BRITISH COLUMBIA CIVIL LIBERTIES ASSOCIATION | ASSOCIATION DES LIBERTÉS CIVILES DE LA COLOMBIE-BRITANNIQUE

Submissions to Standing Committee on Public Safety and National Security regarding Bill C-22, An Act respecting lawful access

June 1, 2026

Prepared by Aislin M. Jackson, Policy Staff Counsel

British Columbia Civil Liberties Association
306 - 268 Keefer Street
Vancouver, BC, Canada V6A 1X5

Tel 604.687.2919
Fax 604.687.3045
Toll-free 866.731.7507

info@bccla.org
www.bccla.org

Introduction

Bill C-22 (the "Bill") is an overbroad and disproportionate attempt to open the digital communications of people in Canada to law enforcement and national security bodies of the state. If enacted in its current form, it will have a profound deleterious effect on the privacy rights and fundamental freedoms of people in Canada. In particular, the Bill will adversely affect the protection of privacy, including informational privacy, against unreasonable search and seizure and the "freedom of thought, belief, opinion and expression, including freedom of the press and other media of communication" enshrined in sections 8 and 2(b) of the *Canadian Charter of Rights and Freedoms*,[1] respectively.

Indeed, the privacy rights of Canadian residents, despite their constitutional protection and fundamental importance to a free and democratic society, appear to have been an afterthought, where they are considered at all. One clear example of this is the lack of any oversight or consultative role for the entity charged with protecting personal privacy rights at the federal level, the Privacy Commissioner of Canada, in making any of the regulations or orders that would be licensed by the Bill.

Part 2, the proposed *Supporting Authorized Access to Information Act* ("SAAIA"), also risks the cybersecurity of millions of individuals, as it would empower the Minister of Public Safety and Emergency Preparedness, through orders, and the government, through regulations, to require digital service providers to build backdoors into their systems, introducing security vulnerabilities. Providers could also be compelled to retain potentially revealing metadata information on all of their customers for up to a year, regardless of whether there are grounds to suspect that the individual is involved in any way with criminal or otherwise undesirable behaviour. The extremity of these powers, together with the other vague and overbroad elements of the Bill, prepares the ground both for over-compliant, unnecessary infringements of personal privacy and for firms that do not wish to compromise the security and integrity of their products to exit the Canadian market, cutting Canadian residents off from the digital services used by the rest of the democratic world.

Both privacy and freedom of expression are core, fundamental rights that must be protected and upheld for our society to remain free and democratic. The British Columbia Civil Liberties Association ("BCCLA") therefore urges Parliament to carefully tailor any legislation facilitating law enforcement or national security access to digital communications in order to ensure that these foundational rights are infringed as little as possible to achieve the legislation's goals, as is required by our *Charter*.

Summary of Recommendations

Recommendation 1: Remove (c) from the definition of "subscriber information" in section 5 of Part 1. Information about the types of services provided, the devices used by the client, and the period during which services were provided go beyond the identification of the subscriber and

[1] Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11.

are capable of revealing sensitive information about an individual's identity and activities at particular points in time.

Recommendation 2: Explicitly exclude medical information – including psychological, psychiatric, and counselling information – as well as solicitor-privileged information from the definition of "subscriber information". Similarly, psychological, psychiatric, and counselling information should be added to the protection for these categories of information in the *Canadian Security Intelligence Service Act*[2] contained in section 31 of the Bill.

Recommendation 3: Replace "reasonable grounds to suspect" with "reasonable grounds to believe" in sections 5, 6, and 7 of the Bill. Transmission data and subscriber information can be revealing, especially when combined with other information, and the lowest standard in criminal law is inappropriate for this level of sensitivity.

Recommendation 4: Remove Part 2 from the Bill in its entirety. SAAIA would licence the conscription of private entities to conduct unconstitutional mass surveillance on behalf of the state and contains only inadequate protections for encryption and cybersecurity.

