David Asper Centre for Constitutional Rights
UNIVERSITY OF TORONTO

A Brief to the Standing Committee on National Security, Defence and Veterans Affairs Regarding Bill C-22, *An Act respecting lawful access*

October 26, 2026

David Asper Centre for Constitutional Rights
Henry N.R. Jackman Faculty of Law, University of Toronto

Roberto De Luca, Research Associate
Cheryl Milne, Executive Director

I. Executive Summary

Bill C-22, *An Act respecting lawful access*, introduces significant changes to Canada's digital surveillance and policing landscape. The bill expands investigative powers under the *Criminal Code*. It also imposes sweeping obligations on newly defined "core providers", and "electronic service providers" (ESPs) more generally, so as to support law enforcement access to private information, via the enactment of the *Supporting Authorized Access to Information Act* (SAAIA).

Bill C-22 has faced substantial and well-founded criticisms since it was tabled. In this brief, the Asper Centre for Constitutional Rights joins what is now a chorus of legal, privacy and technical experts who have expressed serious concerns about the constitutionality of Bill C-22.

We acknowledge the government's efforts to remedy several of the most pressing issues highlighted by initial criticisms of the bill and its precursor, Parts 14 and 15 of Bill C-2. We also acknowledge the real public safety aims of the legislation. Be that as it may, we write out of a concern that neither the bill's recent amendments nor the bill's ostensible purposes are sufficient to resolve the several constitutional issues posed by the bill, including especially their likely violation of the *Charter*-protected right to privacy. We also write out of a special concern that the government's legislative efforts to date, from Bill C-2 through Bill C-22 as amended, have consistently failed to heed express Supreme Court of Canada guidance as to what the *Charter* requires in the informational privacy context.

Bill C-22's insufficient attention to court guidance is related to our second broad area of concern: the bill's promulgation of a scheme that would routinely frustrate the possibility of meaningful judicial and administrative oversight of our policing and national security institutions. Indeed, Bill C-22 would do so in areas of law where *Charter* interests are especially elevated (i.e., the digital information universe, wherein third parties enhance the state's capacity to aggregate information with respect to our most intimate biographical details), where the probability of *Charter*-violating conduct is high, and where the remedial options post-violation are low (i.e., privacy, once breached, cannot simply be restored).

This second overarching concern has, unfortunately, been exacerbated by Bill C-22's unusual path to the Senate. The bill's clause-by-clause examination noticeably featured RCMP and CSIS representatives but excluded the Office of the Privacy Commissioner of Canada – i.e., a known critic of the bill and Canada's chief independent oversight institution with respect to the right to privacy. The government then compounded these procedural issues by fast tracking the bill through the clause-by-clause process. Taken as a whole, this flawed process deepens our constitutional concern that passing Bill C-22, as is, would give second class standing to *Charter* protections and to the principles of constitutionalism and the rule of law more generally.

For these and related reasons, our chief recommendation would be to withdraw Bill C-22, or Part 2 specifically, and begin any necessary legislation anew, with due attention to *Charter* protections and court guidance on the issues raised by the bill. In the alternative, and given the realities faced by this Senate Committee, we address several provisions that we submit are constitutionally flawed. Our recommendations with respect to these discrete provisions are appended below.

II. Part 1: New Investigative Powers and Section 8 of the *Charter*

Bill C-22's new privacy engaging investigative powers, and its unhelpful endorsement of "voluntary disclosures" and the collection of data "available to the public", will undermine relevant Charter protections, including as they

have been described by the Supreme Court of Canada in *R v Spencer* and *R v Bykovets.*[1] Because these provisions invariably interact with one another to create a policing scheme that is greater than the sum of its parts, it is best to consider the provisions as a whole.

The Key Provisions in Brief

Clause 5 of Bill C-22 would amend the *Criminal Code* (proposed s. 487.0121) to provide law enforcement with the power to demand telecommunications service providers confirm that a specific subscriber, client, account, or identifier does or does not use their service. To issue the demand, law enforcement must meet the standard of "reasonable grounds to suspect" that an offence – under any Act of Parliament – has or will be committed: s. 487.0121(2). To be valid, a confirmation of service demand must also assist in the investigation of the suspected offence, on this same standard of reasonable suspicion: s. 487.0121(2). The demands may impose a non-disclosure condition for up to one year, subject to certain conditions: 487. 0121(6). Analogous powers are given to CSIS with respect to threats to the security of Canada or the collection of information concerning foreign states and persons: Clause 31, proposed s. 20.22 of the *Canadian Security Intelligence Service Act*.

