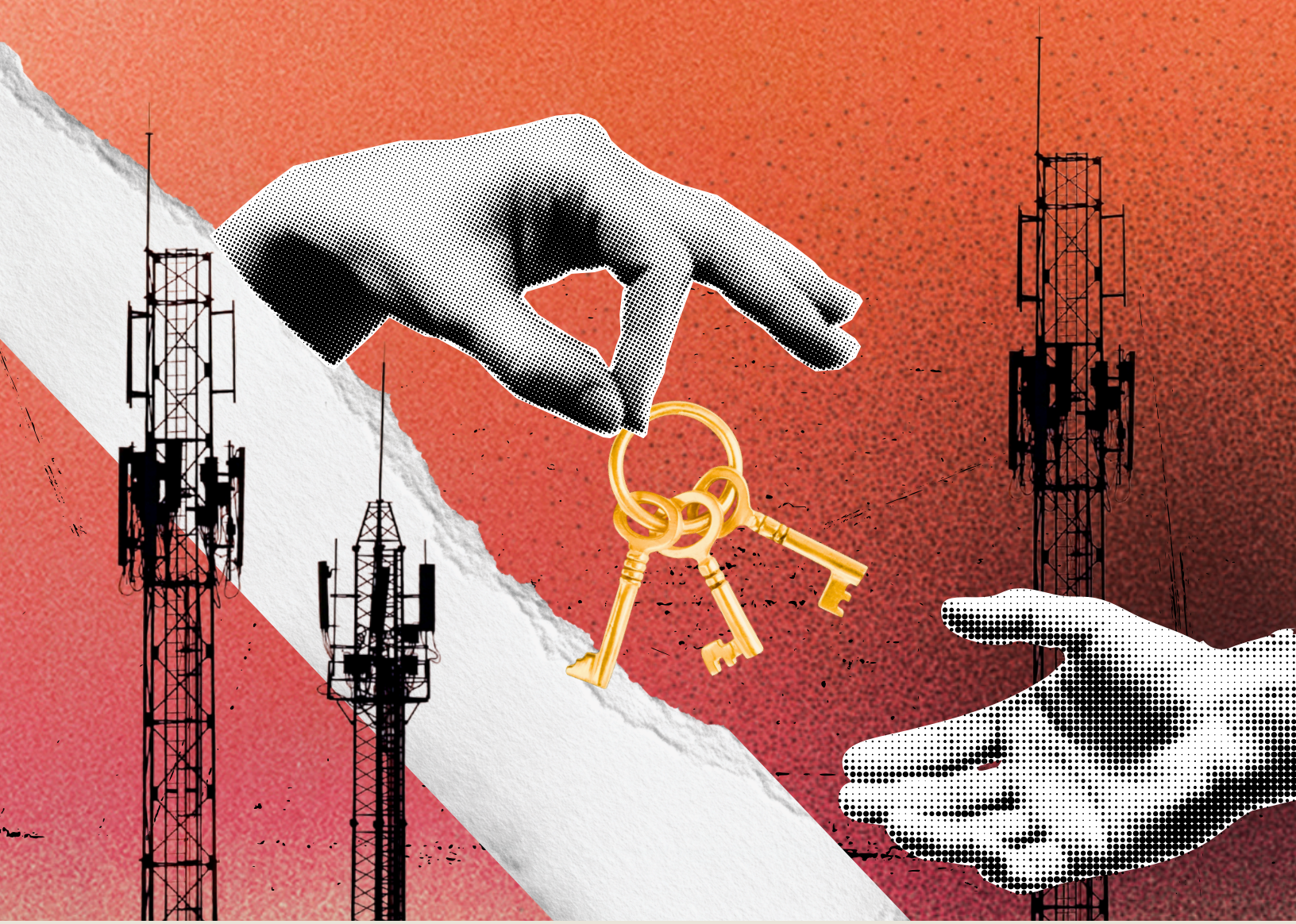
(UN)FORCED ERRORS

Analysis of Proposed Surveillance Law Expansion under Bill C-22, *An Act respecting lawful access*

June 2, 2026

By Cynthia Khoo, Tamir Israel, and Kate Robertson



THECITIZENLAB

munkschool OF GLOBAL AFFAIRS & PUBLIC POLICY

UNIVERSITY OF TORONTO

CANADIAN CIVIL LIBERTIES ASSOCIATION

ASSOCIATION CANADIENNE DES LIBERTÉS CIVILES

Table of Contents

Introduction and Overview

1. Bill C-22, the *Lawful Access Act*, proposes a range of new surveillance authorizations to be made available to Canadian law enforcement agencies and the Canadian Security Intelligence Service ("CSIS"). The bill effectively reintroduces what were formerly Parts 14 and 15 of Bill C-2, the *Strong Borders Act*, with modifications. While we acknowledge that efforts were made to address some of the problematic elements of Bill C-2, several deeply concerning issues remain. Some modifications even broaden the scope of what was proposed in the earlier legislation. More than one aspect of the bill is almost certainly constitutionally fatal.

2. In this brief, we provide targeted analysis and priority recommendations focused on aspects of Bill C-22 with the most pressing and far-reaching implications. Due to the urgent timeline that has been established for study of the bill by the House of Commons Standing Committee on Public Safety and National Security ("SECU"), the analysis provided in this brief is far from exhaustive. In fact, the very rush instilled by the government in its haste to pass this bill is itself cause for concern and reason to question the soundness of the proposed legislation. By comparison, the less complex Bill C-8, the *Critical Cyber Systems Protection Act*, has been granted far more time in committee for due scrutiny and broad expert input, while the Australian equivalent of Part 2 of this bill was subject to no less than 173 amendments before being passed.[1]

3. Our core recommendation is to entirely withdraw **Part 2** of the bill. As presented, Part 2 is fundamentally flawed in ways that are difficult to address in the committee process. This is due to its combination of an open-ended scope of application with flexible, ill-defined safeguards and a framework heavily immunized from judicial authorization and control. Overall, Part 2 provides the government with maximum flexibility, minimal restrictions, and minimal judicial scrutiny; this is an unacceptable combination and one that makes the proposed legislation simply unfit for purpose. Our recommended amendments should be viewed as a last-resort measure provided in the spirit of harm reduction, not as an indicator that Part 2 is acceptable; from a constitutional and human rights standpoint, it is not.