Privacy

Privacy is not only a freestanding right protected by section 8 of the *Charter*, but also and important precondition for the exercise of other *Charter*-protected rights: freedom from unjustified surveillance affords us the space to think and believe freely, to associate with who we choose, and to enjoy intimate relationships with our family and friends that are necessary for our wellbeing. An awareness of being surveilled is psychologically harmful, resulting in stress and self-censorship, distorting individual behaviour and chilling participation in public discourse.

This is no less true online than it is on a city street or in a private home. Canadians must not, in the words of the Supreme Court of Canada, be "required to become digital recluses in order to maintain some semblance of privacy in their lives";[3] we must be able to use the internet to conduct our ordinary lives without undue interference with our privacy.

Recent polling commissioned by the Center for Democracy and Technology reinforces the value that people in Canada place on the privacy of their online communications: for example, 90% of the Canadians they surveyed agreed that "no one should be able to access their personal messages without a court order", and 63% said they would self-censor their social media behaviour if law enforcement were able to access these private messages.[4] People in Canada expect and deserve that their elected representatives protect their privacy rights, allowing them to be curtailed or infringed only when it is truly necessary for a *bona fide* public good, not simply when it would be convenient for law enforcement.

---

[2] RSC 1985, c C-23.
[3] *R v Jones*, 2017 SCC 60 at para 45.
[4] Tom Bowman and Greg Nojeim, "Canadians Value Encryption and Reject Key Surveillance Powers in Bill C-22: Emerging Research from the Center for Democracy & Technology" (May 2026), online (pdf): *Center for*

Part 1 – Timely Access to Data and Information

Part 1 of the Bill makes several amendments to the *Criminal Code*[5] and other statutes. Some of these measures, such as the new *Criminal Code* definition of "computer data", are genuine modernizations, but others create new information demand powers and types of production order that raise *Charter* concerns.

Definition of subscriber information is too expansive

Section 4(2) of the Bill would add the following definition to the *Criminal Code*:

> ***subscriber information***, in relation to any client of a person who provides services to the public or any subscriber to the services of such a person, means
>
> **(a)** information that may be used to identify the subscriber or client, including their name, pseudonym, address, telephone number and email address;
>
> **(b)** identifiers assigned to the subscriber or client by the person, including account numbers; and
>
> **(c)** information relating to the services provided to the subscriber or client, including
>
> **(i)** the types of services provided,
>
> **(ii)** the period during which the services were provided, and
>
> **(iii)** information that identifies the devices, equipment or things used by the subscriber or client in relation to the services. (*renseignements relatifs à l'abonné*)

Notably, this definition is not specific to electronic service providers, and could be applied to brick-and-mortar service providers like booksellers, daycares, and counselors. The definition is referenced in the creation of a new warrantless confirmation of service demand power and a production order power in the *Criminal Code*. (This information can currently be obtained through the general production order provided for in section 487.014 of the *Criminal Code*.)

While 'subscriber information' as it is usually understood, the information that businesses maintain to identify and contact their clients, is already sensitive personally identifying information that merits robust legal protection as discussed below, this definition does further still: it includes, in subsection (c), information on the type, timing, and devices used by the client in connection with the service. This information is not limited to disclosing whether a customer uses a Samsung phone or an Apple notebook computer to access a digital service, but would also include identifiers unique to the specific machine, such as the unique MAC address assigned to

---

Democracy and Technology < https://cdt.org/wp-content/uploads/2026/05/upd-2026-05-16-CDT-SS-Canada-encryption-polling-quick-brief-final-2.pdf>.

[5] RSC 1985, c C-46.

each network interface controller in a device, and even the use of assistive devices to access physical spaces.

This information can be revealing of the client's biography and intimate life. For an example of how the information referred to in subsection (c) can be intimately revealing, consider the services provided by a relationship counselor: simply disclosing the nature of the services provided and the period during which those services were provided would reveal that the subject of the information was experiencing strife or disharmony within their most intimate relationship, as well as the time window in which this relationship strain occurred.