As these provisions indicate, the proposed demand power would *not* be subject to prior judicial authorization. In the first instance, law enforcement institutions and the Service are being asked to police themselves when issuing demands. Judicial oversight would be available, but only via a more limited route – the judicial review of already-issued demands. That is, TSPs can seek review of the demands, within 5 days of receiving the demand, but only if prior notice of intention to apply is provided to the law enforcement officer or to the Service making the demand: *Code*, s. 487.0121(8)-(9); *CSISA*, s. 20.23.

We acknowledge that these provisions have been substantially refined and improved from their first iteration in Bill C-2, including by restricting the allowable recipients of information demands and by expressly narrowing the scope of information that may be disclosed. While we welcome these improvements, the reality is that the confirmation of service demand power will very likely be used routinely and with little judicial oversight. This outcome is a matter of incentives. Law enforcement and the Service have a demonstrated interest in the information. TSPs often have limited incentive to oppose such institutions – i.e., to challenge law enforcement's or the Service's view that the relevant standards have been satisfied – in the ordinary case, unless they face reputational risks related to the disclosure. As addressed more fully below, Bill C-22 further stacks the incentives in favour of voluntary disclosure and its *Charter*-undermining normalization by providing TSPs with immunity for such cooperation (Clauses 11 and 31). The result is that the demand power will often be used, with no judicial involvement, to secure initial "breadcrumbs" that will underlie more substantial searches.

To this last point, a critical intersecting power is found at Clause 6 of Bill C-22 (proposed s. 487.0142). S. 487.0142 would provide law enforcement with a power to obtain "subscriber information" from anyone "who provides services to the public", via a court-imposed production order. Law enforcement institutions already possess a similar investigative power. Under the *Criminal Code's* general production order power (s. 487.014), law enforcement can secure "documents", including communications held by a telecommunications company (such as historical text messages sent and received), and the information required to link IP addresses and other information to individual clients, via an *ex parte* application to a justice or judge.[2]

The key difference between the general production power and the proposed addition is that the latter would intentionally lower the standard that law enforcement must meet to secure production of certain *Charter*-protected

[1] *R v Spencer*, 2014 SCC 43 [*Spencer*]; *R v Bykovets*, 2024 SCC 6 [*Bykovets*].
[2] See, e.g., *R v Jones*, 2017 SCC 60 at paras 75 – 81.

information. The general production power requires an applicant to satisfy the justice or judge that there is "reasonable grounds to believe" that an offence has been or will be committed and that "the document or data is in the person's possession or control and will afford evidence respecting the commission of the offence": s. 487.014. By contrast, the subscriber information production order would be issued if the applicant satisfies the justice or judge of mere "reasonable grounds to suspect" that these same conditions are met: s. 487.0142(2). A lower standard for production is restricted to the defined subclass of information being produced: subscriber information. Subscriber information is defined by the bill at Clause 4 (proposed s. 487.011**)**, and would include names, addresses, account details, types of services received, and device identifiers. As set out below, the key legal issue arising from this change is whether the privacy interest in "subscriber information", so defined, is of a low enough value to justify what is a substantially lower standard for production. We submit that it is not.

The above provisions must also be understood in their fuller context. Most notably, the above law enforcement powers would be substantially buttressed by additional powers that Bill C-22 presents as mere clarifications. The first power states that "voluntary" preservation requests and unsolicited disclosures by TSPs or other persons, are permitted, so long as the information preserved or shared is lawful: Clause 11 (proposed s. 487.0195). This permission is strengthened via a subsection stating that persons engaging in the preservation or voluntary disclosure of information in such circumstances are immune from civil and criminal liability: s. 487.0195(2). A second power would, "for greater certainty", clarify that an order, warrant, or confirmation of service demand is not required for law enforcement to obtain information that is "available to the public": 487.0195(4). Relatedly, Clause 31 would immunize TSPs and persons acting on behalf of TSPs from "civil or criminal proceedings" with respect to voluntary requests for confirmation of service information from the Service: s. 20.26. As set out below, the likely result of such provisions is that the confirmation of service demand power – enforced as such or otherwise secured via voluntary co-operation –will often be sufficient to secure information over which individuals have a reasonable expectation of privacy, without ever requiring judicial pre-authorization for the search (i.e., under the less rigorous proposed s. 487.0142 or otherwise).