4. We further recommend that SECU suspend its study of **Part 1** until the federal government complies with the *Policy on Tabling of Treaties in Parliament*. Our analysis of this bill raised serious concerns regarding the extent to which it appears to be laying the groundwork for foreign data-sharing arrangements with consequential repercussions, including a more closely interlocked law enforcement system and legal regime with the United States ("US"). Specifically, we call on the Canadian government to provide full transparency regarding Canada's potential adoption of two international data-sharing treaties that are linked to Bill C-22: the Second Additional Protocol to the Budapest Convention on Cybercrime ("2AP"), and a Canada-US data-sharing agreement under the US *Clarifying Lawful Overseas Use of Data* Act ("CLOUD Act").

5. Further in Part 1, we recommend that the provisions regarding "publicly available information" and "voluntary provision" of information both be removed from the bill. Both provisions involve

[1] Parliament of Australia, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, Parliament no 45, online: <https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6195>; Parliament of Australia, House of Representatives, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, EK171, online: <https://parlinfo.aph.gov.au/parlInfo/download/legislation/amend/r6195_amend_2ef65c47-7a59-45e1-9427-cf3e7400ef4d/upload_pdf/EK171.pdf>.

misleading characterizations of the current state of the law, and are unnecessary for their ostensible respective purposes. Worse than unnecessary, if enacted as drafted, they would contradict decades of Supreme Court of Canada jurisprudence regarding, respectively, the existence of reasonable expectations of privacy in public spaces, and the law on consent to search and seizure as well as the long-abandoned third-party consent doctrine. In the event these provisions are not removed, again we provide suggested amendments to ameliorate, as a mitigatory measure.

6. The complete list of our recommendations arising from this brief, including proposed amendment language for drafting, is provided in a table in Part E.

7. The remainder of this brief is organized as follows:

About the Submission and Authors

8. This brief provides joint comments regarding Bill C-22, the *Lawful Access Act*, from Kate Robertson, Senior Research Associate, and Cynthia Khoo, Senior Fellow, who are legal experts and researchers at the Citizen Lab (Munk School of Global Affairs & Public Policy, University of Toronto), in their professional and individual capacities, and Tamir Israel, Director of the Privacy, Surveillance & Technology Program, on behalf of the Canadian Civil Liberties Association ("CCLA"). The authors and their respective organizations have specialized for many years in, collectively, privacy law and policy—in both its consumer data protection and constitutional dimensions—national security law and policy, cybersecurity and encryption policy, state surveillance, commercial surveillance, and the interaction of digital technologies and information networks with human rights and civil liberties. This has included working on, in various modalities, earlier iterations of lawful access legislation introduced by successive Canadian governments.[2]

9. The CCLA is an independent, national, nongovernmental organization that was founded in 1964 with a mandate to defend and foster the civil liberties, human rights, and democratic freedoms of all people across Canada. Its work encompasses advocacy, research, and litigation related to the criminal justice system, equality rights, privacy rights, and fundamental constitutional freedoms.

[2] See e.g. Lex Gill, Tamir Israel, and Christopher Parsons, "Shining a Light on the Encryption Debate: A Canadian Field Guide," Joint Research Publication, Citizen Lab & the Canadian Internet Policy & Public Interest Clinic (May 2018), online: <https://citizenlab.ca/wp-content/uploads/2018/05/Shining-A-Light-Encryption-CitLab-CIPPIC.pdf>; Christopher Parsons, Lex Gill, Tamir Israel, Bill Robinson & Ronald Deibert, "Analysis of the Communications Security Establishment Act and Related Provisions in Bill C-59 (An Act respecting national security matters), First Reading (December 18, 2017)," The Citizen Lab, Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC) (December 2017), online: <https://citizenlab.ca/wp-content/uploads/2017/12/C-59-Analysis-1.0.pdf>; Christopher Parsons and Tamir Israel, "Canada's Quiet History of Weakening Communications Encryption," Citizen Lab Research Report No 60, University of Toronto (August 2015), online: <https://citizenlab.ca/research/canadas-quiet-history-of-weakening-communications-encryption/>.

Working to achieve government transparency and accountability with strong protections for personal privacy lies at the core of the CCLA's mandate.

10. The Citizen Lab, at the Munk School of Global Affairs & Public Policy, University of Toronto, is an interdisciplinary laboratory which focuses on research, development, and high-level strategic policy and legal engagement at the intersection of information and communication technologies, human rights, and global security. Its work relies on a "mixed methods" approach to research combining practices from political science, law, computer science, and area studies. Citizen Lab research has included, among other work: investigating digital espionage against civil society; documenting Internet filtering and other technologies and practices that impact freedom of expression online; analyzing privacy, security, and information controls of popular applications; and examining transparency and accountability mechanisms related to the relationship between corporations and state agencies regarding personal data and other surveillance activities.

A. The Supporting Authorized Access to Information Act (SAAIA)

11. Part 2 of Bill C-22 would enact the *Supporting Authorized Access to Information Act* ("SAAIA"), creating a surveillance capability regime by which the government can impose any obligation onto any electronic service provider ("ESP") for the purpose of facilitating lawful use of surveillance authorizations. Under the proposed SAAIA, the government could potentially require any ESP to access, record, and keep any sensitive metadata within their reach on every person in Canada or abroad for up to one year.

12. The SAAIA creates a far-ranging framework by which the government will be able to impose various obligations onto a wide range of digital services with the objective of facilitating surveillance. The regime is framed so broadly that it rivals any existing authorization currently in our *Criminal Code* in terms of its capacity to expand the intrusiveness of surveillance powers. Surveillance capability regimes such as the SAAIA also pose a real threat to cybersecurity. The frameworks they create allow governments to impose their shifting surveillance ambitions at the cost of the cybersecurity of all. Too frequently, governments have reached the wrong conclusion when considering the tradeoffs involved, with severe consequences.[3]

13. The need to align Canada with its Five Eyes partners has been a frequent justification for adoption of the SAAIA. However, as the National Security Intelligence Committee of Parliamentarians ("NSICOP") found in their 2025 report on lawful access, only half of our Five Eyes partners—the United Kingdom ("UK") and Australia—have enacted surveillance capability regimes that approach the SAAIA in terms of breadth. Frameworks in the other half—the US and

[3] Zack Whittaker, "The 30-year-old internet backdoor law that came back to bite," Tech Crunch (7 October 2024), online: <https://techcrunch.com/2024/10/07/the-30-year-old-internet-backdoor-law-that-came-back-to-bite/>; Susan Landau, "The Dangers Lurking in the U.K.'s Plan for Electronic Eavesdropping," Lawfare (25 February 2025), online: <https://www.lawfaremedia.org/article/the-dangers-lurking-in-the-u.k.-s-plan-for-electronic-eavesdropping>; Lex Gill, Tamir Israel, and Christopher Parsons, "Shining a Light on the Encryption Debate: A Canadian Field Guide," Joint Research Publication, Citizen Lab & the Canadian Internet Policy & Public Interest Clinic (May 2018), online: <https://citizenlab.ca/wp-content/uploads/2018/05/Shining-A-Light-Encryption-CitLab-CIPPIC.pdf>; Christopher Parsons and Tamir Israel, "Canada's Quiet History of Weakening Communications Encryption," The Citizen Lab Research Report No 60, University of Toronto (August 2015), online: <https://citizenlab.ca/research/canadas-quiet-history-of-weakening-communications-encryption/>.

