Bill C-22

An Act respecting lawful access

Remaining Matters After the June 18, 2026, Revisions on Third Reading in the House of Commons

Submitted to the
Standing Senate Committee on National Security, Defence and Veterans Affairs
(SECD)

By Louis-Philippe Noël, MBA

Note:

SECU = Standing Committee on Public Safety and National Security (SECU) – House of Commons

1. General Assessment of the Adopted Amendments

Bill C-22, as passed at third reading in the House of Commons on June 18, 2026, represents a genuine improvement over the original text introduced in March 2026. The amendments adopted by the SECU Committee demonstrate that serious consideration was given to the concerns raised by several stakeholders, including the Privacy Commissioner of Canada (OPC), the Quebec Bar Association, Google, and citizens who submitted briefs.

Four developments deserve recognition. The reduction of the metadata retention period from twelve to six months, coupled with a “necessity” criterion, is a step in the right direction. The requirement for prior approval by the Intelligence Commissioner for ministerial orders and the limitation of such orders to two years strengthen the oversight mechanism. The improvement to the threshold defining systemic vulnerability by reference to recognized international technical standards partially addresses a shortcoming identified in several briefs. Finally, the provision allowing for the disclosure of breaches related to ministerial orders to regulatory authorities addresses the OPC’s central concern.

After acknowledging these advances, this brief will focus solely on the unresolved issues that the Senate has the authority and constitutional responsibility to address before the bill receives royal assent.

2. Comparison Table: Initial Version and Adopted Version

The following table summarizes the main changes and identifies the remaining challenges.

Provision	Initial version (March 2026)	Version adopted on the 3rd reading (June 18, 2026)	Remaining issue
Metadata Retention	Up to 12 months, universal and preventive	Reduced to 6 months; essentiality criterion added	Universal retention maintained— constitutional risk remains (Bykovets)
Encryption Protection	"Substantial" vulnerability — threshold too high	Recognized international technical standard — improved threshold	End-to-end encryption not explicitly protected; unregulated access to camera and microphone
Secret Ministerial Orders	Indefinite / no fixed expiry	Limited to 2 years; prior approval by the Intelligence Commissioner	Lack of judicial authorization; permanent gag order still in effect
Standard of Proof (Orders to Produce Documents)	"Reasonable grounds for suspicion" — low threshold	Unchanged	Unconstitutional according to Spencer, Bykovets, and R. v. West
Oversight by the OPC / equivalent authorities	Absent	Disclosure Authorized to the NSIRA	OPC or its successor (C-34/C-36) not included in the main oversight mechanism
Definition of "service provider"	Too broad — hospitals, law firms, Equifax	Unchanged	Risk of accessing medical, legal, or financial records without specific supervision

3. Remaining Challenges: Analysis and Recommendations

3.1 Mandatory metadata retention remains unconstitutional

The amendment reducing the retention period from twelve to six months and adding an "essentiality" criterion is a step forward, but it does not resolve the fundamental constitutional problem. Section 5(2)(d) of the *Supporting Authorized Access to Information Act* (SAAIA) maintains the principle of preventive and universal retention of metadata concerning all users of the targeted providers, without any suspicion of unlawful activity.

The Supreme Court of Canada, in *R. v. Bykovets (2024 SCC 6),* ruled by a majority that the IP address itself is protected by section 8 of the *Canadian Charter of Rights and Freedoms*, as it constitutes the key to accessing an individual's Internet activity and, ultimately, their identity. Justice Karakatsanis, writing the majority opinion, explicitly rejected any piecemeal approach to privacy protection: constitutional protection is assessed based on the totality of information that a piece of data is capable of revealing. Metadata retained for six months makes it possible to reconstruct a person's movements, habits, relationships, and lifestyle, thereby constituting what the Court calls the "biographical core" protected by the Charter.

