

SUBMISSION TO THE STANDING SENATE COMMITTEE ON NATIONAL SECURITY, DEFENCE AND VETERANS AFFAIRS

REGARDING BILL C-22, AN ACT RESPECTING LAWFUL ACCESS

November 2, 2026

CHARTER ADVOCATES CANADA
2200-181 University Avenue
Toronto, Ontario M5H 3M7

www.charteradvocates.ca

Daniel C. Santoro, LL.B., Legislative Counsel

[redacted]

BILL C-22: Rendering True Online Privacy Illegal

Prepared by: Daniel C. Santoro, LL.B., Legislative Counsel, Charter Advocates Canada

BACKGROUND OF CHARTER ADVOCATES CANADA

Charter Advocates Canada is a Canadian charity and *pro bono* law firm registered with the law societies of Ontario and Alberta. CAC's mission is to uphold Canadians' constitutional freedoms, civil liberties and human rights. CAC maintains a team of lawyers across Canada who provide *pro bono* legal representation to defend Canadians against government overreach and the violation of their *Charter* rights.

EXECUTIVE SUMMARY OF SUBMISSIONS ON BILL C-22

Bill C-22 overrides the current freedom of individuals and businesses to employ measures to protect digital security and privacy. It also mandates "backdoor access" making private information vulnerable to public dissemination. Further, it contains sweeping secrecy provisions so that the public will not even know when their privacy is violated. Finally, it allows for warrantless searches contrary to foundational s. 8 *Charter* jurisprudence.

These submissions are divided into the following sections:

1. Bill C-22 would outlaw services used to preserve digital security and privacy

    - *Service providers required to develop and implement any technical capability*
    - *Metadata limiting provision provides no substantial protections*
    - *Prohibition against decryption is likewise extremely narrow*
    - *Good reasons why people take measures to protect their digital security*
    - *Forced "backdoor access" renders private information vulnerable to hackers*
    - *Requiring services to retain metadata infringes the privacy of their users*

2. Bill C-22 contains sweeping secrecy provisions preventing public scrutiny

3. Bill C-22 contains warrantless search provisions contrary to s. 8 of the *Charter*

OVERVIEW OF BILL C-22

These submissions are focussed on the powers contained in Part 2, the Supporting Authorized Access to Information Act ("SAIA"). The "meat" of the SAIA is contained in sections 5 and 7, which empower regulations and orders respecting the development and implementation of technical capabilities and the installation of devices to enable authorized persons to access information. As such, the following are feasible use cases:

- A regulation or order requiring smart speakers to function as devices to intercept private communications (i.e. a 'room probe' - Part VI of the *Criminal Code*)
- A regulation or order requiring devices with cameras to function to surreptitiously record video (i.e. a 'covert camera' under 487.01(4) of the *Criminal Code*)
- A regulation or order to a Virtual Private Network (VPN) to retain metadata
- A regulation or order prohibiting VPNs
- A regulation or order requiring a "master encryption key" to access e-mail or other information stored by a third-party that is not encrypted by the user
- A regulation or order requiring computers, smart-phones, or tablets to implement capabilities to access and transmit private communications

To make matters worse, such orders are secret: service providers are by default not permitted to disclose the existence of any orders received to their users (s. 14(c)).

The privacy implications of this Bill are profound and will be subject to challenge in the courts for violating s. 8 of the *Charter*.

1. **Bill C-22 would outlaw services used to preserve digital security and privacy**

Service providers required to develop and implement any technical capability

Section 5(2)(a) of the SAIA is drafted extremely broadly. On its face, regulations could require service providers to develop and implement *any technical capability*. The use of the word "including" means that what follows, "extracting and organizing information that is authorized to be accessed …" is only an example of a technical capability that may be ordered. It reads as follows:

> (a) the development, implementation, assessment, testing and maintenance of operational and technical capabilities, ***including*** capabilities related to extracting and

organizing information that is authorized to be accessed and to providing access to such information to authorized persons [emphasis added]

Metadata limiting provision provides no substantial protections

The limiting provision in s. 5(4) (below) provides no substantial limitations to these powers because it only limits the protections to the s. 5(2)(d) power to harvest "metadata" and not the general powers in s. 5(2)(a) (technical capabilities) and (b) (devices to enable authorities to access information).

> (2) The Governor in Council may make regulations relating to the obligations of core providers, respecting:
>
> ...
>
> (d) the retention of categories of metadata ...
>
> ***
>
> (4) ***Paragraph (2)(d)*** [emphasis added] does not authorize the making of regulations that require core providers to retain information that would reveal
>
> (a) the content — that is to say the substance, meaning or purpose — of information transmitted in the course of an electronic service;
>
> (b) a person's web browsing activities history; or
>
> (c) a person's social media activities.

Prohibition against decryption is likewise extremely narrow

Section 2(4) (below) contains an overarching protection against ordering decryption. However, it only applies to information encrypted by the user and not encrypted information generally.