New Zealand—remain limited to imposing wiretap capabilities onto telecommunications carriers, which only provide access to phone systems and the Internet.[4]

14. The constitutionality of the UK regime is currently being challenged after a secret government order from the UK's Home Office issued to Apple was leaked to the public.[5] In 2022, Apple introduced a critical encryption safeguard to protect iCloud backups ("Advanced Data Protection"). As a result of this order, that safeguard has now been removed for Apple devices connecting from the UK. The Australian regime, for its part, was held to be "incompatible with [human] rights" by the Parliamentary Joint Committee on Human Rights when it conducted its mandatory assessment of the regime, due to being "unlikely to constitute a proportionate limitation on the rights to privacy and freedom of expression."[6]

15. At the same time, narrower technical capability regimes, such as those enacted in the US and New Zealand, are still vulnerable to cybersecurity attacks, and have been successfully and secretly targeted multiple times by foreign intelligence agencies.[7] A leaked US National Security Agency document, for example, details how the agency actively targets and exploits "lawful intercept" capabilities imposed in other jurisdictions to facilitate its foreign intelligence gathering.[8] The most recently discovered compromise, attributed to the advanced persistent threat actor with ties to the government of China, Salt Typhoon, has been characterized as one of the most severe national security breaches in US history.[9] Technical modifications made in

---

[4] National Security Intelligence Committee of Parliamentarians, "Special Report on the Lawful Access to Communications by Security and Intelligence Organizations" (September 2025) at page 15 (Table 2.1), online: <https://nsicop-cpsnr.ca/reports/rp-2025-09-15-sr/250915_NSICOP_Lawful_access_report.pdf>.

[5] Privacy International, "PI Apple TCN Challenge," online: <https://privacyinternational.org/legal-action/pi-apple-tcn-challenge>; Privacy International, "The Second Order: The UK Government's new secret order still strikes at Apple's security" (1 October 2025), online: <https://privacyinternational.org/news-analysis/5685/second-order-uk-governments-new-secret-order-still-strikes-apples-security>; Apple Inc v Secretary of State for the Home Department, [2025] UKPITrib 1, online: <https://investigatorypowerstribunal.org.uk/wp-content/uploads/2025/04/IPT-25-68-CH-Judgment.pdf>; Human Rights Watch, "UK Encryption Order Threatens Global Privacy Rights" (14 February 2025), online: <https://www.hrw.org/news/2025/02/14/uk-encryption-order-threatens-global-privacy-rights>; Joseph Menn, "U.K. orders Apple to let it spy on users' encrypted accounts," Washington Post (7 February 2025), online: <https://www.washingtonpost.com/technology/2025/02/07/apple-encryption-backdoor-uk/>.

[6] Australia, Parliamentary Joint Committee on Human Rights, Human Rights Scrutiny Report (4 December 2018) at para 2.196, online: <https://www.aph.gov.au/-/media/Committees/Senate/committee/humanrights_ctte/reports/2018/Report_13/Report_13_of_2018.pdf>.

[7] "CCLA and Coalition of Coalitions Call for Withdrawal of Bill C-2," (11 July 2025), online: *Canadian Civil Liberties Association* <https://ccla.org/privacy/ccla-joins-calls-for-withdrawal-of-bill-c-2/>; Ryan Devereux, Glenn Greenwald & Laura Poitras, "Data Pirates of the Caribbean," *Intercept* (19 May 2024), online: <https://theintercept.com/2014/05/19/data-pirates-caribbean-nsa-recording-every-cell-phone-call-bahamas/>; Vassilis Prevelakis & Diomidis Spinellis, "The Athens Affair," (2007) 44(7) *IEEE Spectrum*, online: <https://spectrum.ieee.org/the-athens-affair>; Susan Landau, "CALEA Was a National Security Disaster Waiting to Happen," *Lawfare* (13 November 2024), online: <https://www.lawfaremedia.org/article/calea-was-a-national-security-disaster-waiting-to-happen>; Testimony of Susan Landau, House of Representatives, Subcommittee on Crime and Federal Government Surveillance of the Committee on the Judiciary (5 June 2025) at page 8, online (PDF): <https://www.congress.gov/119/meeting/house/118335/witnesses/HHRG-119-JU08-Wstate-LandauS-20250605.pdf>.

[8] United States, National Security Agency, "Exploiting Foreign Lawful Intercept (LI) Roundtable," TOP SECRET//SI/REL TO USA, FVEY," online (PDF): <https://christopher-parsons.com/wp-content/uploads/2023/01/nsa-exploiting-foreign-lawful-intercept-li-roundtable.pdf>, document published in James Bamford, "A Death in Athens," *Intercept* (28 September 2015), online: <https://theintercept.com/2015/09/28/death-athens-rogue-nsa-operation/>. For a summary, see Christopher Parsons, "Exploiting Foreign Lawful Intercept (LI) Roundtable," online: *Technology, Thoughts & Trinkets* <https://christopher-parsons.com/resources/the-sigint-summaries/nsa-summaries/#exploiting-foreign-lawful-intercept-li-roundtable>.

[9] Internet Society, "Open Letter: Bill C-22, An Act Respecting lawful access," online: <https://www.hilltimes.com/sponsored/open-letter-bill-c-22-an-act-respecting-lawful-access/>; Susan Landau, "CALEA Was a National Security Disaster Waiting to Happen," *Lawfare* (13 November 2024), online: <https://www.lawfaremedia.org/article/calea-was-a-national-security-disaster-waiting-to-

compliance with these obligations are also notoriously difficult to secure. When the US National Security Agency tested CALEA-compliant equipment for potential use in government networks, it found that every single switch it tested had a security flaw.[10]

16. Governments today also generally recognize the importance of cybersecurity and encryption.[11] But at different times over the years, various government agencies have advanced numerous different proposals that would in effect compromise, circumvent, bypass, or weaken encryption.[12] When initially advanced, these proposals are never presented as a "backdoor" or an attempt to undermine encryption, but rather as a mechanism for Public Safety and other government agencies to access secure data on a case-by-case basis. While none of these proposals have withstood public scrutiny and all have been shown to present a significant cybersecurity threat, the underlying belief still persists among various government agencies that exceptional access to secure data is possible.