> Recommendation 1: Remove (c) from the definition of "subscriber information" in section 5 of Part 1. Information about the types of services provided, the devices used by the client, and the period during which services were provided go beyond the identification of the subscriber and are capable of revealing sensitive information about an individual's identity, medical needs, and activities at particular points in time.

Although the Bill contains a carveout for medical information and information subject to solicitor-client privilege, "medical information" is not a defined term in the *Criminal Code* and it is not clear that information about counselling services received, or even treatment for diagnosed mental illnesses, would be considered "medical information" within the meaning of that exclusion. This information is no less sensitive, intimate, or personal than is information relating to physical injury or illness, and in some cases will be much more so.

The structure of this protection – which requires that demands not be made in respect of the protected information, rather than excluding this information outright – is likely to result in unnecessary court applications. This is so because the party seeking the information does not know what it contains at the time the request is made, so they are poorly positioned to understand whether protected information has been scoped in. It is the recipient of the demand who will have this complete understanding, and the Bill would provide them with no alternative but to apply in court for a revocation or variation upon review. This is an inefficient use of public resources, and it can easily be avoided by excluding the protected information from the scope of all such demands.

> Recommendation 2: Explicitly exclude medical information – including psychological, psychiatric, and counselling information – as well as solicitor-privileged information from the definition of "subscriber information". Similarly, psychological, psychiatric, and counselling information should be added to the protection for these categories of information in the *Canadian Security Intelligence Service Act*[6] contained in section 31 of the Bill.

[6] RSC 1985, c C-23.

Inappropriately low standard for information demand powers and new production order

Sections 5, 6, and 7 of the Bill would create new *Criminal Code* production orders and information demands, the latter of which are issued unilaterally and without court oversight by law enforcement.

Information to identify clients and, in the case of online services, to link a specific person with online activity is sensitive and potentially very personally-revealing. Even if the information referred to in subsection (c) is excluded in accordance with Recommendation 2, subscriber information contains sensitive personally identifying information that, in the right context, can be deeply revealing. Information of this kind merits more protection than is provided by requiring only "reasonable grounds to suspect", the lowest standard in the criminal law.

The sensitivity of this information has been considered by the Supreme Court of Canada twice: *Spencer*[7] considered subscriber information in the sense of the name, address and phone number, as described in subsection (a) of the SAAIA definition; and *Bykovets*[8] considered IP addresses, identifiers assigned to consumers by internet service providers and therefore falling within the subsection (b) description. In both cases, the Court found that there was a reasonable expectation of privacy in this information, attracting constitutional protection: in *Spencer*, a police request "for subscriber information corresponding to specifically observed, anonymous Internet activity engage[d] a high level of informational privacy"[9]; in *Bykovets*, the Court pointed out that an IP address, especially when cross-referenced against other information which can be obtained by police, acts as "the first digital breadcrumb" in a trail that would reveal online activity.[10]

The key to these analyses is that Canadian courts are concerned with "not only the nature of the precise information sought, but also at the nature of the information that it reveals."[11] We urge the members of this committee to take a similarly broad view of the informational privacy effects of disclosure.

> Recommendation 3: Replace "reasonable grounds to suspect" with "reasonable grounds to believe" in sections 5, 6, and 7 of the Bill. Transmission data and subscriber information can be revealing, especially when combined with other information, and the lowest standard in criminal law is inappropriate for this level of sensitivity.

[7] *R v Spencer*, 2014 SCC 43 [*Spencer*].
[8] *R v Bykovets*, 2024 SCC 6 [*Bykovets*].
[9] *Spencer*, *supra* note 7, at para 51.
[10] See *Bykovets*, *supra* note 8, at para 9.
[11] *Spencer*, *supra* note 7, at para 26.

