Communications by Security and Intelligence Organizations," His Majesty the King in Right of Canada, 2025. Online: https://nsicop-cpsnr.ca/reports/rp-2025-09-15-sr/250915_NSICOP_Lawful_access_report.pdf

[5] United Nations. Universal Declaration of Human Rights. 10 Dec. 1948, United Nations UDHR. Online: https://www.un.org/en/about-us/universal-declaration-of-human-rights

[6] United Nations (General Assembly). "International Covenant on Civil and Political Rights." Treaty Series, vol. 999, Dec. 1966, p. 171. Online: https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

[7] 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-

Based on these concerns, our coalition is calling on Members of Parliament to reject Bill C-22 and to vote against it. Should Bill C-22 proceed through Parliament, at a minimum, significant amendments must be made to Part 1, and Part 2 must be withdrawn.

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*, has been changed from Bill C-2 in one significant way: It narrows Bill C-2's previously broad powers for police and intelligence agents to require companies that offer services to the public to provide information about account holders without a warrant, previously known as "Information Demands."

Instead, such requests would now be restricted to telecommunication service providers (TSP) and to simple yes/no answers about whether a TSP holds an account associated with an individual's name, email, phone number, etc. While narrower, the precedent of allowing 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, is still alarming, and raises concerns that it could be broadened in the future as it gains acceptance.

Unfortunately, other serious problems in this section of the legislation have not been addressed.

b. Production orders for subscriber information

Bill C-22 will create a new "production order" power based on the very low threshold of "reasonable grounds to suspect" for police to obtain personal information about the clients of any entity that provides a service to the public (known as "subscriber information").

While "subscriber information" has been described as narrow in scope, it actually captures very broad and revealing information, including:

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.

---

government-tries-to-make-the-case-for-bill-c-22-why-its-own-use-cases-reveal-disproportionate-overreach/ [*Geist 2026*]

Such information can be very revealing about personal aspects of an individual's life, much more so than simple "phone book information". Given the breadth of information included, the threshold of reasonable grounds to suspect is much too low. Instead, at a minimum, the threshold should remain at reasonable grounds to believe – which is the current standard for requesting this kind of information from a service provider.

Bill C-22 will further create a new extra-territorial power, allowing law enforcement to issue a "request" to foreign telecommunications services for information that they hold – again on the same minimal level of "reasonable grounds to suspect."

c. Amendments to the *Mutual Legal Assistance in Criminal Matters Act*

Bill C-22 also proposes to amend the *Mutual Legal Assistance in Criminal Matters Act* by creating a regime whereby foreign entities may submit a request to the Minister of Justice for the production of transmission data or subscriber data that is in the possession or control of a person in Canada. The requests would then go before a judge who could authorize the request. Similar to the new subscriber data production order described above, the request must only meet the low bar of "reasonable grounds to suspect." Once again, this is much too low a threshold on which to authorize the collection of information that can carry serious privacy interests.

Beyond the low threshold, there is no dual criminality requirement—meaning the foreign offence need not also be an offence in Canada—posing serious risks that the Canadian legal system could support investigations into conduct that would not be criminal here. This concern is compounded by the fact that once information is released to a foreign entity, it leaves Canadian legal control and may be used or shared in ways that would violate Canadian law or the *Canadian Charter of Rights and Freedoms*.

Unlike other forms of information sharing by government departments and foreign entities, which can be governed by the *Avoiding Complicity in Foreign Mistreatment Act*, there are no safeguards built into the legislation to weigh the risks that the information disclosed may result in the serious mistreatment of an individual.

Finally, there are serious concerns that these amendments will pave the way for Canada to ratify the Second Additional Protocol to the Budapest Convention (2AP) and to negotiate a CLOUD Act agreement with the United States, both of which pose significant threats to privacy and other human rights. For further analysis, we refer you to the Citizen Lab's report, "Unspoken Implications,"[8] and OpenMedia's brief on Bill C-22.[9]

---

[8] Robertson, Kate. "Unspoken Implications," The Citizen Lab, 16 June 2025. Online at: https://citizenlab.ca/research/a-preliminary-analysis-of-bill-c-2/

[9] OpenMedia. "Brief: Bill C-22, An Act respecting lawful access," OpenMedia, 15 May 2026. Online at: https://openmedia.org/assets/OM_SECU_Submission_-_May_15%2C_2026_shortened.pdf [*OpenMedia 2026*]

For these reasons, we oppose the adoption of Part 1 of Bill C-22.

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

Of greatest concern in Bill C-22 is the proposed creation 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 from law enforcement, as well as retain sensitive personal data about users for up to a year, without adequate safeguards to protect against security vulnerabilities that such orders will create. The new regime would also lack adequate accountability or transparency provisions.

Taken together, 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 presented in Bill C-2. While some new safeguards were introduced, these are offset by, among other things, the escalation in the order-making powers to include the retention of metadata for a year.

While the government claims to have listened to concerns from privacy, civil liberties, and national security experts, this is true only for Part 1. Despite consistent warnings about fundamental flaws in the SAAIA, the government returned with essentially the same framework.

Given all of this, the ICLMG joins others in recommending that Part 2 of Bill C-22 be withdrawn, and urges committee members and all parliamentarians to vote against it.

Issue 1: Application of the SAAIA is overly broad

The SAAIA's order and regulation making powers will apply to all "electronic service providers" (ESPs). While the public may assume this to category to be focused on telecommunications and internet service providers, or large social media and digital communications sites, the scope is much broader.

An ESP is defined as a "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."

While this captures large online platforms and telecommunications companies such as Meta, X, Amazon, Bell, and Rogers, it goes much further. It could also capture 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 website or blog operators who allow messages to be shared 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.