> Decryption
>
> (4) No obligations under this Act are to be construed as compelling an electronic service provider to decrypt, or to ensure that an authorized person is able to decrypt, any information that is encrypted by a person to whom the electronic service provider provides services, ***unless the encryption was provided by the electronic service provider and the provider possesses the information necessary to decrypt the information*** [emphasis added].

Good reasons why people take measures to protect their digital security

There are many good reasons why people want to protect the privacy of their online activities and the integrity of their personal devices. For example:

- Individuals choose to use encrypted VPNs to protect their online security and privacy. This was in fact recommended by the Canadian government in 2021 during the "Get Cyber Safe" campaign.[1]
- People escaping dangerous situations such as intimate partner violence use VPNs to prevent their online activities from being monitored.[2]
- Journalists use VPNs to protect their reporting on sensitive matters, e.g. involving confidential sources.[3]
- Individuals including reporters and dissidents in oppressive regimes rely on VPNs to protect their privacy and security.[4]
- Individuals and businesses might employ various additional security and privacy protection measures to ensure the integrity of their digital activities including: encryption, secure e-mail and communication platforms, and services that do not track and retain metadata.

Individuals and businesses are currently free to employ various measures to protect their digital security and privacy. In particular, they may choose to use programs and devices which are specifically designed to preserve high levels of security and privacy. There exist numerous technology companies who offer such services for free and for payment. For example:

- Virtual Private Networks (VPNs) which ensure that an IP address is not detectable by the websites being accessed or potentially the VPN itself;
- Services including communication services which strip metadata from messages and otherwise do not collect and retain such metadata;
- Software or devices designed to eliminate invisible background tracking and automatic collection of measurements and data.

Such services take great pains to ensure that their systems are not vulnerable to hacking thereby protecting the integrity of their users' data.

---

[1] https://www.getcybersafe.gc.ca/en/secure-your-connections/vpns
[2] As recommended by organizations which help such people: https://dvapriverside.org/digital-empowerment-utilizing-technology-for-safety-and-support/ and https://breakthesilencedv.org/?p=19406
[3] https://freedom.press/issues/how-journalists-rely-on-vpns-to-protect-press-freedom/
[4] https://freedom.press/digisec/blog/choosing-a-vpn/

The provisions of Bill C-22 empower the government to force service providers to eliminate or override such measures thereby rendering meaningful online privacy illegal. Authorities would be able to issue regulations (s. 5) and orders (s. 7) requiring the development and implementation of technical capabilities of any kind (s. 5(2)(a)) and devices to enable authorized persons to access information (s. 5(2)(b)).

The power to mandate third parties to implement technical capabilities and install devices capable of harvesting private information engages the right to be free from unreasonable search and seizure per s. 8 of the *Charter*. The third-party service providers are compelled into cooperation with the state and thereby become state agents.[5] Provisions forcing an individual to disclose their private information to a third-party engages their "reasonable expectation of privacy"[6] and thereby constitutes a search. Depriving individuals of the ability to conduct their affairs with services designed to protect their digital security and privacy likewise engages their reasonable expectation of privacy. The absence of any meaningful limit to these powers renders these provisions unreasonable contrary to s. 8 of the *Charter*.

Forced "backdoor access" renders private information vulnerable to hackers

The SAIA compels service providers to develop and implement technical capabilities and install devices which can be used to intercept the full contents of their digital activities. In other words, these services would be required to provide "backdoor access" to allow surveillance by law enforcement.

Once such backdoor access is available, there is no way to limit its access to law enforcement. Malicious online actors, i.e. hackers, will inevitably exploit these built-in vulnerabilities to harvest private information. Recent events have demonstrated that this is not speculative, but a real risk:

- In 2026, the full details of more than 1.5 million Crime Stoppers tips were made available for download on the internet. These tips are afforded the highest possible protection known to law and the leak puts lives at risk.[7]
- In August 2025, there was a House of Commons data breach in which an unknown malicious actor gained access to a database which contained non-public employee information including: names, job titles, office locations,

[5] *R v. Broyles,* [1991] 3 S.C.R. 595 at 608.
[6] *R. v. Bykovets,* 2024 SCC 6 at para. 31.
[7] "More than 1.5 million Canadian Crime Stoppers tips leaked," October 21, 2026: https://www.cbc.ca/news/investigates/canadian-crime-stoppers-tips-leaked-hack-investigation-9.7388820
According to the Supreme Court of Canada in *R. v. Liepert*, [1997] 1 S.C.R. 281, informer privilege is an "ancient and hallowed" protection necessary to protect informers from bodily harm or death.

and emails, along with information about their House of Commons issued computers and mobile devices.[8]

- In April 2025, there was a data breach at Nova Scotia Power in which approximately 900,000 customers' data was compromised: addresses, birth dates, driver's license and social insurance numbers and banking information.[9]