Part 2 – Supporting Authorized Access to Information Act

Privacy rights insufficiently protected

In the context of the internet, informational privacy is constantly at risk of erosion as information about users' identities and activities is tremendously valuable to private interests and law enforcement alike. As the Supreme Court of Canada has recognized, there is a porous boundary between online surveillance by private entities and surveillance by law enforcement and other arms of the state, such that "the Internet has fundamentally altered the topography of informational privacy under the *Charter* by introducing third-party mediators between the individual and the state — mediators that are not themselves subject to the *Charter*."[12]

The government, through this Bill, seeks to exploit this very dynamic to evade constitutional scrutiny for privacy violations by routing state surveillance through such private entities. It is revealing and alarming that the *Charter* statement for the Bill does not even consider that section 8 search and seizure rights may be implicated by SAAIA, which lays the legislative groundwork to conscript private service providers to carry out indiscriminate mass surveillance for the benefit of law enforcement and national security state agencies by collecting and retaining metadata of all their clients, whether or not there exist any grounds to suspect any individual client of involvement in wrongful behaviour, for up to a year.[13]

This attempt is constitutionally brittle and is likely to fall when challenged in court: in Canadian law, private entities that conduct searches or seizures at the direction of the state, behaving in ways that they would not but for the interference of the state, are state agents.[14] Any such evidence collection by private individuals acting as state agents is subject to the same constitutional requirements as searches performed directly by police.[15] In particular, evidence collected in breach of section 8 cannot be used to obtain a valid warrant[16] and may be excluded from evidence at trial in accordance with section 24(2) of the *Charter*. For this reason, the tools that the Bill seeks to create for law enforcement are likely poisoned; their use doomed to result in voided warrants and dismissed or stayed charges, rather than the desired successful prosecutions. They would therefore provide no actual benefit to the administration of justice to justify the mass privacy violations SAAIA would create.

Encryption and cybersecurity threatened

SAAIA has repeatedly been described by proponents as "encryption neutral", which can only be true if the regulations and orders it would licence are completely disregarded. While it may be

---

[12] *Bykovets*, *supra* note 8, at para 10.
[13] SAAIA, s 5(2)(d).
[14] See *R v M (MR)*, [1998] 3 SCR 393, at para 29; *R v Pham*, 2025 BCCA 324 at para 97.
[15] See *R v Buhay*, 2003 SCC 30 at para 25.
[16] See, e.g., *R v Plant*, [1993] 3 SCR 281, 1993 CanLII 70 (SCC) at 291. "This Court has determined that peace officers cannot benefit from their own illegal acts by including in informations sworn to obtain warrants facts which were retrieved through searches without lawful authority."

true that the text of SAAIA itself does not itself require the creation of any backdoors to encryption, the subject matter for regulations and orders described in section 5(2) – particularly subsections (a) and (b) – would clearly do so.

Backdoors that allow third parties, including the government and service providers themselves, to access otherwise secure communications are fundamentally incompatible with end-to-end encryption on a technical level: by definition, end-to-end encryption only exists when the data cannot be decoded by anyone except the sender and the intended recipient. End-to-end encryption is a foundation stone of cybersecurity, second only to restraint in data collection. The safest information is that which has never been collected or stored, and the second-safest is that which is end-to-end encrypted. Even if these backdoors are never actually used, their creation would undermine the privacy and security of countless people, both in Canada and abroad. When combined with a metadata retention scheme, as is contemplated by the regulation and order making power, which would create data-rich targets for hackers, SAAIA's threat to cybersecurity is profound.

Subsections 5(5) and 7(5) provide that a service provider is not required to comply with requirements of a regulation or order, respectively, if doing so would introduce a systemic vulnerability into an electronic service or prevent them from fixing such vulnerabilities. These provisions are facially reassuring, but unfortunately rely upon a definition of "systemic vulnerability" that is unworkably narrow and vague.

SAAIA's definition of "systemic vulnerability" is "a vulnerability in the electronic protections of an electronic service that creates a substantial risk that secure information could be accessed by a person who does not have any right or authority to do so." This definition is narrow in that it is restricted to vulnerabilities not just in the service provider's systems generally, but vulnerabilities in the "electronic protections" (defined as authentication, encryption, and any others specified in the regulations) of an "electronic service" (defined as a service or feature of a service that "involves the creation, recording, storage, processing, transmission, reception, emission or making available of information" in intangible form), excluding forms of vulnerability beyond those listed in the legislation and vulnerabilities in features or software systems that are not services.

