Standing Senate Committee on National Security, Defence and Veterans Affairs
The Senate of Canada
Ottawa, Ontario, K1A 0A4
November 19, 2026

Subject: Nearly 13,000 Canadians are petitioning the Senate of Canada to reform encryption-breaking Bill C-22

Dear Senators,

We are writing to deliver our petition to reform Bill C-22, and our amendment recommendations on how best to do it. We are proud to speak for OpenMedia, Canada's community-based non-profit organization of approximately 230,000 dedicated to keeping the internet open, affordable, and surveillance-free.

We believe in strengthening the Canadian public's digital safety; yet as written Bill C-22, the so-called "Lawful Access Act", does just the opposite. The bill allows government authorities to force installation of backdoors into any electronic service provider in Canada that it chooses that will have the effect of compromising encryption. An extraordinary range of companies can also be forced to track and retain six months of the movements and metadata of every user on their services – available to law enforcement on warranted demand.

This proposed legislation is already threatening to chase privacy-first digital services from Canada, including Signal, Proton, multiple VPNs and What'sApp. To comply with such a law, organizations simply cannot operate according to the well-respected principle of Privacy by Design, which includes both data minimization and effective end to end encryption as core technical and organizational measures.

Critically, this is a uniquely poor time for Canada to be weakening organizational cybersecurity, because AI agents are making cyberattacks much faster and easier to carry out. OpenAI, Microsoft and Anthropic are all warning there is a high "possibility of a catastrophic AI-driven cyberattack" in the next 6-12 months, that could cripple banks, hit hospitals, water plants, power systems, and internet infrastructure.

Canadians want laws that close the security gaps instead of creating new ones. Since the Liberal government introduced lawful access provisions in Bill C-2 in 2025, and re-introduced them in Bill C-22, the OpenMedia community has sent nearly 25,000 messages to MPs against these proposals, and over 300 organizations have spoken out against the bill's sweeping surveillance powers. Today we are delivering a new expert letter to Prime Minister Carney, asking him to intervene in Bill C-22's course, and highlighting the legislation's deep incompatibility with European privacy law, and resulting threat to his economic integration agenda.

In our most recent petition, **nearly 13,000 action takers** are calling on Senators to give the surveillance powers of Bill C-22 the full study the House did not. The petition text is included in Appendix A, and a list of signatures available at https://openmedia.org/ReformC22-signatures.

The written submission that follows expands on this petition, and outlines minimum necessary fixes to Bill C-22 before it may be safe for Canadian rights.

Remove Part 2 of Bill C-22; or substantially reduce its surveillance architecture

OpenMedia's position is that Part 2, the SAAIA, should be removed from Bill C-22 entirely. Cybersecurity experts have confirmed for many years that there is no form of mandated technical access capability that is safe for Canadians' privacy or cybersecurity.

If Part 2 is not removed, we urge the Committee to extend its study of Part 2 of the bill with further expert and public witnesses to ensure the legislation works in favour of Canadians' privacy rights, and that the proposed safeguards will not create serious technical vulnerabilities in our systems or threats to our national security, especially in the age of AI-powered cyberattacks.

Haste cannot and should not justify the emergence of a permanent poorly studied surveillance regime. If you do not extend study today, we suggest adding a five-year sunset clause requiring Parliament to reauthorize the SAAIA, preceded by a strengthened mandatory parliamentary review at three years, informed by publication of aggregated operational statistics, an independent assessment by NSIRA, and a Privacy Commissioner report on the regime's operation.

More immediately, we urge you to address serious problems with Bill C-22 through the following targeted amendments:

I. **Define and limit the scope of "electronic service provider" and "core provider" plainly in statute.** Currently, Section 2(1) defines "electronic service provider" (ESP) as any service involving the creation, recording, storage, processing, transmission, or making available of information in electronic form. That captures messaging platforms, cloud storage, email services, social media, device manufacturers, operating system providers, app stores, VPN providers, AI service providers, streaming services, and any foreign company with Canadian users or business activities. This definition is limitless.

The government has said that the heavier default obligations apply only to core providers listed in the Schedule. But the Bill's Schedule is blank. Parliament is being asked to vote on a framework whose actual reach will be determined by Cabinet decisions made after the bill passes, and by successive Cabinets thereafter. This leaves the scope of surveillance obligations outside of Parliament's control. A clearly defined set of core and non-core providers should be set out in the legislation itself.