17. With this troubling historical track record in mind, the SAAIA is fundamentally flawed in three inter-related ways. First, it is exceedingly broad in scope. This breadth appears designed to give the government the maximum amount of flexibility to address any current or future technology or surveillance technique it might want to deploy. Second, the SAAIA's safeguards and limitations are also designed to provide the government significant flexibility in achieving its surveillance objectives. Finally, the SAAIA's oversight regime is by design heavily deferential to executive decision-making, limiting its capacity for judicial control and enabling it to operate both in secrecy and without broad stakeholder input.

18. Collectively, this mix of open-ended powers, flexible safeguards, and a government-driven oversight framework that excludes strict judicial controls creates significant human rights, privacy, and cybersecurity hazards. We elaborate on these concerns below.

A.1. SAAIA is Overbroad in Scope and Application

19. The SAAIA would enact a technical surveillance capability regime that allows the government to compel electronic service providers to re-engineer their services in order to facilitate and expand police and CSIS's use of existing data access authorizations. The Act is framed broadly in terms

---

happen>; Joe Mullin and Cindy Cohn, "Salt Typhoon Hack Shows There's No Security Backdoor That's Only for the 'Good Guys'" (9 October 2024), online: *Electronic Frontier Foundation* <https://www.eff.org/deeplinks/2024/10/salt-typhoon-hack-shows-theres-no-security-backdoor-thats-only-good-guys>; David E Singer, Julian E Barnes, Devlin Barrett & Adam Goldman, "Emerging Details of Chinese Hack Leave US Officials Increasingly Concerned," *New York Times* (22 November 2024), online: <https://www.nytimes.com/2024/11/22/us/politics/chinese-hack-telecom-white-house.html>; Marie Woolf, "Lawful-access bill could threaten encryption, deter investment," *Globe and Mail* (1 May 2026), online: <https://www.theglobeandmail.com/politics/article-lawful-access-bill-could-threaten-encryption-deter-investment-chamber/>.

[10] Testimony of Susan Landau, House of Representatives, Subcommittee on Crime and Federal Government Surveillance of the Committee on the Judiciary (5 June 2025) at page 8, online (PDF): <https://www.congress.gov/119/meeting/house/118335/witnesses/HHRG-119-JU08-Wstate-LandauS-20250605.pdf>.

[11] Mason Boycott-Owen, "UK intelligence: 100 nations have spyware that can hack Britain," *Politico* (22 April 22, 2026), online: <https://www.politico.eu/article/u-k-intelligence-100-nations-have-spyware-that-can-hack-britain/>.

[12] Lex Gill, Tamir Israel, and Christopher Parsons, "Shining a Light on the Encryption Debate: A Canadian Field Guide," Joint Research Publication, Citizen Lab & the Canadian Internet Policy & Public Interest Clinic (May 2018) at pages 21-29 ("Part 3: Going Dark? Four Decades of Debate"), online: <https://citizenlab.ca/wp-content/uploads/2018/05/Shining-A-Light-Encryption-CitLab-CIPPIC.pdf>.

of both the types of ESPs that could face obligations and the types of obligations that could be imposed. Moreover, the SAAIA can be invoked to facilitate investigations of even the most minor of offences, and the obligations it puts in place are not time-limited.[13]

20. The SAAIA also includes a data retention regime that can be used to compel electronic service providers to record and keep sensitive metadata that they do not currently have access to at all. While the SAAIA's technical surveillance capability regime and its metadata retention regime both share many of the same problems with overbreadth, it is helpful to consider these two regimes separately.

A.1.i. Overbreadth of Technical Surveillance Capabilities Regime

21. Under the current definition, any provider of any service that includes a digital mechanism can qualify as an ESP,[14] and be thus subject to obligations under the SAAIA.[15] This includes anything from phone and Internet access providers, to social media sites, to private messaging applications, to the operating system on a phone or laptop. A fast-food chain, university, or library are considered ESPs if they operate a Wifi network, and so might be compelled to embed various surveillance capabilities, as we learned from the Australian experience.[16] Consider an electronics store (e.g. Apple, Best Buy) or any store with an online or mobile shopping option: all have been listed as valid and even anticipated targets under the Australian regime.[17] Chatbots based on generative artificial intelligence ("AI") and

[13] By contrast, obligations under Australia's Technical Capability Notice regime expire after one year, can only be applied to facilitate investigations of serious crimes, and the Attorney-General must not give a TCN to a designated provider unless satisfied that the requirements imposed are reasonable and proportionate, and that compliance is practicable and technically feasible: Australia, *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*, No. 148, 2018, ss 317T(2)-(3) (TCNs limited to serious Australian or foreign offences or safeguarding national security), s 317TA(1A)("An expiry date specified in a technical capability notice must not be later than 12 months after the notice was given."); and s 317(V): "must not give a technical capability notice to a designated communications provider unless: (a) the Attorney-General is satisfied that the requirements imposed by the notice are reasonable and proportionate; and (b) the Attorney-General is satisfied that compliance with the notice is: (i) practicable; and (ii) technically feasible."

[14] Bill C-22, *An Act respecting lawful access*, First Session, Forty-fifth Parliament, 3-4 Charles III, 2025-2026, Part 2, *Supporting Authorized Access to Information Act*, s 2(1) (emphasis added) ("electronic service" means a service, or a feature of a service, that involves the creation, recording, storage, processing, transmission, reception, emission or making available of information in electronic, digital or any other intangible form by an electronic, digital, magnetic, optical, biometric, acoustic or other technological means, or a combination of any such means.; "electronic service provider" means a person that, individually or as part of a group, provides an electronic service, including for the purpose of enabling communications, and that (a) provides the service to persons in Canada; or (b) carries on all or part of its business activities in Canada") [SAAIA].

