OpenMedia is a community-based organization that safeguards the possibilities of the open Internet.

Bill C-22, An Act respecting lawful access

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

Submitted May 15, 2026

Summary

OpenMedia is Canada's largest grassroots digital rights advocacy community, working to keep the internet open, affordable, and surveillance-free. Our community has sent nearly 20,000 messages to Parliament opposing the lawful access provisions first introduced as Bill C-2, and now reintroduced in Bill C-22. We thank the Committee for the opportunity to contribute to its study.

Part 1 has been meaningfully improved relative to Bill C-2. Yet the most concerning area of Bill C-2 – the proposals now packaged in Part 2 of C-22, the Supporting Authorized Access to Information Act (SAAIA) – have been repackaged from C-2 substantially unchanged. In one critical respect, the new metadata retention regime, Bill C-22 has been very dangerously expanded. OpenMedia's core position, shared by more than 25 leading rights and privacy organizations and experts, is that the bill should be withdrawn. Failing that, the mass surveillance architecture in Part 2 must be removed. This will require either dropping Part 2, or major structural amendments that no amount of regulation-making can supply after the fact.

2. What changed between C-2 and C-22 — and what didn't

OpenMedia acknowledges the improvements the government made in moving from C-2 to C-22. Part 1's information demand power has been replaced with a much narrower confirmation-of-service demand, limited to telecommunications service providers under the Telecommunications Act. Part 2 ministerial orders are now subject to Intelligence Commissioner review under section 9. We thank the Committee and the more than 300 civil society organizations that contributed to that outcome.

What did not change is the core surveillance architecture of Part 2. The SAAIA has been transplanted from C-2 into C-22 with the same vast definitional breadth, the same secret ministerial order-making powers, continued gag provisions, and the same regulatory blank cheque for defining terms like "encryption" and "systemic vulnerability." The apparent safeguards added to Bill C-22 are not functional; they provide the illusion of checks on the Minister's power to break Canadian privacy, not true oversight and limitation of potential future abuse.

On May 7, this Committee heard from Professor Michael Geist, Professor Robert Diab, and David Fraser. Their testimony was substantively aligned on the core flaws of Bill C-22. OpenMedia agrees with their analysis, and does not repeat the detailed legal and technical case they presented in detail here. Our purpose is to amplify their concerns, and identify minimum amendments necessary to address them.

3. Residual concerns with Part 1

3.1 Lowered threshold for subscriber-information production orders (s. 487.0142)

The new subscriber-information production order uses the "reasonable grounds to suspect" standard — the lowest threshold in Canadian criminal law — to compel a bundle of information that includes name, address, phone number, email, IP addresses, and device identifiers (IMEI, MAC). R. v. Spencer found that subscriber information attracts a high informational privacy interest, and R. v. Bykovets confirmed the privacy interest in IP addresses specifically. The Charter Statement asserts that the information sought "does not, by itself, constitute particularly sensitive information." That sentence cannot be reconciled with Supreme Court jurisprudence, and the provision will invite Charter litigation that may overturn the regime's application in practice.

3.2 Cross-border data sharing: MLAT, the CLOUD Act, and the Budapest Convention

For length we will not recap the full concerns here, but refer to and support Citizen Lab's analysis of Bill C-2, which continues to apply. In "Unspoken Implications," Kate Robertson documented that the powers carried forward into Bill C-22 are designed to enable Canada to ratify the Second Additional Protocol to the Budapest Convention (2AP) and to negotiate a CLOUD Act agreement with the United States. Justice Canada officials acknowledged this purpose directly at a June 9, 2025 technical briefing on Bill C-2, and the relevant provisions have been carried forward into C-22. Both frameworks raise serious constitutional and human rights concerns.

We recognize that C-22 preserves judicial authorization. The concern is that protections offered by that authorization are being weakened along several specific dimensions, This shift matters because the foreign legal environment Canadians are now exposed to is not the one MLACMA was designed for. Several real risks follow:

- **Politically charged investigations using surface-legitimate framings.** A Canadian judge reviewing a foreign request under MLACMA's dual criminality requirement assesses whether the named offence is a Canadian offence. U.S. state prosecutions in politically contested areas — reproductive health being the clearest current example — are typically pled as homicide, fraud, conspiracy, or controlled-substance offences rather

than as abortion offences directly. The surface framing satisfies dual criminality; the underlying investigative target is not visible in the request.