The Legal Context

An appreciation of why the above provisions, including especially when considered together as a cohesive whole, are constitutionally problematic requires consideration of the relevant jurisprudence, both recent and longstanding.

Section 8 of the Charter provides everyone with a right to be secure against unreasonable search or seizure and includes within it an implied right to privacy. A "search" occurs where the state invades a reasonable expectation of privacy. Courts analyze an expectation of privacy by considering the subject matter of the search, the claimant's interest in the subject matter, the claimant's subjective expectation of privacy, and whether the subjective expectation of privacy was objectively reasonable.[3]

The Supreme Court of Canada has repeatedly found that a reasonable expectation of privacy, and thus the s. 8 right, extends to online conduct and informational privacy. In the landmark decision of *R v Spencer*, the SCC found that individuals have a reasonable expectation of privacy in their online conduct, an expectation that extends to subscriber information associated with an internet protocol (IP) address. In *Spencer*, the Court reasoned, in part, that PIPEDA's statutory provision allowing "for disclosure without consent to a government institution where that institution has identified its *lawful authority* to obtain the information" could not be a factor at all in the analysis because the statutory provision could not resolve the *Charter* issue: i.e., whether Mr. Spencer had a reasonable expectation of privacy in any subscriber information secured via that provision (which, in the result, he did).[4] In *R*

[3] See, e.g., *Spencer* at 18; *Bykovets* at 31.
[4] *Spencer* at 62.

v Bykovets, the SCC has more recently clarified and strengthened this holding by finding that a reasonable expectation of privacy extends to IP addresses themselves.[5]

In arriving at these conclusions, the Court has reasoned that the principal object of the protection of informational privacy is "informational self-determination", i.e., "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others".[6] Contained within this foundational principle is Canada's well-established prohibition on so-called third party consent to disclosure, i.e., the notion that third parties (e.g., telecoms) are authorized to voluntarily disclose information about an individual (e.g., their users) based upon an alleged authority flowing from the third party's relationship with the individuals in issue. Based upon the above prohibition, courts have repeatedly found that warrantless searches or seizures require the voluntary, informed consent by the individual whose information is the subject of the search or seizure, notwithstanding U.S. doctrine to the contrary.[7]

Critically, the Supreme Court's most recent jurisprudence has also been careful to emphasize the explanatory power of information held by telecommunications and other digital service providers. In *Bykovets*, for instance, the majority observed that the "Internet has exponentially increased both the quality and quantity of information stored about Internet users, spanning the most public and the most private human behaviour", and that this information is distinct because it is "highly centralized, easily accessible, and 'not filtered through human memory and motivation but can be produced as a copy of its original form'".[8] The result is that information "revealed to the state in pieces can now be 'compiled, dissected and analyzed to lend new insights into who we are as individuals or populations'".[9] Within this array of information capable of revealing our most private selves, identifiers such as IP addresses are critical keys that link the relevant information to an individual user. Once such keys are known, data aggregation and analysis can quickly transform what appeared to be mundane information into information that is "profoundly revealing when situated in context with other data points".[10]

Given this new informational reality, third parties wield immense informational resources and power. Specifically, private corporations have "the ability to collect vast stores of user information and to aggregate that data into sharp images of their users' online activity to determine what their users want and when they want it".[11] The Court has stated that this reality *must* shape the constitutional analysis because it has added a "third party to the constitutional ecosystem", a shift that "has *enhanced*, rather than constrained, the state's informational capacity".[12] The cumulative result is that ostensibly trivial or innocuous data points must not be understood as information in themselves, but as identifiers that are intended to lead to a treasure trove of personal information (that would have been unthinkable decades previous).