[15] Under the SAAIA, the government will be able to impose various obligations onto electronic service providers ("ESPs"). Obligations can be imposed by various means. Under section 5 of the proposed SAAIA, Cabinet can issue regulations imposing obligations onto subsets ESPs designated as "core providers." Under section 7, the same set of obligations can be imposed on any ESP, including a designated core provider, by order of the Minister of Public Safety. Finally, under section 24, any ESP or core provider can be required to take specific steps to ensure compliance with an order or regulation through a compliance order issued by any person designated by the Minister.

[16] Paul Karp, "Spies with that? Police can snoop on McDonald's and Westfield wifi customers," Guardian (28 May 2019), online: <https://www.theguardian.com/business/2019/may/28/spies-with-that-police-can-snoop-on-mcdonalds-and-westfield-wifi-customers>; Australia, Department of Home Affairs, "The Assistance and Access Act - An Interim Guide for: Security, Intelligence and Law Enforcement" (26 July 2019, documents released under the Freedom of Information Act 1982 (Cth), FA 19/06/00892) at page 20, online: <https://www.homeaffairs.gov.au/foi/files/2019/fa190200278-document-released.PDF> ("Examples of designated communications providers: McDonald's; Westfield or other free wifi providers").

[17] Australia, Department of Home Affairs, "The Assistance and Access Act - An Interim Guide for: Security, Intelligence and Law Enforcement" (26 July 2019, documents released under the Freedom of Information Act 1982 (Cth), FA 19/06/00892), online: <https://www.homeaffairs.gov.au/foi/files/2019/fa190200278-document-released.PDF> at page 20 ("Examples of designated communications providers: Apple Store … any Australian retailer who offers a mobile phone application for online shopping or offers an application for mobile viewing").

"AI agents" may also be subject to this regime,[18] and could be ordered to assist with law enforcement surveillance on their users via SAAIA obligations.

22. As for the obligations themselves, under the proposed bill, the government would be able to simply make regulations or orders "respecting the obligations" of service providers.[19] The SAAIA provides an indicative list of the types of obligations that might be imposed. This list is so broad that, in practice, the primary restriction that the SAAIA places on potential obligations is that they would need to advance the SAAIA's purpose, which is to "ensure that [ESPs] can facilitate the exercise of authorities to access information."[20] Drawing on existing police powers and examples from other jurisdictions, the government could obligate:

    a. an email provider to develop a system-wide tool that automates resetting a police target's password, provides police with the new password so they can access the account, and then surreptitiously restoring the original password so the target never becomes aware their account was compromised;[21]
    b. a mobile device operating system to develop the ability to block secure private messaging applications from operating on specific devices in order to force specific targets to rely on less secure communications for specific periods of time to facilitate lawful intercept;[22]

---

[18] For purposes of this brief, we use the term "artificial intelligence" ("AI") to refer generally to classes of technologies currently broadly understood to fall under the umbrella term "AI" at time of writing, whether or not they would strictly meet a given scientific or technical definition associated with "AI," and understanding the phrase is more often than not used as a marketing term or to advance a regressive political and economic agenda. Referenced technologies may include, for example, large language models ("LLMs"), generative AI chatbots, or algorithmic decision-making, surveillance, or analytics tools. For more details, see British Columbia Law Institute, *Report on Artificial Intelligence and Civil Liability*, BCLI Report no 96 (April 2024) at pages 5-8 ("2. Definitional Elements"), online (PDF): <https://www.bcli.org/wp-content/uploads/Report-AI-and-civil-liability-final.pdf>; Kara Williams & Ben Winters, "Specific Terms for Specific Risks: The Need for Accurate Definitions of AI Systems in Policymaking" (1 October 2025), online: EPIC <https://epic.org/specific-terms-for-specific-risks-the-need-for-accurate-definitions-of-ai-systems-in-policymaking/>; and Emily Tucker, "Artifice and Intelligence," *Tech Policy Press* (16 March 2022), online: <https://www.techpolicy.press/artifice-and-intelligence/>.

[19] SAAIA, s 5(2): "The Governor in Council may make regulations respecting the obligations of core providers, including regulations respecting (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; (b) 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; (c) notices to be given to the Minister or other persons, including with respect to any capability referred to in paragraph (a) and any device, equipment or other thing referred to in paragraph (b); and (d) the retention of categories of metadata — including transmission data, as defined in section 487.011 of the Criminal Code — for reasonable periods of time not exceeding one year."

[20] SAAIA, ss 3, 5(2) and 7(1); See, e.g. *Bell Canada v Bell Aliant Regional Communications*, 2009 SCC 40, at paras 28-32; *Reference re Broadcasting Regulatory Policy CRTC 2010-167 and Broadcasting Order CRTC 2010-168*, 2012 SCC 68, at paras 26-27; *Telus Communications v Federation of Canadian Municipalities*, 2025 SCC 15, at paras 33-34.

[21] *R v Strong*, 2020 ONSC 7528, at para 100(c); see also Australia, Department of Home Affairs, "The Assistance and Access Act - An Interim Guide for: Security, Intelligence and Law Enforcement" (26 July 2019, document released under the Freedom of Information Act 1982 (Cth), FA 19/06/00892) at pages 21-23, online: <https://www.homeaffairs.gov.au/foi/files/2019/fa190200278-document-released.PDF> (Examples: "Requesting a cloud storage provider changes the password on a remotely hosted account to assist in the execution of a warrant"; Requesting that the provider delete an audit log in a customer's device relating to a computer access warrant; Requesting a provider restore a password that was temporarily changed to enable a computer access warrant").

[22] Australia, Department of Home Affairs, "The Assistance and Access Act - An Interim Guide for: Security, Intelligence and Law Enforcement" (26 July 2019, documents released under the Freedom of Information Act 1982 (Cth), FA 19/06/00892) at page 22, online: <https://www.homeaffairs.gov.au/foi/files/2019/fa190200278-document-released.PDF> ("Temporarily blocking internet messaging to force a device to send messages as unencrypted SMS").

c. a social media platform to create a tool that automates creation of detailed, realistic fake profiles to be used in undercover operations;[23]
d. an Internet Service Provider to create an automated tool for a target to be assigned a particular IP address so that their computer can be accessed remotely by police;[24]
e. a secure private messaging application to create fake hidden accounts and surreptitiously add these to targeted group chats;[25]
f. an online banking website to develop the ability to disable a specific target's second factor authentication mechanism;
g. a secure email service to create a password interface that can be deployed against any specific target in order to bypass password security protocols for that target;[26]
h. a server host to install a government data surveillance device in its hosting facility;[27] or
i. a mobile Internet provider to develop the ability to downgrade any targeted customer's cell service from 5G to a less secure and more easily compromised connectivity protocol (3G).