- **Journalist and activist sources.** Canadian journalists protecting U.S.-based sources, and Canadian activists communicating with U.S.-based collaborators, face exposure when the underlying U.S. investigation is pled as an ordinary offence (theft of trade secrets, conspiracy, 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.** The 2AP is open to states that have been documented engaging in transnational repression. Serbia, an early ratifier, has used INTERPOL channels to facilitate the rendition of dissidents in violation of European Court of Human Rights injunctions. Canadians with ties to such states could see their data shared with foreign law enforcement through 2AP arrangements — particularly through the Article 7 carve-out from dual criminality.
- **No notice, no remedy.** Canadians whose data is shared under these arrangements will generally never know it has happened, and have no effective remedy in Canadian or foreign courts. Canadian judicial review at the enforcement stage does not include notice to or representation of the affected person.

The Committee should put a direct question to the government on the record: does Bill C-22 enable Canada to ratify the 2AP without further parliamentary action? If so, the Committee is being asked to approve, by indirection, a major treaty commitment that warrants its own legislative process — including specific consideration of the OPC's recommendation to opt out of Article 7.

4. Part 2 is the heart of Bill C-22's problems

OpenMedia's strongly held position is that Part 2 should be removed from Bill C-22 entirely. There is no form of mandatory technical backdoor capacity that is safe for Canadian privacy or cybersecurity. This is a technical reality that has been confirmed many times over many years by cybersecurity experts. If Part 2 is not removed, at minimum four structural problems must be addressed by committee through targeted amendments.

4.1 The scope of "electronic service provider" is virtually unbounded

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, social media, device manufacturers, operating system providers, app stores, VPN providers, AI service providers,

streaming services, and any foreign company with Canadian users or Canadian business activity. As the Canadian Constitution Foundation and David Fraser have both flagged, in a modern digital economy this definition is, in effect, limitless.

The government's response is that the heavier default obligations only apply to core providers listed in the Schedule. This is misleading in two key respects. First as a legislative proposal, this Schedule is blank. Parliament is being asked to vote on a framework whose actual reach will overwhelmingly be determined by successive Cabinet decisions long after the bill passes.

4.1.1 Non-core providers are even more exposed than core providers — not less

Second, there is an additional critical misunderstanding created by Bill C-22's deliberately complex design. A "core provider" faces heavier *default* obligations than other service providers; yet in practice, **non-core providers can face the same substantive obligations through a weaker procedural pathway, and have less recourse to challenge them.** The core/non-core distinction does not protect non-core providers from inappropriately intrusive orders; it only makes these orders face less scrutiny if and when they occur.

- **Same obligations available.** Section 7(1) allows the Minister to issue an order to any ESP — core *or* non-core — imposing any obligation that could be contained in a regulation under section 5(2). That includes all of the technical capabilities, equipment installation, and metadata retention that being a core provider could entail.
- **Worse procedural protection.** Regulations under section 5 affecting core provider default obligations are public, made by Cabinet, and subject to the Statutory Instruments Act. Orders under section 7 are exempted from the Statutory Instruments Act (s. 7(6)) and are not gazetted. Combined with the section 15 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.
- **Weaker resources for compliance and challenge.** Smaller, potentially non-core providers — including small Canadian cloud providers, privacy-focused messaging apps, encrypted email services and so on — have fewer legal and technical resources to challenge an order under section 8, or to engineer compliance without making errors that break their security model. The result is that the providers Canadians turn to specifically for privacy are the providers most exposed to undocumented surveillance mandates. The rash of announcements from companies such as Signal, Windscribe and NordVPN over the last few days reflect this vulnerability.

4.2 Mandatory metadata retention is mass surveillance

Section 5(2)(d) authorizes regulations requiring core providers to retain categories of metadata, including transmission data, for periods of up to one year. On a mobile network, that captures every cell tower a device connects to and when. Aggregated across the population, that is a comprehensive surveillance map of where Canadians go, who they communicate with, and when — retained, in advance of any investigation, regardless of suspicion. This is an extraordinary, unprecedented expansion of mandatory data collection on ordinary Canadians, and wildly out of step with comparable democratic jurisdictions. The Court of Justice of the European Union struck down similar proposals 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. This is discussed further in section 5.