II. **Address the confusion between core and non-core providers.** Section 7(1) allows the Minister to issue an order to any ESP imposing any obligation that could be

contained in a regulation under section 5(2), including technical capabilities, equipment installation, and metadata retention.

Regulations under section 5 affecting core provider default obligations are public, made by Cabinet, and subject to the Statutory Instruments Act. However, orders under section 7 need not be gazetted. Combined with the section 14 prohibition on disclosure, the practical effect is that a non-core ESP can be quietly compelled by ministerial order to do anything a core provider could be regulated into doing, with neither the public nor Parliament ever knowing. While the amendments made in the House are modest improvements, they continue to leave secrecy as the default: secret orders are capped at two years but can be reissued in identical form, disclosure provisions are at the Minister's option, and section 15 covers regulators only. Canadians deserve better from our government.

We urge the Committee to amend section 7 and 14 so that ministerial orders cannot be used to impose any provider obligations that would otherwise require a public regulation. Ensure that any order imposing technical capability, installation, or retention obligations on a provider—whether core or non-core—is subject to the same public transparency, oversight, and judicial review safeguards.

III. **Remove mandatory metadata retention.** Section 5(2)(d) authorizes regulations requiring core providers to retain categories of metadata, including transmission data, which can include identifiers of devices and accounts involved in a communication and information identifying a device location, for periods of up to six months.

While the bill excludes direct monitoring of content, web browsing history and social media activity, the breadth of metadata collected would still build a standing map of all Canadians' everyday lives, assembled in advance of any investigation, and regardless of suspicion. For a survivor of intimate partner violence, it can reveal their new address, a shelter, their workplace, and their child's school route. For politicians, journalists, human rights defenders, and members of the judiciary, it can reveal who they communicate and interact with, their precise location, and details about their family members, children, sources, and colleagues. This spring when data of 2.9 million Alberta voters was leaked online, the Canadian Anti-Stalking Association reported at least one survivor had to flee their location with their children.

As discussed in our letter to Prime Minister Carney, Europe's highest court has repeatedly struck down general and indiscriminate retention of traffic and location data as incompatible with fundamental rights, as in Digital Rights Ireland (2014), Tele2 Sverige (2016), and La Quadrature du Net (2020).

Outside of lawful, warranted access, mandating this enormous pot of Canadian data gold is extraordinarily dangerous. Dozens or hundreds of diverse service providers that are forced to comply will create new global interest in black hat hacking communities in targeting the affected

providers, at a particularly vulnerable time. Breaches like this are neither hypothetical nor remote risks.

The 2024 Salt Typhoon intrusion is the most consequential cybersecurity event of the last few years, where PRC-linked actors compromised the CALEA-mandated lawful intercept infrastructure of multiple major US telecoms. By August 2025, the FBI identified at least 200 companies in 80 countries affected. In February 2026, PRC-linked actors breached an internal FBI system that held pen register and trap-and-trace surveillance data. Critically, the attackers did not breach the FBI's network directly, but by exploiting a vulnerable commercial ISP vendor's infrastructure.

The lesson is direct and structural. Our government has blamed individual companies for poor cybersecurity practices in these instances, but this misses the point; once vulnerabilities are introduced in dozens or hundreds of different companies' systems, some will always fail to keep up. If the FBI, the leading US advocate of lawful access mandates and an agency with vast security resources, cannot keep its own surveillance data secure once mandatory vulnerabilities are introduced, Canadian providers without those resources will fare worse. Effective digital security in the AI-agent world will require both data minimization - having as little valuable data for as little time as possible, to reduce your attractiveness as a target - and rapid closure of breaches before AI agents hone in on them. Yet Bill C-22's metadata provision demands the opposite – data maximization, in which providers can be asked to keep extraordinary volumes of sensitive, valuable, personal data about Canadians, held within intentionally insecure cybersecurity systems.

Therefore, we urge you to strike the power in section 5(2)(d) to require retention of metadata on all users. Police already have preservation and production orders under Canada's existing preservation framework (Criminal Code ss. 487.012–487.0192) to begin securing relevant data about specific people under investigation. If the Committee declines to remove the provision, cap retention at 30 days, and tie it to specific judicially authorized preservation orders for specific user data. That is the targeted approach that respects the *Charter*, and that people in Canada expect.