This reasoning has clear and obvious import for how digital information searches must be conducted. Under section 8 of the *Charter*, the default standard for a reasonable search is and always has been a system of judicial pre-authorization (i.e., requiring a prior finding by a neutral and impartial arbiter, acting judicially, that the search or seizure is supported by reasonable and probable grounds, established on oath[13]). This is because a chief purpose

---

[5] *Bykovets* at paras 14 and 90 – 92.
[6] *Bykovets* at para 32, citing to *R v Tessling*, 2004 SCC 67 at para 23 and *R v Jones*, 2017 SCC 60 at para 39 [*Jones*].
[7] See, e.g., *R v Cole*, paras 77 – 79.
[8] *Bykovets* at para 73, citing to L. M. Austin, "Technological Tattletales and Constitutional Black Holes: Communications Intermediaries and Constitutional Constraints" (2016), 17 *Theoretical Inquiries L.* 451, at p. 457.
[9] *Bykovets* at para 73.
[10] *Bykovets* at para 74, citing to N. Hasan et al., *Search and Seizure* (2021), at p. 59.
[11] *Bykovets* at para 75.
[12] *Bykovets* at paras 78-79 (emphasis added).
[13] *Hunter et al v Southam Inc* [1984] 2 SCR 145.

of section 8 is to prevent unreasonable searches *before* any breach of privacy occurs. This purpose flows, in part, from the fact that "[p]rivacy, once breached, cannot be restored".[14] Because the analysis for any given search is contextual and must account for both the state objective and the degree of impact on the individual's privacy interest, the Court's repeated recognition of the substantial impacts that flow from searches of our digital information (including subscriber information) on our privacy interests argues powerfully against loosening the standards that might apply to them.

Assessing the Proposed New Powers

To the extent Bill C-22 attempts to meet the above *Charter* obligations, it principally does so in two ways: it limits the information available via the confirmation of service demand power (i.e., the power not requiring prior judicial authorization); and it subjects the powers to a standard of "reasonable suspicion".

From a *Charter* perspective, this is small comfort. The threshold issue is the severity of the privacy interests at stake. Read against the Court's jurisprudence, the proposed powers are designed to facilitate production about deeply private, high value information.

First and foremost, the proposed s. 487.0142 would facilitate easier production of "subscriber information". As it is currently defined at Clause 4, subscriber information is not restricted to basic identifying details about a user, such as their name, address, and IP address. Subscriber information expressly includes information regarding services and devices used *and* the when and where of such use. As remarked by Professor Robert Diab, it would appear, for instance, to include information about the channels to which a user has subscribed or whether and how a user has interacted with online gambling services – i.e., lifestyle information that goes directly to the biographical core of the users in issue.[15] The result is that the scope of information collected will be broad and the degree of impact on individuals' privacy interests will be high. Second, "subscriber information" is not stand-alone information that will have no other informational value. Like the subscriber information in *Spencer* and the IP addresses in *Bykovets*, the information that is targeted by s. 487.0142 will tend to support inferences in relation to other highly personal information.[16]

The weight of the privacy interests at stake calls into question s. 487.0142's use of a "reasonable suspicion" standard, i.e., the bill's most significant remaining hedge against *Charter* violations. The distinction between "reasonable suspicion" and "reasonable grounds to be believe" is well-trodden ground. Reasonable suspicion requires an objective expectation that the target of a search is *possibly* engaged in criminal activity; it does not require *probability*. As Justice Karakatsanis explained for a unanimous Court in *Chehil*, this has a logical consequence: while both standards must deal in objective facts, "[t]he fact that reasonable suspicion deals with possibilities, rather than probabilities, necessarily means that in some cases the police will reasonably suspect that innocent people are involved in crime".[17] In brief, it is an exception that will, in the ordinary case, apply to innocent people. For this reason, reasonable suspicion is and must be available only as a limited exception to the general rule. The exception is available, for instance, if the search is "minimally intrusive, narrowly targeted, and highly accurate", and otherwise coupled with particularized suspicion.[18]

---

[14] *Bykovets* at para 6.
[15] Robert Diab, "Ottawa Reboots Its Lawful Access Bill: What C-22 Fixes and What It Doesn't" (March 14, 2026) https://robertdiab.substack.com/p/ottawa-reboots-its-lawful-access.
[16] *Spencer* at para 26; *Bykovets* at 38 (citing to *Spencer* at para 26 and *R v Marakah* at para 20).
[17] *R v Chehil*, 2013 SCC 49, para 28 [*Chehil*].
[18] *Chehil* at para 28.

The Court's guidance with respect to this limited exception cannot be reconciled with the scope and significance of the information that would be collected via s. 487.0142, professionally wielded. Notably, one Court of Appeal has already effectively come to this conclusion. Specifically, the ONCA has found that the *Criminal Code's* general production power could not justify a search for highly revealing digital information such as an IP address when the information to obtain merely met a "reasonable suspicion" standard.[19] The same applies to a statutory provision designed to produce that and additional information. The default "reasonable grounds to believe" standard must apply.