4.3 The systemic vulnerability safeguard is hollow

Sections 5(5) and 7(5) of Bill C-22 provide that a provider "is not required to comply" with a regulation or order if compliance would require introducing a systemic vulnerability. On its face this sounds like a backdoor prohibition. It is not. Three structural problems hollow it out:

- Sections 12 and 13 make compliance unconditional, and provide that orders prevail over inconsistent regulations. As Professor Geist told this Committee on May 7: "that leaves a safeguard that exists in name only, that is cloaked in secrecy, with the burden of invoking it falling on the provider."
- Section 47(1)(c) gives the Governor in Council the power to define "any term or expression" in the Act by regulation. Critical, foundational terms such as "Electronic service provider," "encryption," "systemic vulnerability" and so on can be reinterpreted in their meaning by Cabinet without returning to Parliament. As a result, any protections afforded by the sections that describe them are only as strong as the government of the day decides they are.
- The "systemic vulnerability" carve-out in Bill C-22 covers encryption and authentication, but not the active, operational layer where most data exists within most systems, most of the time. A communications service involves far more than the encrypted-in-transit and authentication moments the safeguard protects. Data is decrypted on servers for spam filtering, abuse detection, indexing, search, advertising, and recommendation systems. It is processed in plaintext at API boundaries, message queues, logging pipelines, backup systems, and operational tooling. Metadata is generated and stored unencrypted by design. An order that compels a provider to install interception capabilities at any of

these points — to retain content in a new unencrypted store, to add a hook to the abuse-detection pipeline, to instrument the logging system, to provision a copy of the message queue — would not introduce a 'systemic vulnerability' within the meaning of sections 5(5) and 7(5), because nothing in the encryption or authentication system would have been weakened.

4.4 Secret orders, sweeping gag provisions, and limited oversight

Ministerial orders under section 7 are not registered publicly, not gazetted, and not subject to the Statutory Instruments Act. Section 15 prohibits the provider — and any person acting on its behalf — from disclosing the existence of the order, the information it contains, the information the Minister relied on, or the fact that the provider is subject to it.

The Intelligence Commissioner review added in section 9 is a meaningful improvement on C-2, but it is a reasonableness review of the Minister's decision, conducted ex parte, without an adversarial proceeding, without a special advocate, and without notice to affected users. This is not how we protect genuinely contesting interests such as public safety and the right to privacy in a democratic society.

5. Salt Typhoon, the FBI breach, and why "poor digital hygiene" is the wrong frame

5.1 Salt Typhoon: the empirical demonstration

The 2024 Salt Typhoon intrusion is the most consequential cybersecurity event of the last few years, and was directly enabled by similar but less sweeping legislation than Bill C-22. PRC-linked actors compromised the CALEA-mandated lawful intercept infrastructure of multiple major U.S. telecommunications carriers, and maintained access to those networks for months. By August 2025 the FBI identified at least 200 companies in 80 countries affected.

5.2 The February 2026 FBI breach

Salt Typhoon was not an isolated event. In February 2026, China-linked actors breached an internal FBI system. The compromised system held pen register and trap-and-trace surveillance data — records of call patterns, phone numbers, and websites visited by people the FBI was actively monitoring. Bloomberg reported the intrusion exposed sealed investigative records.

Critically, the attackers did not breach the FBI's network directly. They got in by exploiting a commercial ISP vendor's infrastructure — the same CALEA-mandated lawful intercept infrastructure that Salt Typhoon exploited at AT&T and Verizon in 2024.

The lesson is direct, and structural. The FBI — the agency that has most aggressively advocated for lawful access mandates in the U.S., with the most resources and the highest baseline operational sophistication — cannot keep its own surveillance systems secure from PRC-linked actors when those systems sit on top of a mandated intercept framework. Mandating equivalent systems across the Canadian digital sector, including non-core providers without comparable resources, multiplies that risk surface many times over.

5.3 C-22 is worse than CALEA in several respects

The government has implied that Bill C-22 simply brings Canada into line with U.S. and G7 practice. That comparison grossly understates how much further C-22 reaches than the U.S. statute Salt Typhoon exploited.

