Justice Centre
for Constitutional Freedoms

253-7620 Elbow Drive SW,
Calgary, AB, T2V 1K2

Privacy is the shield of a free people

How Bill C-22 undermines Canadians' right to privacy

Brief to the Standing Committee on Public Safety and National Security

Submitted by:
John Carpay, B.A., LL.B.

May 12, 2026

Introduction

Bill C-22 significantly expands state surveillance powers in the digital age. While presented as modest legislation "to keep Canadians safe" and "to disrupt crime, investigate serious threats, and protect our communities,"[1] this legislation risks undermining the fundamental right to privacy protected by section 8 of the *Canadian Charter of Rights and Freedoms*.

Bill C-22's most troubling features are:

- the creation of new production order powers for subscriber information on the lower standard of "reasonable suspicion" rather than "reasonable belief," and
- the creation of a mandatory data retention and backdoor-access regime under the *Supporting Authorized Access to Information Act (SAAIA)*

These aspects of Bill C-22 threaten to expose information about the biographical core of Canadians to government and law enforcement. Such measures invite constitutional challenges and erode the trust that free citizens place in their government.

We urge this Committee to recommend substantial amendments, without which Bill C-22 should be rejected. Canadians deserve security without sacrificing privacy.

What Bill C-22 actually does

Bill C-22 has two main parts. Part 1 amends the *Criminal Code* and *CSIS Act* to create "timely access" to information. This includes:

- A new power for police to demand that any telecommunications service provider (and potentially others) confirm whether they provide services to a specific person or identifier (new s. 487.0121), on mere reasonable suspicion and, notably, **without judicial oversight**.
- A new production order (new s. 487.0142) that allows police to then obtain "subscriber information" from **anyone who provides services to the public**. The Bill states: "a justice or judge may order a person who provides services to the public to prepare and produce a document containing all the subscriber information…"[2] This includes names, addresses, account details, types of services received, and device identifiers. It applies on the lowered threshold of reasonable suspicion rather than the higher threshold of reasonable grounds to believe, which the Supreme Court has stated is the presumptively required standard for authorizing searches in circumstances where a person has an undiminished reasonable expectation of privacy.[3]

---

[1] Government of Canada, "Canada introduces new tools for law enforcement to investigate threats and keep Canadians safe," Canada.ca, March 13, 2026. Available at: https://www.canada.ca/en/public-safety-canada/news/2026/03/canada-introduces-new-tools-for-law-enforcement-to-investigate-threats-and-keep-canadians-safe3.html

[2] Bill C-22, *An Act respecting lawful access*, 1st Sess, 45th Parl, 2026, first reading March 12, 2026 [Bill C22].

[3] *Hunter v. Southam Inc.*, [1984] 2 S.C.R. 145 at p. 167-168.

Police can first use the warrantless confirmation demand under s. 487.0121 to identify the relevant service provider. They can then rely on that confirmation when applying for the production order. This new production order power could even apply to doctors, psychologists, lawyers, counsellors, and other professionals whose records touch the most intimate aspects of a person's life.

Part 2 enacts the *Supporting Authorized Access to Information Act* (*SAAIA*). This broad statute defines "electronic service providers" so expansively that it covers virtually every business with a digital presence in Canada. It empowers the government to force these companies to build technical capabilities and "backdoor access" to make users' data easier for authorities to seize, and to retain metadata (including location and transmission data) for up to one year, even though such data may otherwise be routinely deleted.

Under section 7 of *SAAIA*, the Minister of Public Safety can issue targeted and secret orders against any specific electronic service provider. These orders require the company to implement the above capabilities and retention rules. They need only the approval of the Intelligence Commissioner (not a court) and are accompanied by heavy gag provisions that prohibit the company from ever disclosing that an order exists.

Instead of police obtaining a warrant and then asking a company for specific data in a specific case, Bill C-22 would empower the government to force private companies to redesign their systems in advance so that data from millions of ordinary Canadians is continuously available, organized, and ready for quick handover.

Charter violations

Section 8 of the *Charter* guarantees everyone the right to be secure against unreasonable search or seizure. As the Supreme Court has repeatedly affirmed, this right protects a reasonable expectation of privacy, particularly in information that reveals the "biographical core" of a person's life.[4] This constitutional protection underpins personal autonomy, dignity, privacy, control over our personal information, and freedom from state surveillance.

The Supreme Court of Canada has repeatedly affirmed that section 8 of the *Charter* protects a broad and meaningful right to privacy in the digital age. In *R v. Spencer* (2014), the Court held that privacy includes the right to control the dissemination of personal information and emphasized that anonymity is a central component of that protection.[5] The Court has further recognized that individuals maintain a reasonable expectation of privacy in their electronic communications, even when those communications are stored or transmitted through third-party systems.[6] Most importantly, the Court has

[4] *Figueroa v. Canada (Attorney General)*, 2003 SCC 37 at para. 20; *R. v. Plant*, 1993 CanLII 70 (SCC), [1993] 3 S.C.R. 281 at p. 291.
[5] *R. v. Spencer*, 2014 SCC 43 at paras. 38–41.

[6] *R. v. Marakah*, 2017 SCC 59 at paras. 27–52 (reasonable expectation of privacy in text messages stored on a third-party cellphone); *R. v. Reeves*, 2018 SCC 56 at paras. 28–30 (privacy in data stored on a shared computer).

cautioned that the state cannot circumvent constitutional protections by relying on intermediaries to obtain information it could not lawfully access directly.[7]

The new subscriber production order in s. 487.0142 fails this test. Lowering the threshold to reasonable suspicion for highly personal information, including the "types of services" a person receives from a doctor or lawyer, is a clear departure from constitutional norms. Knowing that someone received couples counselling, addiction treatment, or sensitive legal advice strikes at the heart of personal dignity and professional confidentiality. This is a direct assault on the privacy expectations that Canadians rightly hold.