Our constitutional concerns do not end there. Intended or not, Bill C-22's provisions with respect to voluntary disclosures and information "available to the public" will compound the risk of unlawful searches of private information, and typically in ways that will be invisible to the courts.

As noted, Canadian courts have repeatedly held that third parties are not at liberty to disclose information in which individuals have a reasonable expectation of privacy, without the individuals' informed consent. Indeed, legal uncertainty on this issue is precisely what prompted the Court's landmark decision in *Spencer*. Clauses 11 and 31 do not clarify this unassailable legal principle but throw it into *Charter*-undermining confusion. That is, by creating a permissive framework for informal, voluntary disclosures and requests, with a constitutionally suspect or confusing[20] grant of civil and criminal immunity for the TSPs disclosing, Clauses 11 and 31 would create a framework capable of facilitating the disclosure and collection of information, including in cases wherein the information cannot be disclosed because it is protected under the *Charter*.

The provision authorizing law enforcement to collect publicly available information is similarly on untenable constitutional ground. Courts in Canada have long held that an individual does not lose their reasonable expectation of privacy simply because the information is semi-publicly or publicly available.[21] Whether or what information is subject to a reasonable expectation of privacy, despite being in the public realm, is instead a fact-specific legal question that must be assessed in context. For instance, a trip to the shopping mall with a friend does not automatically make one's "publicly available" biometrics or the contents of one's conversations fair game. More nefariously, being the target of a data breach, or having one's individual social media traits and data compiled into a sophisticated user profile, does not negate an individual's potential claim that they nevertheless hold a reasonable expectation of privacy in the now "publicly available" information. Clauses 11 and 31 ignore this *Charter*-imposed complexity. If the intent of the provisions is to facilitate use if, and only if, such complicated and fact-sensitive restrictions do not apply, it is both unhelpful and misguided. In actual effect, the provision will read as a permission slip for law enforcement and the Service to use private information and information on the darkest corners of the internet, notwithstanding the perverse incentives that will be created by such apparent permission, and notwithstanding *Charter* protections against such use. While this may not be Parliament's intent, the fact that some will read it as such will result in *Charter* violations. The provisions should be withdrawn or significantly amended.

II. **Part 2 of the Lawful Access Act**, the proposed *Supporting Authorized Access to Information Act* (*SAAIA*)

Our brief places an emphasis on Part 1 of Bill C-22. Our focus reflects our overarching concern that the government's legislative package has been brought forward despite its inconsistency with well-established legal

[19] *R v West*, 2020 ONCA 473 (evidence excluded under s. 24(2) of the Charter in a case wherein the officer mistakenly pled and established reasonable grounds to suspect, but not believe, in his information to obtain with respect to an IP address).
[20] Among other things, the *Charter* grants courts remedial discretion to determine just and appropriate remedies for *Charter* violations: s. 24(1). The statutory provision cannot undo this constitutional grant of discretion. If no liability (*Charter* or otherwise) can arise because the information is being lawfully preserved or disclosed, there is no need for immunity.
[21] See, e.g., *R v Jarvis*, 2019 SCC 10.

precedents. This is not a statement that it is the more problematic of the two Parts. If anything, the reverse is arguably true. Accordingly, we endorse the view that withdrawing and re-submitting Part 2 – a legislative package that would transform Canada's lawful access framework, and in ways that continue to be constitutionally problematic – would be a reasonable substitute to withdrawing and re-submitting the bill as a whole, including for reasons set out by witnesses before the House Committee.[22]

That said, we offer brief comment as to how this Committee might meaningfully mitigate some of the most concerning features of the *SAAIA*. This focus is not intended to serve as an implicit endorsement of issues unaddressed, such as its flawed approach to the question of "backdoor" access.