- **Far broader scope.** CALEA applies to telecommunications carriers and equipment manufacturers - a critical layer of our tech stack, but only one layer. C-22's SAAIA scopes in any "electronic service provider" — including messaging apps, cloud services, AI services, email, social media, device manufacturers, operating systems. As the chairs of the U.S. House Judiciary and Foreign Affairs Committees confirmed in a May 2026 letter to Minister Anandasangaree, "the U.S. law does not apply to 'electronic service providers' — which could include social-media services and other businesses — as proposed in Canada."
- **Mandatory retention that CALEA never required.** CALEA does not require carriers to retain communications data in advance. C-22 explicitly authorizes regulations requiring retention of metadata for up to one year. Illicit backdoor operations are often a time-limited proposition; while the Salt Typhoon hackers had months of access, other attackers may have access to a system for just days, even hours. By requiring our services to collect, retain, and prepare for easy handover these data troves, Canada is forcing them to create lucrative, highly saleable hacking targets whose disclosure would compromise every affected person in Canada's privacy. Salt Typhoon demonstrated what happens when intercept systems are compromised; but mandated retention databases multiply the volume and value of exploitable information many times over.
- **Secret ministerial orders CALEA does not authorize.** CALEA operates through public rulemaking. C-22's section 7 orders are exempted from the Statutory Instruments Act, are not gazetted, and are accompanied by a permanent gag on the provider. As David Fraser told this Committee, "the UK equivalent of a Ministerial Order was used by the UK government to secretly order Apple to remove encryption on iCloud globally. Part 2 of Bill C-22 does not contain any guardrails that would prevent that overreach."

5.4 Blaming providers for Salt Typhoon is wrong as a matter of fact and policy

The government and supporters of expanded lawful access have argued that Salt Typhoon was a story of poor cybersecurity hygiene by a few American telcos. This framing misunderstands what mandates do. When the government mandates surveillance capabilities across an entire sector, some providers failing on security is not an individual failure — it is a statistical inevitability. The wider the mandate, the more providers, the more attack surface, the more certain the eventual compromise. C-22 is broader than CALEA in every dimension: more providers covered, more capabilities required, more data retained. The certainty of compromise is correspondingly higher.

6. The new threat environment: frontier AI is changing the math

On April 7, 2026, Anthropic announced Claude Mythos Preview, a frontier AI model that autonomously identifies zero-day vulnerabilities and constructs working exploits across every major operating system and major web browser. Anthropic determined the model was too dangerous to release publicly and is making it available only through a restricted partner program.

Mythos Preview has already identified thousands of high-severity zero-day vulnerabilities. Its capabilities have been repeatedly independently verified, with the UK's AI security institute warning: *Mythos Preview can exploit systems with weak security posture, and it is likely that more models with these capabilities will be developed…. future frontier models will be more capable still, so investment now in cyber defence is vital.*

Three points follow directly. **First, the attacker timeline has collapsed.** What used to take elite security researchers weeks now takes a frontier model just hours, with much less need for specialized expertise. **Second, Mythos-class capabilities will proliferate.** Anthropic's own team estimates similar capabilities will emerge from other labs within six to eighteen months. Some of those labs will not implement the same access restrictions Anthropic has, and the techniques will eventually become available to state and non-state adversaries. We can expect Mythos quality attacks and better to become common at roughly the same time vulnerabilities now required by C-22 are being introduced to Canadian digital infrastructure. **Third, the C-22 scope problem is a huge attack-surface problem.** CALEA narrowly applied to U.S. telecom carriers, who have the resources and years of experience to somewhat harden their mandated systems. C-22 scopes in many smaller companies with neither these resources nor the operational maturity. Mandating intercept capacity across that broader set, at exactly the

moment AI-augmented adversaries are rapidly gaining the ability to find and chain vulnerabilities, is the wrong policy at the worst possible time.

7. Minimum necessary amendments to Bill C-22

OpenMedia's preferred outcome is the withdrawal of Bill C-22, or the complete removal of Part 2 of Bill C-22. If Part 2 proceeds, the following amendments are the minimum necessary to bring the regime within the Charter framework, mitigate the security risks identified by international precedent and the changing threat environment, and restore meaningful parliamentary and public accountability.