Even more concerning is *SAAIA*'s metadata retention scheme. Forcing private companies to retain location data and other metadata for up to one year turns ordinary Canadians' phones, computers, and smart devices into government tracking tools. While the government claims access will still require authorization, the reality is that Bill C-22 removes the strongest protection privacy has: the ability of companies and individuals to delete data.

International experience with mandatory metadata retention supports this concern. The European Union's 2006 Data Retention Directive,[8] which required blanket retention of metadata for 6–24 months, was struck down by the Court of Justice of the EU (CJEU) in the landmark *Digital Rights Ireland* (2014) case as a disproportionate violation of privacy and data protection rights.[9] The CJEU later ruled against similar indiscriminate national regimes in countries like Sweden, the UK, Germany, and France (*Tele2 Sverige*[10], *SpaceNet*[11], and others), while emphasizing that blanket retention creates excessive surveillance risks without sufficient justification.

In Australia, the 2015 mandatory metadata retention scheme[12] (which lasted two years) has led to documented abuses, **including unauthorized access by police to journalists' data and to the data of more than 3,000 other users**,[13] plus access requests by non-law-enforcement bodies such as local councils and professional boards.

These examples show that compulsory retention often leads to overreach, security vulnerabilities, and disproportionate privacy intrusions that are directly applicable to *SAAIA*'s one-year mandate.

---

[7] *R. v. Duarte*, [1990] 1 S.C.R. 30 at 44–45 (state cannot do indirectly what it cannot do directly through electronic surveillance).
[8] Directive 2006/24/EC: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32006L0024
[9] *Digital Rights Ireland Ltd v Minister for Communications*, Joined Cases C-293/12 and C-594/12 (8 April 2014): https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62012CJ0293
[10] *Tele2 Sverige AB v Post-och telestyrelsen*, Joined Cases C-203/15 and C-698/15 (21 December 2016): https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62015CJ0203
[11] *SpaceNet AG v Bundesrepublik Deutschland*, Joined Cases C-793/19 and C-794/19 (20 September 2022): https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62019CJ0793
[12] Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015
[13] The Guardian, "ACT police admit unlawfully accessed metadata more than 3,000 times" (26 July 2019): https://www.theguardian.com/australia-news/2019/jul/26/act-police-admit-unlawfully-accessed-metadata-more-than-3000-times

The Supreme Court has consistently adopted a purposive interpretation of *Charter* rights, and the purpose of section 8 is to protect a reasonable expectation of privacy.[14] Mandatory metadata retention undermines this protection. It not only creates a standing database that makes future searches and seizures far easier, but it also exposes Canadians to a heightened risk of data breaches, hacking by non-government actors, and misuse of power by the state itself, as other governments have done. While the law may not directly authorize new searches, it deliberately builds the infrastructure and preconditions that make far more intrusive state surveillance possible.

Finally, all forms of mass surveillance are known to create a chilling effect on expression, particularly political and artistic expression. When Canadians know that their digital data may be retained and accessible, they are likely to self-censor.

Recommendations

To bring Bill C-22 into compliance with the *Charter*, the Justice Centre recommends the following:

1. **Remove the new subscriber information production order** in s. 487.0142 entirely. This provision unconstitutionally lowers the threshold to reasonable suspicion for highly sensitive subscriber information. However, raising the threshold to the constitutionally compliant "reasonable grounds to believe" standard would simply make the new power redundant with existing production orders. Accordingly, the better approach is to delete this section altogether.
2. **Remove the compulsory metadata retention power** in s. 5(2)(d) of the *SAAIA*. This provision was not included in the earlier Bill C-2 and significantly undermines Canadians' ability to protect their own privacy by choosing service providers that delete data after shorter periods. Mandatory retention creates unnecessary risks of breaches, abuse, and chilling effects.
3. **Amend s. 7 of the *SAAIA*** to remove the Minister's power to issue orders and replace it with a requirement for judicial authorization by a judge of the Federal Court.
4. **Delete or substantially narrow s. 15 of the *SAAIA*** (the gag / non-disclosure provisions) so that companies are not prohibited from disclosing the existence of an order to affected users or the public after a reasonable period.
5. **Exclude health care providers, lawyers, counsellors, therapists, and other sensitive professions** from any remaining production orders that allow access to subscriber-type information by adding a new subsection to the *Criminal Code* (immediately after the definition of "subscriber information" in s. 487.011).
6. **Add a sunset clause** to Bill C-22 stating that all new powers in Part 2 (the *SAAIA*), including sections 5, 7, and 15, expire no more than three years after the day on which this Act comes into force, unless Parliament passes legislation to renew them.

If these changes are not made, Bill C-22 should be withdrawn. Privacy is the shield of a free people. Canadians expect their elected representatives to protect it.

---

[14] *Figueroa v. Canada (Attorney General)*, 2003 SCC 37 at para. 20; *R. v. Plant*, 1993 CanLII 70 (SCC), [1993] 3 SCR 281 at p. 291.

About the Author

John Carpay, B.A., LL.B. is President of the Justice Centre for Constitutional Freedoms, a registered charity founded in 2010. The Justice Centre defends the constitutional rights and freedoms of Canadians through litigation and education.