Requiring services to retain metadata infringes the privacy of their users

Metadata is information about data itself, and can include markers about authorship, the time and location data was produced, and websites users visit. IP addresses and its related subscriber information is an example of metadata. The Supreme Court of Canada has held that forms of metadata are protected from unreasonable search and seizure per section 8 of the *Charter*. Such data contains core biographical information about a person's habits, lifestyle choices and beliefs. It can be used as a "digital breadcrumb" by which to trail internet activity. [10] Requiring third parties to hold onto this information for a maximum of 6 months puts the privacy of individuals who access the internet at risk.[11]

2. Bill C-22 contains sweeping secrecy provisions allowing authorities to operate behind closed doors without public scrutiny

Section 7 of the SAIA confers power on the Minister to make an order to any electronic service provider to do anything which might be done by regulation under s. 5(2). These include all of the examples referenced above. While s. 5 regulations are not secret, s. 7 orders are. Even the bare existence of such an order is secret (s. 14(c)). Disclosing the existence of such an order is an offence punishable by up to $100,000 per day for an individual or $500,000 per day for "any other person" (s. 41(1)(a) and (2)). While other provisions in Bill C-22 restrict the secrecy of orders to circumstances in which disclosure would jeopardize the conduct of an ongoing investigation,[12] s. 7 orders are subject to secrecy without qualification. The provision is as follows:

---

[8] Kate McKenna, "House of Commons hit by cyberattack from 'threat actor': internal email", *CBC* (14 August 2025), online: https://www.cbc.ca/news/politics/house-of-commons-data-breach-1.7608061.
[9] "Nova Scotia Power notifying customers whose data was affected by cyber breach", *CBC* (14 May 2025), online: https://www.cbc.ca/news/canada/nova-scotia/nova-scotia-power-cyber-breach-1.7534623. See also Sean Mott, "NS Power says 900K current, former customers impacted by 2025 cyberbreach," *CTV News* (25 March, 2026), online: https://www.ctvnews.ca/atlantic/nova-scotia/article/ns-power-says-900k-current-former-customers-impacted-by-2025-cyberbreach/.
[10] *R. v. Bykovets,* 2024 SCC 6 at paras. 4, 8-13; *R. v. Spencer,* 2014 SCC 43 at paras 32-33.
[11] Bill C-22 Part 2 at s. 5(2)(d).
[12] s. 487.0121(6)

> **Prohibition on disclosure**
>
> **14** An electronic service provider and any person acting on its behalf must not disclose any of the following information except as permitted under this Act or the *Canada Evidence Act*:
>
> **(a)** information contained in an order made under subsection 6(1) or 7(1);
>
> ...
>
> ***(c) the fact that the electronic service provider is or was subject to the order;*** [emphasis added]

The possibility of a Ministerial exemption does not attenuate the secrecy problems. First, there is secrecy by default not when required for serious reasons. Second, there are no standards governing the circumstances in which exemptions are granted. It is left entirely up to what the Minister "considers reasonable." The provision is as follows:

> **Authorization to disclose**
>
> **15 (1)** At an electronic service provider's request, the Minister may issue a written authorization permitting, on any terms that the Minister considers reasonable, the electronic service provider to disclose any information referred to in section 14.

This general secrecy provision obstructs users' informed consent respecting the digital services they use. A user would have no way of knowing that a supposedly private and secure digital service is in fact subject to a sweeping order requiring technical capabilities designed to harvest private information. Given the secrecy requirement, this would infringe their right to unreasonable search and seizure contrary to s. 8 of the *Charter*. It is also a restriction of their freedom of expression per s. 2(b) of the *Charter*, and the absolute requirement of secrecy would be overbroad and therefore not a reasonable limit per s. 1 of the *Charter*.[13] Absolute secrecy prevents any sort of public scrutiny surrounding s. 7 orders. Transparency is necessary for "discouraging mischief and ensuring confidence in the administration of justice through transparency."[14]

---

[13] If the measures adopted are "arbitrary, unfair or based on irrational considerations" there is no rational connection. Likewise, if they are overbroad, there is no minimal impairment. *R. v. Oakes*, [1986] 1 S.C.R. 103 at para. 70.

[14] *Sherman Estate v. Donovan*, 2021 SCC 25 at para. 44.

3. Bill C-22 grants government authorities the power to conduct searches of premises without judicial authorization contrary to s. 8 of the *Charter*

Section 20 of the SAIA grants the Minister's designate the power to search any premises, other than a dwelling place, for verifying compliance or non-compliance with the Act. The Supreme Court of Canada has held that such search powers require prior authorization granted by a neutral person acting in a judicial capacity.[15] This rule applies to businesses as well as dwelling places. Therefore, the restriction of this search power to non-dwelling places does not result in compliance with s. 8 of the *Charter*.

Additional Note: Coming into Force Amendment

There should be a "coming to force" date to allow sufficient time for service providers to take any steps they deem necessary.

[15] *Hunter v. Southam,* [1984] 2 S.C.R. 145 at 161-162.