International experience confirms this constitutional vulnerability. The Court of Justice of the European Union struck down the European Data Retention Directive (Digital Rights Ireland, 2014) and subsequently reaffirmed this principle in Tele2 Sverige (2016) and SpaceNet (2022): only targeted data retention, linked to specific threats, is compatible with fundamental rights. Australia, which adopted a mandatory two-year retention regime in 2015, has documented systemic abuses, including unauthorized access by the ACT Police to more than 3,000 user records and requests for access by agencies with no national security functions. **[1]**

The targeted data retention mechanism already provided for in section 487.012 of the *Criminal Code* is a practical alternative that is constitutionally sound and aligned with international best practices. It allows a peace

officer to order the retention of existing data when there are reasonable grounds to suspect an offence. This mechanism achieves the operational objective of data availability without creating a preventive surveillance database that affects the entire population.

Recommendation 1 — Replace mandatory retention with targeted preservation

The Senate is expected to amend Section 5 (2)(d) of the SAAIA to remove the mandatory metadata retention requirement and replace it with a strengthening of the existing targeted preservation mechanism (Sec. 487.012 of the Criminal Code), supplemented, if necessary, by a time-limited preventive preservation authority applicable only to categories of data identified in the context of a specific investigation.

3.2 End-to-end encryption, the camera, and the microphone must be protected by a judicial warrant

The amendment to the systemic vulnerability threshold is a genuine technical improvement, but it remains insufficient in three critical areas.

First, end-to-end encryption (E2EE) is not explicitly protected in the text of the bill. The SAAIA could be interpreted as authorizing ministerial orders requiring providers to weaken their cryptographic infrastructure, even if this does not constitute a "systemic vulnerability" as defined. Google, in its brief to the SECU committee, proposed specific wording to this effect, which was not adopted.

Second, access to the camera and microphone on users' devices is not governed by any specific provision in the bill. If these interception capabilities were imposed by secret ministerial order, they would constitute the most serious form of intrusion into the private sphere protected by the Charter, without any judicial warrant being required.

Third, academic research in European fundamental rights law establishes that any measure that negatively affects the availability, application, or effectiveness of encryption technologies constitutes an interference with the right to privacy and freedom of expression (Van Daalen, "The right to encryption: Privacy as preventing unlawful access," *Computer Law & Security Review*, vol. 49, 2023). **[2]**

This analytical framework is relevant to the interpretation of section 8 of the Canadian Charter: the risk of unauthorized access—by criminals or foreign governments—created by the weakening of encryption is itself an infringement on privacy, regardless of any authorized government access.

The current system of secret ministerial orders requires only the approval of the Intelligence Commissioner—an oversight official, not a court. For measures affecting encryption or access to a device's components, the minimum constitutional standard requires judicial authorization, as established by the Supreme Court in *Hunter v. Southam* as early as 1984.

Recommendation 2 — Explicit Protection of Encryption and Mandatory Judicial warrant

The Senate should amend the SAAIA to: (a) include in the definition of systemic vulnerability any requirement that has the effect of weakening, circumventing, or compromising end-to-end encryption; (b) require that no ministerial order may compel access to a device's camera, microphone, or encrypted communications without prior authorization from a Federal Court

judge; (c) specify that a provider cannot be compelled to decrypt communications that it did not encrypt itself, and extend this protection to authentication mechanisms.

3.3 The evidentiary standard for production orders remains unconstitutional

Bill C-22 maintains the threshold of "reasonable grounds to suspect" for orders to produce subscriber information (section 487.0142 of the *Criminal Code*). This threshold is lower than the "reasonable grounds to believe" required for other types of warrants involving personal information.

In *R. v. West, 2020 ONCA 473*, the Ontario Court of Appeal struck down a production order because the authorization was based on the lower threshold of "reasonable grounds to suspect" rather than "reasonable grounds to believe," finding a violation of section 8 of the Charter. The Quebec Bar Association expressly raised this issue before SECU, and the OPC also highlighted the risks associated with an order targeting sensitive subscriber information based on mere reasonable suspicion.

The lack of protection for medically or legally privileged information in section 487.0142, combined with the broadening of the scope of application to include individuals "providing services to the public," creates a real risk that mental health, addiction treatment, or legal consultation records could be accessed based on a mere suspicion. This is precisely the type of intrusion into the core of a person's private life that Canadian constitutional case law prohibits.