IV. **Forbid secret orders that have the effect of circumventing encryption in digital services.** The government's answer to encryption concerns is that providers cannot be required to introduce a "systemic vulnerability" (sections 5(5) and 7(4)). The bill describes a systemic vulnerability as a vulnerability in the electronic protections of an electronic service. That safeguard protects the encryption itself, but not the communications encryption exists to protect.

The best-known methods of defeating encrypted communications are designed to leave the encryption untouched:

- **A "ghost" participant**. The provider silently adds an extra recipient to a conversation. The encryption works exactly as designed; it simply encrypts to one more party than the user knows about. When the UK's GCHQ floated this approach publicly in 2018, it was presented as a way to gain access without breaking encryption.
- **Client-side scanning**. Content is inspected on the user's device before it is encrypted or after it is decrypted, so the encryption is never weakened.
- **Targeted malicious updates**. A provider is compelled to deliver modified software to a particular user that captures their messages or keys.

A government lawyer could argue in good faith that none of these introduces "a vulnerability in the electronic protections of an electronic service." Each one nonetheless defeats the security that users of encrypted services rely on. As drafted, the systemic vulnerability safeguard does not reliably rule any of them out. This is not a hypothetical risk. The United Kingdom's Investigatory Powers Act allows the Home Secretary to issue secret technical capability notices to providers. In 2025, Apple withdrew its Advanced Data Protection encryption feature from users in the UK rather than comply with such a notice. UK users lost a security protection, and the law prevented them from being told why. Section 7 orders, combined with the secrecy imposed by section 14, would allow the same thing to happen in Canada without anyone outside government knowing an order exists.

We urge the Committee to amend the Act so that, for the purposes of sections 5(5) and 7(4), a systemic vulnerability expressly includes any requirement to: (a) add an undisclosed participant or recipient to a communication; (b) scan, monitor, copy or capture content on a device before encryption or after decryption; (c) disclose, escrow, weaken or replace encryption keys, or otherwise reduce the strength of encryption; (d) disable or downgrade end-to-end encryption for any user or class of users; or (e) develop or deliver modified software or updates to particular users in order to enable access to their communications.

We further urge the Committee to amend sections 5 and 7 so that no regulation or ministerial order may require a provider to access, intercept or expose the content of end-to-end encrypted communications, whether *before* encryption or *after* decryption. Finally, secrecy and encryption cannot be separated. Under section 14, a provider could not tell its users that it had been ordered to change how its service works, so Canadians would have no way of knowing whether a service they trust still protects them. The default secrecy of section 14 must end, as outlined below.

V. Strengthen judicial authorization and independent oversight.

Section 7 orders currently take effect with Intelligence Commissioner approval. True public accountability and transparency for a powerful intelligence capacity over private information demands much more than this. We urge the Committee to:

- **Require all section 7 orders to be published in the Canada Gazette**: at issuance in non-emergency cases, and within a fixed statutory period (for example, 90 days) where the Minister certifies exigent circumstances at issuance. Redactions should be permitted only where a Federal Court judge authorizes them under defined statutory criteria.
- **In non-emergency cases, replace Intelligence Commissioner approval with prior judicial authorization**. Non-exigent section 7 orders should require Federal Court approval before taking effect, with an amicus or special advocate to test the application. Emergency orders should be reviewed by the Federal Court within a fixed statutory period (for example, 14 days of issuance) against a necessity-and-proportionality standard, and quashed if they fail it.
- **Return to a 'reasonable grounds to believe' standard.** In current text, the new subscriber-information production order in Part 1 (Criminal Code s. 487.0142) uses the "reasonable grounds to suspect" standard, the lowest threshold in Canadian criminal law, to compel a bundle of information including name, address, phone number, email, IP addresses and device identifiers (IMEI, MAC). R. v. Spencer found that subscriber information attracts a reasonable informational privacy interest, and R. v. Bykovets confirmed the privacy interest in IP addresses specifically. The government's Charter Statement asserts that the information sought "does not, by itself, constitute particularly sensitive information." That cannot be reconciled with the Supreme Court's jurisprudence, and the provision invites Charter litigation that could undo the regime in practice. We urge the Committee to amend section 487.0142 to require "reasonable grounds to believe."

VI. **Separate out concerning cross-border data provisions.** Bill C-22 amends the Mutual Legal Assistance in Criminal Matters Act (MLACMA) so that Canadian authorities can enforce foreign production decisions for transmission data and subscriber information held in Canada. It does so just as Canada is taking on new international data-sharing commitments.