Scope

1. Define "electronic service provider" and "core provider" plainly in statute. Fix Schedule 1 in the bill itself.
2. Limit the "core provider" category to telecommunications service providers as defined under the Telecommunications Act — the same scope as the narrowed Part 1.
3. Remove section 7; or at minimum require all section 7 orders are made publicly, gazetted, time-limited, and subject to a strict necessity-and-proportionality test reviewable by a court.
4. Plainly exclude end-to-end encrypted messaging services, zero-knowledge cloud storage, and privacy-enhancing technology providers from the substantive obligations in sections 5(2) and 7.

Metadata retention

5. Strike section 5(2)(d) entirely. Canada's existing preservation framework (Criminal Code ss. 487.012–487.0192) provides the targeted tools law enforcement needs. If the Committee declines to remove the provision, cap retention at 30 days and tie it to specific judicially authorized preservation orders.

Encryption and systemic vulnerabilities

6. Define "systemic vulnerability" in statute to cover the full operational surface of the service, not just encryption and authentication. The current statutory definition turns on "electronic protections" — encryption and authentication. As discussed above, this leaves the operational layer (logging pipelines, abuse-detection systems, message queues, backup systems, indexing, recommendation pipelines) available for mandated interception while creating the impression that communications are protected.

7. Remove the Governor in Council's power under s. 47(1)(c) to redefine these terms by regulation.

8. Add an express statutory prohibition on orders that would require providers to weaken security at any layer — encryption, authentication, or operational. This should include orders that would require: developing, installing, or maintaining decryption capabilities for end-to-end encrypted services; weakening security at the operating system or device level; extending data retention beyond what the service operationally requires; altering plaintext operational pipelines for the purpose of interception; or retaining copies of message queues, logs, or backup systems for the purpose of authorized access.

Transparency and oversight

9. Strike section 7(6) and require all section 7 orders to be published in the Canada Gazette. Orders should be published at time of issuance in non-emergency cases, and within a defined statutory time period (e.g., 90 days) where the Minister certifies exigent circumstances at issuance. Redactions should be permitted only where authorized by a Federal Court judge applying defined statutory criteria.

10. In non-emergency circumstances, replace Intelligence Commissioner review with prior judicial authorization. Non-exigent Section 7 orders should require Federal Court approval before they take effect, with provision for an amicus or special advocate to test the application. Emergency orders should be reviewed by the Federal Court within a defined statutory time period (e.g., 14 days of issuance) against a necessity-and-proportionality standard, and quashed if they fail to meet it.

11. Amend section 15 to require aggregate transparency reporting by providers, including the number of orders received and the categories of obligations imposed, on a delayed-publication basis.

12. Add a five-year sunset clause requiring Parliament to reauthorize the SAAIA, preceded by a mandatory parliamentary review at three years, informed by publication of aggregate operational statistics, an independent assessment by NSIRA, and a Privacy Commissioner report on the regime's operation.

Cross-border data sharing

13. Remove the MLACMA amendments from Bill C-22, and table them as standalone legislation.

14. Preserve the two-gate structure in the existing MLAT process: ministerial authorization plus Canadian judicial authorization applying Canadian Charter standards before any foreign order is enforced in Canada.

Charter and subscriber information

15. Amend section 487.0142 of the Criminal Code to apply the “reasonable grounds to believe” standard rather than “reasonable grounds to suspect.”

8. Closing

Canadians have heard a version of this debate before. In 2012, Bill C-30 was withdrawn after a public outcry. In 2014, the Supreme Court decided Spencer. In 2024, it decided Bykovets. In 2025, more than 300 organizations united against Bill C-2 and the government withdrew its warrantless demand powers. When surveillance powers are made visible, debated transparently, and tested against the Charter, Canadians do not accept them.

Your Committee is charged with advancing public safety, and Bill C-22 as written is simply not safe. The threat environment is more, not less, hostile than when the Salt Typhoon attack initially occurred. The bill is broader, not narrower, than the U.S. statute Salt Typhoon exploited. The case for restraint has strengthened, not weakened, since C-2 was first tabled.

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 to specific clauses or amendments under consideration.