Our starting point is the broad regulatory powers envisioned by the *SAAIA*. Section 5 of the SAAIA would provide the Governor in Council with powers governing the lawful access capabilities of electronic service providers that are deemed "core providers" by regulation. Section 7 would empower the Minister of Public Safety and Emergency Preparedness to impose orders on electronic service providers that are "core providers". Combined, the provisions would enable the government to issue regulations or make ministerial orders regarding "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": ss. 5 and 7. The regulations and orders would also extend to "the installation, use, operation, management, assessment, testing and maintenance of any device, equipment or other thing that may enable an authorized person to access information": ss. 5 and 7. Despite widescale opposition, the regulations and orders would continue to allow for the compelled retention of certain categories of metadata for up to six months: ss. 5 and 7. Service providers can object to actions if they would create "a systemic vulnerability," i.e., "a vulnerability in the electronic protections of an electronic service that creates a credible risk, based on recognized international technical standards, that secure information could be accessed by a person who does not have any right or authority to do so . . .": s. 2.

These provisions appear to provide for an almost limitless scope of the government's powers under the *SAAIA*. They deputize third parties in law enforcement and national security efforts and in ways that that threaten Canadians' security in their private information. They have been widely criticized, and amendments to date have done little to address these widespread concerns with the provisions. For instance, the lowering of the retention time frame from 12 months to 6 months is neither tailored to specific policing requirements or the likely privacy impacts imposed by the sweeping retention policy. Similarly, the strengthening of the definition of systemic vulnerability continues to be overly narrow, such as by failing *to prohibit* regulations and orders that would have the effect of creating systemic vulnerabilities,[23] and by focusing on vulnerabilities that may arise via the provision of "services" while neglecting other, potentially more critical vulnerabilities, such as those that can be created by extraction technologies that are located within operating systems.[24]

We do not canvass these full concerns here. We instead offer a statement of support for the well-founded recommendations that they have prompted, and the further recommendations we anticipate will come before this

---

[22] See, e.g., Citizen Lab & Canadian Civil Liberties Association, "(Un)Forced Errors: Analysis of Proposed Surveillance Law Expansion under Bill C-22, An Act respecting lawful access" (brief submitted to the House of Commons Standing Committee on Public Safety and National Security (SECU), 2 June 2026), and especially the larger joint report incorporated by reference therein.

[23] See Office of the Privacy Commissioner of Canada, Submission to the House of Commons Standing Committee on Public Safety and National Security regarding Bill C-22, An Act Respecting Lawful Access (21 May 2026) at 4 [*OPC*].

[24] Robert Diab et al, "Open Letter Calling for Amendments to Bill C-22" (4 May 2026), online: Robert Diab https://www.robertdiab.ca/posts/open-letter-c22/ ["Open Letter"].

Committee.[25] We instead focus our remaining comments on our significant concern that SAAIA's legislative and regulatory scheme would operate largely in secret and without meaningful, *Charter*-informed oversight.

We acknowledge that the scheme is not without oversight altogether and that the Intelligence Commissioner and the National Security and Intelligence Review Agency would play an oversight role in the scheme's operations. This includes the Intelligence Commissioner's role in approving any ministerial orders targeted at non-core providers. We also acknowledge the recent addition of s. 15.1 to the *SAAIA*, which permits and potentially compels disclosure to regulatory bodies to facilitate the exercise of their own duties or functions.

Be that as it may, this oversight scheme is insufficient. While the proposed s. 15.1 is a step in the right direction, the provision would still make the Minister the necessary intermediary and arbiter as to when and whether information may pass to a relevant regulator, such as the Privacy Commissioner of Canada. A system premised on permanent secret orders, unless such secrecy is undone by Ministerial intervention, cannot facilitate sufficiently independent and transparent oversight. The provision should instead be revised to acknowledge, expressly, that the appropriate regulatory bodies have *independent* rights of access and review, i.e., rights of access and review that do not depend upon Ministerial discretion or action. The change would better facilitate necessary and timely disclosures to appropriate regulatory bodies and would otherwise permit timely judicial resolution of any disputes arising as to whether the regulatory body is entitled to access and use the information in question.

More broadly, the appropriate regulatory bodies, including especially the Privacy Commissioner of Canada, should be further incorporated in the regulatory scheme in other ways. The present scheme provides affected ESPs with limited avenues through which to facilitate independent oversight or scrutiny of orders, absent Ministerial authorizations under s. 15.1. Accordingly, regulations and orders are not subject to a meaningful justification or review process, thereby leaving issues such as necessity and proportionality, and the justification for secrecy for any particular order, to the discretion of the executive branch.[26] The ultimate result is a mostly unfettered regulatory scheme that will often operate in secret, with little assurance that the privacy rights of Canadians are being heard or protected.