While ESPs will be divided into two categories, core providers and all other ESPs, 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.

The Governor in Council may issue public regulations governing classes of core providers. 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 true scope of orders served on key ESPs will therefore be unknowable, and nothing will be known about orders served on all other ESPs. 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 are overly broad

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;

Both provisions appeared in Bill C-2. However, the government has added a new and deeply troubling provision: the retention of categories of metadata for up to one year.

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.

Scenarios we can envision today include:

- The government, either publicly or in secret, could order ESPs to modify their systems to allow for real-time surveillance of communication, collection and retention of communication information by law enforcement or CSIS, or in other ways to facilitate access to data.
    - Ex: being able to collect real time information over an internet service providers network
    - Ex: creating backdoors in private messaging devices, possibly even encrypted messaging
- The government could order ESPs to organize information they already collect so it is more accessible and useful for law enforcement/CSIS, i.e. CSIS dataset collection
- The government could order ESPs to collect highly-revealing metadata - data about our communications, including senders, recipients, time, date, location, and our activities - for up to a year, with no link to an investigation

What are the risks?

- Rapid expansion of state surveillance powers. We have seen in the past how new surveillance powers, especially those exercised in secret, often expand over time, resulting in rights violations, 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

Two areas of risk are especially worrisome:

First, as discussed in the next section, proposed safeguards around "systemic vulnerabilities" are much too weak. Combined with the breadth of scope for what ESPs can be ordered to do, the result will be an overall weakening of private communications and the transmission of data online. This is particularly true due to the lack of specific and clear protections for encrypted data. The components of the legislation leave open the possibility that under this or future governments, backdoors could be built into encrypted communications. While this may not be encryption keys themselves, they will still be vulnerabilities that could render the protections afforded by encryption meaningless. 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.

Second is the new metadata retention provision, which is unacceptable. It raises serious concerns about the deputization of private corporations into government data collection. Metadata may not contain the contents of communications, but what it reveals about private lives is highly revealing—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, who travels to the same places at the same times, and so on. 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."[10] Under no circumstances should this degree of personal information be ordered retained without judicial authorization. Even then, authorization for a full year of retention should be treated as an exceptional circumstance requiring a high burden of proof.

Beyond the *Charter* implications, it 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 individuals they find attractive.

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 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. Future 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 to accelerate 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 Agency for operating in novel, unaccountable ways after their adoption in 2019.
- Accessed by foreign law enforcement, including the United States, for investigations and prosecutions that threaten entire communities—such as individuals seeking abortion or

[10] *Geist 2026*

other reproductive healthcare, or gender-affirming care (including US citizens lawfully accessing such care in Canada).

Issue 3: Inadequate safeguards & unjustified secrecy

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

First, 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. ESPs will be under indefinite non-disclosure not just regarding the content of an order, but even as to whether they have received any order at all. There is no justification for this level of secrecy over all orders made to individual ESPs.

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 susceptible to politicization or resource cuts. Only judicial oversight would provide the necessary certainty—if secret orders are to be accepted at all.

Nor are they concerns allayed by either the public reporting or the required review three years after the enactment of the SAAIA regime.

At the core of these concerns is that this new regime will further expand the growing number of secret orders, procedures and regimes under the guise of protecting national security. This includes the use of secret trials for security certificates, the closed-door administrative processes underpinning the Passenger Protect Program and the Terrorist Entities List, CSIS' threat reduction powers, and other expanded powers granted under the Combatting Foreign Interference Act, and the CSE's active and defensive cyber operations, among others. All of which is underpinned by the ever-growing use of secret evidence in court. This secret evidence is used in large part to protect against revealing investigative methods used by law enforcement and CSIS; a new regime meant to vastly expand the ability for these agencies to engage in secret investigatory actions will only deepen this problem.

We also echo NSIRA's concern that it is baffling the agency has not been given a greater role in this regime. As NSIRA has suggested, at a minimum it should receive the reports and underlying information to facilitate proactive future review.

The proposed protections against systemic vulnerabilities are also wholly inadequate.

First, as detailed by OpenMedia in its brief,[11] the structure of the SAAIA itself undermines these protections in two ways: first, by granting the government the power to redefine any term in the legislation by mere regulation, and second by both saying that an ESP is not required to

[11] *OpenMedia 2026*

enact an order that would create a systemic vulnerability, but also makes it an offense to not carry out an order.

Even should these legislative issues be resolved, the definition of a systemic vulnerability is deeply flawed. The SAAIA states that a systemic vulnerability is a:

> vulnerability in the electronic protections, including authentication, encryption or other prescribed type of data protection, 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. [emphasis added].**

This protection rests on the notion that it is possible to create a vulnerability that could not, to a high degree of certainty, be accessed by an unauthorized person. First, "substantial risk" is subjective, and leaves open the real possibility that the temptation to create vulnerabilities useful for national security or law enforcement could gradually erode that threshold. Second, as demonstrated by the Salt Typhoon example and by recent AI experiments, measuring the risk posed by vulnerabilities once in place is incredibly difficult—if not impossible. To base a key protection on the assumption that only Canada and its allies will have access to these entry points poses a serious risk to the security of our online communications.

Conclusion

In response to Bill C-2, hundreds of civil society organizations spoke out about the serious attack that it presented on fundamental rights in Canada. Central to this were concerns around new surveillance powers. While Bill C-22 makes modest efforts to address these concerns, it continues to propose legislative changes that 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 electronic service providers subject to the new regulations and secret orders regime created in the SAAIA.

Given these concerns, our coalition is calling on Members of Parliament to reject Bill C-22 and to vote against it. Should Bill C-22 proceed through Parliament, at a minimum, significant amendments must be made to Part 1, and Part 2 must be withdrawn.