Police and national security agencies would still require a court order to make use of these capabilities, but that does nothing to mitigate the intrusiveness of the capabilities themselves.

23. As mentioned above, the breadth of the proposed SAAIA is even more notable when compared to those operated by Canada's Five Eyes partners. Regimes in the US and New Zealand are limited in terms of service providers covered (confined to telecommunications carriers alone) and in terms of the types of obligations that can be imposed (confined to the ability to intercept or wiretap communications).[28] The US regime, for its part, is further limited in that its obligations are met through the adoption of equipment that meets any publicly accepted wiretapping standards.[29]

---

[23] *Ibid* at page 22 ("Operational examples from agencies … Requesting that a social media platform assist with testing or development of a tool to automate the creation of online personas and historical content to facilitate online engagement").

[24] *Ibid* at page 22 (Operational examples from agencies … Requesting a provider allocate a specific dynamic IP address relating to remote access pursuant to a computer access warrant to conceal the access").

[25] *Ibid* at page 22 (extrapolating from "Operational examples from agencies … Requesting the creation of fake accounts, focused on social media sites"); see also Paul Rosler, Christian Mainka & Jorg Schwenk, "More is Less: On the End-to-End Security of Group Chats in Signal, WhatsApp, and Threema, (2018) *IEEE Euro S&P*, online (PDF): <https://eprint.iacr.org/2017/713.pdf>.

[26] Ryan Singel, "Hushmail to Warn Users of Law Enforcement Backdoor," Nov 19, 2007, *WIRED*, <https://www.wired.com/2007/11/hushmail-to-war/>; Lex Gill, Tamir Israel, and Christopher Parsons, "Shining a Light on the Encryption Debate: A Canadian Field Guide," Joint Research Publication, Citizen Lab & the Canadian Internet Policy & Public Interest Clinic (May 2018), online: <https://citizenlab.ca/wp-content/uploads/2018/05/Shining-A-Light-Encryption-CitLab-CIPPIC.pdf>, at pages 63-64.

[27] Australia, Department of Home Affairs, "The Assistance and Access Act - An Interim Guide for: Security, Intelligence and Law Enforcement" (26 July 2019, documents released under the Freedom of Information Act 1982 (Cth), FA 19/06/00892) at page 21, online: <https://www.homeaffairs.gov.au/foi/files/2019/fa190200278-document-released.PDF>: "Requesting a shared data centre provide access to customers computer rack to enable the execution of a computer access warrant or installation of a data surveillance device under warrant."; SAAIA, s 5(2)(b) 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."

[28] National Security Intelligence Committee of Parliamentarians, "Special Report on the Lawful Access to Communications by Security and Intelligence Organizations" (September 2025) at page 15 (Table 2.1), online: <https://nsicop-cpsnr.ca/reports/rp-2025-09-15-sr/250915_NSICOP_Lawful_access_report.pdf>.

[29] United States, Federal Bureau of Investigation, National Domestic Communications Assistance Center, "Lawful Intercept Standards" (24 September 2019), online (PDF): <https://ndcac.fbi.gov/file-repository/listandardscip-1.pdf/view> [https://web.archive.org/web/20251211060730/https://ndcac.fbi.gov/file-repository/listandardscip-1.pdf/view]; Christopher Parsons, "The Governance of Telecommunications Surveillance: How Opaque and Unaccountable Practices and Policies Threaten Canadians," Telecom Transparency Project (2015), online (PDF): <https://christopher-parsons.com/wp-

24. The ability to impose an open-ended set of obligations on a broad range of ESPs creates direct challenges for any attempt to meaningfully constrain the SAAIA, leaving little to no way to ensure that it will be applied in a manner that is consistent with privacy and other human rights while respecting cybersecurity integrity. This will be even more so the case as surveillance technologies continue to evolve.

25. With a growing arsenal of AI-based surveillance techniques on the horizon, the SAAIA's potential for intrusiveness will grow apace. For example, various police agencies are developing an interest in centralizing live video feeds for the purpose of applying AI monitoring tools including visual analytic tools and facial recognition capabilities.[30] In light of the SAAIA's ability to compel direct access and organization of information, the creation of an AI monitoring tool that centralizes live feeds from different camera companies would be squarely within the scope of the law,[31] despite the clearly destructive impacts on Canadian privacy.

26. The *Criminal Code*'s general warrant regime, encoded in s. 487.01, compounds the open-ended nature of the proposed SAAIA. Police can use s. 487.01 to authorize the use of any investigative technique that cannot be authorized by any existing surveillance power.[32] Initially introduced to facilitate authorization for CCTV surveillance, the regime has been used to authorize some of the most intrusive emerging surveillance techniques, including the use of "On-Device Investigative Tools" ("ODITs"), commonly referred to as spyware. ODITs are a surveillance capability that compromises vulnerabilities within electronic services or devices to implant spyware on targets' phones.[33] Given that spyware is a currently relied-upon police technique lawfully authorized under s. 487.01, it would similarly fall within the scope of the SAAIA to compel an ESP to create entry points for this type of highly intrusive surveillance.

A.2.ii. Overbreadth of Mandatory Data Retention Regime

27. The SAAIA's mandatory data retention regime suffers from similar problems of overbreadth. Under the regime, any ESP can be obligated to retain categories of metadata on every individual for up to one year. The SAAIA lacks any restrictions or limitations on when police (or foreign

---

content/uploads/2022/07/1d2f2-the-governance-of-telecommunications-surveillance_-how-opaque-and-unaccountable-practices-and-policies-threaten-canadians-parsons-2015.pdf>.

[30] Nora T Lamontagne, "La police de Montréal peut maintenant vous surveiller en temps réel avec l'IA," *Le journal de montéal* (1 December 2025), online: <https://www.journaldemontreal.com/2026/01/10/le-spvm-peut-maintenant-vous-surveiller-en-temps-reel-avec-lia>; Mrinali Anchan, "Edmonton Police Service partners with US company to test use of facial-recognition bodycams," *CBC News* (2 December 2025), online: <https://www.cbc.ca/news/canada/edmonton/edmonton-police-facial-recognition-cameras-9.7000389>.

[31] SAAIA, s 5(2)(a) (including "organizing" and "access").

[32] *R v TELUS Communications Co*, 2013 SCC 16, at paras 16 and 54.