To remedy this oversight deficit, we endorse several recommendations that were raised during the bill's progress through the House.[27] First, core provider obligations and ministerial orders should be made subject to the requirements of necessity and proportionality, and should be made subject to review by the Privacy Commissioner of Canada, before they take effect.[28] Second, the Minister should be required to justify confidentiality for all orders. Finally, confidentiality restrictions on orders should receive an automatic sunset, the terms of which (and any necessary exemptions from which) should be set by this same justification and oversight framework.

III. Conclusion

While we repeat our overarching recommendation that the best course of action would be to withdraw Bill C-22, or Part 2 specifically, we recognize that some of the bill's most significant constitutional deficiencies may yet be mitigated. Based upon the foregoing, including our above caution that our submissions are not intended to be exhaustive with respect to the *Charter*-issues raised by Bill C-22, we summarize our recommendations as follows:

---

[25] We agree in full with the analysis and recommendations provided by several distinguished privacy law scholars and lawyers in response to the bill as first tabled. See *ibid*.
[26] See *OPC* at 3 and Open Letter at 4 – 5, respectively.
[27] *Ibid*.
[28] *OPC* at 3.

Recommendation 1 (Clause 4, Subscriber Information Definition)
Narrow the definition of "subscriber information" to discrete identifying information necessary to link an individual to a service or account. Information relating to services used, devices used, or the when and where of service use should be excluded.

Recommendation 2 (Clauses 5 and 31, Confirmation of Service Demands)
Replace the "reasonable grounds to suspect" standard applicable to confirmation of service demands with a "reasonable grounds to believe" standard.

Recommendation 3 (Clause 6, Subscriber Information Production Orders)
Replace the "reasonable grounds to suspect" standard applicable to subscriber information production orders with a "reasonable grounds to believe" standard.

Recommendation 4 (Clause 11, Voluntary Disclosure and Publicly Available Information)
Remove the provisions purporting to authorize or clarify: voluntary disclosure requests; unsolicited disclosures; immunity from civil and criminal liability; and the collection of information characterized as "available to the public". In the alternative, substantially amend these provisions to expressly preserve *Charter*-protected privacy interests and to clarify that they do not authorize the collection or disclosure of information in which a reasonable expectation of privacy exists.

Recommendation 5 (Clause 31, CSIS Immunity Provisions)
Remove the immunity provisions shielding voluntary disclosures to CSIS from civil and criminal proceedings.

Recommendation 6 (Clause 41, Scope of Regulatory Powers)
Amend the *SAAIA* to prohibit regulations or orders that would: require providers to alter products or services offered in the ordinary course of business; require providers to collect or retain information for non-business purposes; or require providers to alter the functionality of products or services for surveillance purposes.

Recommendation 7 (Clause 41, Independent Regulatory Access and Review)
Amend proposed s. 15.1 to provide the Privacy Commissioner of Canada and other appropriate regulatory bodies with independent statutory rights of access to relevant information, without requiring ministerial authorization or intervention.

Recommendation 8 (Clause 41, Necessity, Proportionality, and Independent Review)
Require all core provider obligations, regulations, and ministerial orders to satisfy express statutory requirements of: necessity, proportionality, and independent review before taking effect, including specifically review by the Privacy Commissioner of Canada where privacy interests are engaged.

Recommendation 9 (Clause 41, Confidentiality Orders)
Require the Minister to justify confidentiality restrictions on a case-by-case basis. Require confidentiality restrictions imposed under the SAAIA to: expire automatically after a defined period unless renewed on justification; be subject to review by the Privacy Commissioner and other appropriate oversight bodies; and remain subject to judicial review.

DAVID ASPER CENTRE FOR CONSTITUTIONAL RIGHTS

The David Asper Centre for Constitutional Rights is a centre within the University of Toronto, Faculty of Law devoted to advocacy, research and education in the area of constitutional rights in Canada. The Centre was established in 2008 by the generous donation of David Asper and was officially launched in early September 2008. It houses a unique legal clinic that brings together students, faculty, members of the bar and other advocates to work on significant constitutional cases and advocacy projects. It is the only Canadian centre in existence that attempts to bring constitutional law research, policy, advocacy and teaching together under one roof. Access to justice and social justice are clear themes that have motivated the advocacy work of the Centre since its inception. The Centre defines these themes more specifically as access to constitutional rights.