On July 16, 2026, Canada signed the United Nations Convention against Cybercrime, after declining to sign at the treaty's opening in Hanoi in October 2025. The Convention began as a 2017 Russian proposal and is open to every UN member state, including governments with documented records of persecuting journalists, dissidents and minorities. It obliges parties to assist one another in gathering electronic evidence not only for cybercrimes, but for any "serious crime" as each requesting state defines it under its own law. Canada has not yet ratified it; the Convention enters into force once 40 states have done so. Canada also signed the Second Additional Protocol to the Budapest Convention (2AP) in 2023 and has not ratified it, and the government is expected to pursue a CLOUD Act agreement with the United States. Bill C-22 preserves judicial authorization, but the international framework it plugs into weakens the protection that authorization offers in several specific ways:

- **Politically motivated investigations using surface-legitimate framings.** Under MLACMA's dual criminality requirement, a Canadian judge assists a foreign criminal investigation only if the conduct would also be a crime in Canada. That safeguard can be defeated by how the foreign charge is worded. A government pursuing a critic can plead the case as fraud, "extremism," terrorism financing or computer misuse, all of which have Canadian equivalents. In the United States, some state prosecutions in politically contested areas, such as reproductive health, are now pled as homicide, fraud, conspiracy or controlled-substance offences rather than as abortion offences. The framing satisfies dual criminality while the real investigative target stays hidden. A treaty with near-universal membership multiplies the number of governments that can make such requests.

- **Journalist and activist sources.** Canadian journalists protecting US-based sources, and Canadian activists communicating with US-based collaborators, face exposure when the underlying US investigation is pled as an ordinary offence, such as theft of trade secrets, conspiracy, or computer fraud, rather than as a press-freedom matter. Canadian source-protection law and Charter section 2(b) protections do not travel with the data once it is produced under a foreign legal standard.

- **Dual nationals and diaspora communities.** Canadians with ties to states that practise transnational repression are the people most at risk when data flows to foreign law enforcement. The 2AP's own record shows why treaty safeguards are not enough: Serbia, the first state to ratify it, extradited a Bahraini dissident in 2022 in defiance of an interim measure from the European Court of Human Rights. The UN Convention is open to far more states, with weaker shared human rights commitments than the Council of Europe framework.

- **No notice, no remedy.** Canadians whose data is shared under these arrangements will generally never know it, and will have no effective remedy in Canadian or foreign courts. Judicial review at the enforcement stage does not include notice to, or representation of, the person affected.

The Committee should put direct questions to the government on the record: Are the MLACMA amendments in Bill C-22 intended to enable Canada to ratify the UN Convention against Cybercrime, the 2AP, or both? Would ratification require any further act of Parliament? If the answer to the first question is yes and the second is no, the Committee is being asked to approve the domestic machinery for major treaty commitments without Parliament ever debating those treaties. They warrant their own legislative process, including consideration of the reservations Canada would need to protect people in Canada.

The foreign legal environment Canadians are now exposed to is not the one MLACMA was designed for. We urge the Committee to remove the MLACMA amendments from Bill C-22 and table them as standalone legislation, preserving the two-gate structure of the existing MLAT

process: ministerial authorization plus Canadian judicial authorization applying Charter standards before any foreign order is enforced in Canada.

Closing Your Committee is charged with advancing public safety, and Bill C-22 as written is simply not safe for the increasingly hostile digital environment we are entering. We call on you to remove Part 2 from the bill, or fundamentally reshape it along the lines of our recommendations. OpenMedia is available to the Committee for any follow-up questions, and would welcome the opportunity to respond in writing on specific clauses or amendments under consideration.

Sincerely,





Matt Hatfield

Executive Director, OpenMedia

matt@openmedia.org

Jenna Fung

Policy Engagement Manager

jenna@openmedia.org

Appendix A: Petition text

OpenMedia and nearly 13,000 community members demand the Senate of Canada to reform Bill C-22

To: Senate of Canada

We call on the Senate to give the surveillance powers of Bill C-22 the full study the House did not. The House rushed this dangerously broad legislation through clause-by-clause review without hearing wide witness testimony or duly considering needed fixes, as committee MPs themselves flagged. The Senate must fully study Bill C-22, hear all interested parties, and reform it to place limits on its surveillance powers before it becomes law.

Sincerely,

12,935 undersigned