[33] Kate Robertson & Song-Ly Tran, "Canada's outdated laws leave spyware oversight dangerously weak," *Policy Options* (2 July 2025), online: <https://policyoptions.irpp.org/2025/07/mercenary-spyware/>; Bill Marczak et al, "Virtue or Vice? A First Look at Paragon's Proliferating Spyware Operations" (19 March 2025), online: *Citizen Lab* <https://citizenlab.ca/research/a-first-look-at-paragons-proliferating-spyware-operations/>; Royal Canadian Mounted Police, "On-Device Investigative Tool (ODIT): Technical Description," online (PDF): <https://www.ourcommons.ca/content/Committee/441/ETHI/WebDoc/WD11922842/11922842/RoyalCanadianMountedPolice-TechBrief-e.pdf>; Betsy Powell, "Ontario Police Fight to Keep Their New Spyware Tech Secret," *Toronto Star* (19 May 2026), online: <https://www.thestar.com/news/ontario/ontario-police-are-using-spyware-that-lets-them-remotely-take-over-your-smartphone-theyre-fighting-to-keep-almost-everything-about-it-secret/article_56ef6906-4008-48ec-8b4c-d56e57a00ea5.html>.

agencies) can access retained metadata, on what the ESP itself can do with retained metadata, or on what happens to the metadata once the retention period expires.

28. The SAAIA does not define metadata, but does confirm that this term is broader than the existing definition in the *Criminal Code*,[34] while excluding information that would reveal the "content" of transmitted information, any person's web browsing history, and any person's social media activity.[35] The specific categories of metadata to be retained are not specified in the SAAIA, and can be imposed in the same manner as any other SAAIA obligation.[36] The SAAIA extends to "retention" of information, not merely preservation of information that is already under an ESP's control.[37] Retention, as opposed to preservation, means that ESPs can be compelled to collect or even intercept metadata they do not currently keep at all. Under the SAAIA, ESPs can even be compelled to retain information that does not relate to the electronic service they are providing.[38] When combined with the SAAIA's technical surveillance capability obligations, ESPs can first be compelled to gain access to new types of information and then be obligated to record and keep that information.

29. The resulting breadth of this regime is staggering. The government could use it to compel the creation of a detailed archive of everyone's personal interactions and precise movements.[39] The SAAIA does not include any mechanisms for limiting how metadata is compartmentalized, the

---

[34] SAAIA, s 5(2)(d) ("the retention of categories of metadata — including transmission data, as defined in section 487.011 of the *Criminal Code* — for reasonable periods of time not exceeding one year") (emphasis added). For a discussion of the existing *Criminal Code* definition, see Tamir Israel and Christopher Parsons, "Gone Opaque?: An Analysis of Hypothetical IMSI Catcher Overuse in Canada," Canadian Internet Policy & Public Interest Clinic, Citizen Lab & Telecom Transparency Project (August 2016) at pages 62-64, online: <https://citizenlab.ca/wp-content/uploads/2016/09/20160818-Report-Gone_Opaque.pdf>.

[35] SAAIA, s 5(4) ("Paragraph (2)(d) 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 history; or (c) a person's social media activities.") Note that web browsing and social media activities are not defined in the Act, and subject to definition in regulations.

[36] SAAIA, ss 5(2)-5(3).

[37] In contrast, the issuance of preservation orders (*Criminal Code*, RSC, 1985, c C-46, s 487.013) are only available with respect to computer data that is in the possession and control of the recipient at the time the order is received. See also: Council of Europe, Convention on Cybercrime, CETS No 185, Explanatory Report (23 November 2001) at paras 150-152, online: <https://rm.coe.int/16800cce5b>: "'Data preservation' must be distinguished from 'data retention'. While sharing similar meanings in common language, they have distinctive meanings in relation to computer usage. To preserve data means to keep data, which already exists in a stored form, protected from anything that would cause its current quality or condition to change or deteriorate. To retain data means to keep data, which is currently being generated, in one's possession into the future. ... The preservation measures apply to computer data that 'has been stored by means of a computer system', which presupposes that the data already exists, has already been collected and is stored."

[38] The SAAIA does not limit any of the obligations it imposes to facilitating surveillance in relation to the specific service an ESP provides. See, in contrast, Australia, *Telecommunications (Interception and Access) Act 1979*, No 114, 1979, Compilation No 132, Part 5-1A–Data Retention, sections 187A(1) and (4)(c): "187A(1) A person…who operates a service…must keep…information…or documents…relating to any communication carried by means of the service … 187(4) This section does not require a service provider to keep, or cause to be kept: … (c) information to the extent that it relates to a communication that is being carried by means of another service: (i) that is of a kind referred to in paragraph (3)(a); and (ii) that is operated by another person using the relevant service operated by the service provider; or a document to the extent that the document contains such information" (emphasis added). Note that this paragraph puts beyond doubt that service providers are not required to keep information or documents about communications that pass "over the top" of the underlying service they provide, and that are being carried by means of other services operated by other service providers.

[39] On the sensitivity of various types of metadata, see: Jonathan Mayer, Patrick Mutchler and John C Mitchell, "Evaluating the Privacy Properties of Telephone Metadata," (2016) 113(20) *PNAS* 5536; Jonathan Mayer & Patrick Mutchler, "Metaphone: The Sensitivity of Telephone Metadata," *Web Policy* (12 March 2014), online: <http://webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone-metadata/>; Written Testimony of Ed Felten, House of Representatives, Subcommittee on Crime and Federal Government Surveillance of the Committee on the Judiciary (2 October 2013), online: *Committee on the Judiciary, Hearing on Continued Oversight of the Foreign Intelligence Surveillance Act* <https://www.judiciary.senate.gov/imo/media/doc/10-2-13FeltenTestimony.pdf>.

conditions under which it might be accessed, or how it can be used once the metadata is accumulated.[40] As a result, these detailed archives could potentially be accessible for any domestic or foreign criminal, regulatory, or civil investigation. In combination with the SAAIA's technical surveillance capability regime, a private messaging service could be compelled to gain access to precise geolocation information from the mobile device of every user, transmit this information to itself, and then record it for up to one year, even where doing so would otherwise be in violation of privacy laws.[41]

30. Requiring the indiscriminate and general retention of telecommunications traffic and location data capable of revealing intimate details of an individual's private life has been ruled to be incompatible with the right to privacy and data protection by the highest court in the European Union ("EU") on multiple occasions,[42] while even less sweeping regimes must be subject to strict access limitations. As structured, the SAAIA's metadata provisions are incapable of meeting these requirements. They are not limited by definition to transmission and tracking data, and they include no mechanism for imposing access limitations.