Recommendation 3 — Raise the standard of proof and protect sensitive professions

The Senate should amend section 487.0142 of the *Criminal Code* to: (a) replace the threshold of "reasonable grounds to suspect" with that of "reasonable grounds to believe," thereby bringing the provision into line with the constitutional requirements established in *R. v. West*; (b) include an explicit exclusion for information protected by attorney-client privilege, medical-client privilege, and therapeutic privilege, equivalent to that provided for in section 487.0121(3).

3.4 The Privacy Commissioner must be integrated into the oversight mechanism

The adopted amendments require that ministerial orders be disclosed to the NSIRA within 30 days. This is a significant step forward, but it does not address a fundamental institutional question: Who monitors the impact of the SAAIA on the privacy of ordinary Canadian citizens—not from an intelligence perspective, but from the perspective of individual rights?

The NSIRA is a security intelligence oversight body. Its mandate is distinct from that of the OPC, whose legal function is specifically to oversee the compliance of government practices with the requirements of the Privacy Act. The OPC, in its own submission to the SECU Committee (Recommendation 8), explicitly requested that providers be allowed to report data breaches related to ministerial orders to the OPC. This request was only partially granted.

Bills C-34 and C-36 [1] could substantially alter federal governance of digital matters, online security, and the protection of personal information. In this evolving context, it would be inconsistent for the SAAIA to create such an intrusive regime of technical access, metadata retention, and secret ministerial orders without formally

[1] Bills reviewed on June 18, 2026, introduced in the House of Commons in June 2026 in their first-reading versions.

incorporating the federal authority responsible for privacy protection—whether it be the current OPC or any institutional structure called upon to perform equivalent functions.

Recommendation 4 — Formal integration of the OPC or its institutional successor

The Senate should amend the SAAIA to: (a) require that any retention order or ministerial order imposed under sections 5(2) and 7(1) be subject to prior review by the Privacy Commissioner of Canada, or any equivalent authority established under Bills C-34 or C-36; (b) provide an exemption from the confidentiality rules in section 15 to allow providers to disclose to the OPC any data breaches resulting from a ministerial order; (c) include the OPC in the mandatory parliamentary review process scheduled for the third year.

4. Conclusion

Bill C-22, in its current form, is a necessary but incomplete piece of legislation. The House of Commons has done a thorough job of amending the bill, and several of the most pressing concerns have been partially addressed. It is now up to the Senate to fulfill its constitutional role as a revising chamber by addressing the four issues that remain unresolved.

Mandatory metadata retention, even if limited to six months, exposes Canada to a serious risk of constitutional invalidation under Section 8 of the Charter, in light of *Bykovets* and comparable international case law. The lack of explicit protection for end-to-end encryption and judicial oversight of access to devices creates a blind spot that is democratically unacceptable. The lowered evidentiary threshold for production orders is directly contradicted by the case law of the Ontario Court of Appeal. And the exclusion of the OPC from the primary oversight mechanism deprives the regime of its most legitimate institutional guardian.

These four amendments are technically straightforward, politically realistic, and constitutionally necessary. They do not compromise the bill's operational effectiveness. They strengthen its democratic legitimacy and long-term legal soundness. It is preferable for Parliament to adopt them before the courts impose them.

Respectfully submitted,

Notes et references

1. ACT Police Admit They Unlawfully Accessed Metadata More than 3,000 Times ». The Guardian, July 26, 2019. https://www.theguardian.com/australia-news/2019/jul/26/act-police-admit-unlawfully-accessed-metadata-more-than-3000-times. See also: *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015 (*Cth). Australia.

2. Daalen, O. L. van. 2023. "The Right to Encryption: Privacy as Preventing Unlawful Access." *Computer Law and Security Review* 49 (July). https://doi.org/10.1016/j.clsr.2023.105804.

3. The documents filed with the SECU of the House of Commons regarding Bill C-22 consist primarily of briefs from the Quebec Bar Association and other Bar associations. They also include a submission from the Privacy Commissioner of Canada (Philippe Dufresne). Other submissions come from Google and other tech companies, and the Justice Centre for Constitutional Freedoms (John Carpay) with other civil liberties organizations and individuals.