A service provider wishing to rely on subsection 5(5) or 7(5) will also bear the burden of proving that the risk is substantial and that the information threatened is secure – and neither standard is defined, resulting in vagueness and an uncertain standard. How substantial must the risk be, and what proof is possible in an environment of rapidly-evolving risk? Service providers must answer these questions right: too narrow in their interpretation, and they imperil their systems' security unnecessarily; too broad, and they risk substantial administrative monetary penalties. The protection for security and encryption in SAAIA, therefore, is more apparent than real.

Overbreadth and vagueness

The definition of "systemic vulnerability" discussed above is one example of vagueness in SAAIA. Another can be found at subsection 5(4)(b), which limits the power to make regulations that would require metadata retention to exclude information that would reveal "a person's web browsing history". The vagueness in this case arises from the unanswered question of to whom it would reveal this information, and in what context: as the Supreme Court of Canada observed in *Spencer* and *Bykovets*, the private surveillance of online activity means that IP addresses can do so. The same is potentially true for device identifiers like MAC addresses, for email addresses, which are near-universally required to register for online services, linking one user with various accounts, and other digital identifiers. If subsection 5(4)(b) is intended to align with the constitutional jurisprudence and exclude these digital breadcrumbs, what metadata can actually be retained, and what legitimate use could law enforcement make of it? If the subsection is not meant to exclude these identifiers, conversely, how can it be constitutional? Which version should a compliance-minded service provider comply with?

Many of SAAIA's flaws discussed above are examples of overbreadth. Orders and regulations requiring mass, suspicionless metadata retention for up to a year, for example, would unavoidably collect and store the data of millions of people who have no connection to any crime under investigation. However, these glaringly inappropriate elements are not the only examples of problematic overbreadth; subsections 15(d)-(f), for example, would make any information submitted to a decision-maker in various applications and representations under SAAIA confidential and subject to penalty for disclosures not explicitly authorized by either the *Canada Evidence Act*[17] or SAAIA itself, regardless of how sensitive that information actually is. Ordinary business information such as a planned expansion of a company's workforce or the opening of a new office would be captured if this information were included in an application to the Minister for a temporary exemption from the regulations. Any subsequent disclosure of this information, even for legitimate business purposes, would be an offense and attract administrative monetary penalties.

Vague and overbroad regulatory schemes incentivize overcompliance, to avoid liability even on the most extreme readings of the requirements, with the most obvious alternative being exit from the market subject to the vague, overbroad regulation. Digital service providers of all sizes and corporate structures – from behemoths like Apple[18] to non-profits like Signal[19] – have publicly implied or stated outright that they would withdraw services from the Canadian market in order to avoid the need to comply with SAAIA due to these flaws. The costs of such market exit will

[17] RSC 1985, c C-5.
[18] Catharine Tunney, "Apple argues Liberals' lawful access bill could put users' personal data at risk", *CBC* (6 May 2026), online: <https://www.cbc.ca/news/politics/apple-argues-liberals-lawful-access-bill-could-put-users-personal-data-at-risk-9.7190092>.
[19] Marie Woolf, "Signal warns it would pull out of Canada if made to comply with lawful access bill", *The Globe and Mail* (13 May 2026), online: <https://www.theglobeandmail.com/politics/article-signal-warns-it-would-pull-out-of-canada-if-made-to-comply-with-lawful/>.

not only fall on the Canadian economy, as workers and enterprises lose access to tools they rely upon, but also political and cultural life, impairing our ability to communicate freely across borders with our peers in other, more privacy-protective and digitally secure jurisdictions.

> Recommendation 4: Remove Part 2 from the Bill in its entirety. SAAIA would licence the conscription of private entities to conduct unconstitutional mass surveillance on behalf of the state and contains only inadequate protections for encryption and cybersecurity.

About the BC Civil Liberties Association

The BCCLA is the oldest civil liberties and human rights group in Canada, advancing litigation, law reform, community-based legal advocacy, and public legal education across the country since 1962.