31. Under the Canadian *Charter*, compelling a company to retain personal information that it would not otherwise retain for the purpose of facilitating government access to that information, amounts to a *de facto* seizure.[43] The indiscriminate nature of the retention and the sensitive nature of the information being retained is not, in our view, constitutionally viable.[44]

32. In conclusion, the SAAIA's core problems begin with its expansive breadth. In the next section, we elaborate on how the SAAIA's specific safeguards are incapable of constraining these various proposals, but it is important to note that a fundamental driver of this insufficiency is the sheer breadth of the regime itself. We then provide a suite of recommendations to address the SAAIA's scope and add needed limitations and safeguards.

---

[40] *Law Quadrature du Net and Ors v France (Ministre de la Culture)*, C-470-21, [2024] EU:C:2024:370 (CJEU, Full Court)

[41] Office of the Privacy Commissioner of Canada, *Joint Investigation Into Location Tracking by the Tim Hortons App*, PIPEDA Findings #2022-001 (1 June 2022), online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2022/pipeda-2022-001>.

[42] See e.g. Joint Cases *Digital Rights Ireland Ltd* and *Seitlinger v Minister for Communications, Marine and Natural Resources and others*, C-293/12 and C-594/12, [2014] ECR I-238; and Joint Cases *Tele2 Sverige AB v Post-Och Telestyrelsen* and *Secretary of State for the Home Department v Tom Watson, Peter Brice, and Geoffrey Lewis*, C-203/15 and C-698/15, [2016] ECR I-572.

[43] *R v Laroche*, 2002 SCC 72, paras 33, 50-55 (requiring objects to be retained is a *de facto* seizure under section 8 if there is a "superadded impact upon privacy rights occurring in the context of administrative or criminal investigation"): "The legal character of restraint orders is more problematic, in that such an order does not involve a change in possession of the property to which it applies. However, when the objectives of a restraint order are considered, there is no doubt that it may be characterized as a seizure within the meaning of s. 8. The name given to that order perhaps too easily invites a comparison to a mere restriction on the exercise on property rights. The conservatory nature of the order reinforces such an inclination. However, given that a restraint order is intended to supplement seizures that are taking place contemporaneously, and that they place property under the control of the justice system that might otherwise have eluded it, whether for the purpose of a criminal investigation or for the punishment of crimes that fall within Part XII.2 of the *Criminal Code*, such an order must be characterized as a seizure within the meaning of s. 8 of the *Charter*." See also *R v Reeves*, 2018 SCC 56, at para 31 (seizing a device for the purpose of preserving the information contained on it engages section 8); *R v Hollaman*, 2025 BCCA 315 (police retaining seized property with an informational content beyond statutory time limit implicates section 8 even if no additional investigative step is then taken); *R v Pham*, 2025 BCCA 324 at para 103, leave to appeal granted, SCC File No 42101 (asking a private company to retain a customer's packages for the purpose of facilitating police access engaged the state agency doctrine and section 8); *R v Khairullah*, 2025 ABCJ 14 (holding a provincial law requiring the retention of personal information for later access by law enforcement engaged s. 8 of the *Charter* and was unreasonable in the circumstances).

[44] *R v Laroche*, 2002 SCC 72; *R v Kang-Brown*, 2008 SCC 18; *R v Chehil*, 2013 SCC 49; *R v Pike*, 2024 ONCA 608; *R v Canfield*, 2020 ABCA 383.

A.2. SAAIA Lacks Adequate Limitations and Safeguards

33. Safeguards and limitations included in the SAAIA are also designed to provide the government with maximum flexibility in imposing technical surveillance capabilities. As a result, they will not provide adequate restraint on the intrusiveness or collateral cybersecurity harm that the SAAIA threatens.

34. The SAAIA includes two core restrictions. First, any obligations imposed onto an electronic service provider must be consistent with a set of criteria encoded in the proposed Act.[45] Second, a service provider can object to any action that would create a systemic vulnerability in an "electronic protection," as defined in the Act.[46] Both of these core restrictions are designed to provide the government with the maximum amount of flexibility, and thus do not provide an effective check on the breadth of the SAAIA.

A.2.i. Systemic Vulnerabilities, Cybersecurity, and Encryption

35. The SAAIA indicates that companies need not implement any obligation that would require the service provider to introduce a "systemic vulnerability" in any "electronic protection" of the specific service being targeted.[47] This limitation is vague and underinclusive, and key elements are subject to reinterpretation through regulations.

36. Ensuring the integrity of encryption systems is of absolute importance to providing a measure of cybersecurity and protection for privacy and other human rights in digital ecosystems.[48] Despite broad recognition of the importance of encryption, a wide array of techniques have been advanced over the years with the intention of bypassing or circumventing encryption.[49] Underpinning many of these proposals is the mistaken, but recurring, perception that it is possible to get around encryption without compromising its security. These recurring proposals have repeatedly been proven to be flawed,[50] but the SAAIA creates an open-ended framework by which these various proposals can nonetheless be imposed. The "systemic vulnerability" limitation proposed by the SAAIA falls far short of ensuring its broad powers will not be used to bypass encryption and undermine cybersecurity in multiple ways, a few of which are described here.

37. First, in limiting itself to "systemic" vulnerabilities, the SAAIA explicitly acknowledges that it will in fact be used to create vulnerabilities that do not meet the "systemic" threshold. The government can also redefine core operative terms that would significantly change the scope of

[45] SAAIA, ss 5(2)-(4), 7(3).

[46] SAAIA, ss 5(5) and 7(5).

[47] SAAIA, s 7(5): "The electronic service provider is not required to comply with a provision of the order, with respect to an electronic service, if compliance with that provision would require the provider to introduce a systemic vulnerability related to that service or prevent the provider from rectifying such a vulnerability." The Act defines a "systemic vulnerability" as "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." The Act defines "electronic protection" as "authentication, encryption and any other prescribed type of data protection."

[48] Lex Gill, Tamir Israel, and Christopher Parsons, "Shining a Light on the Encryption Debate: A Canadian Field Guide," Joint Research Publication, Citizen Lab & the Canadian Internet Policy & Public Interest Clinic (May 2018), online: <https://citizenlab.ca/wp-content/uploads/2018/05/Shining-A-Light-Encryption-CitLab-CIPPIC.pdf>, at pages 11-20 ("Part 2: Why Encryption Matters").

[49] *Ibid* at pages 21-38 ("Part 3: Going Dark? Four Decades of Debate").

[50] *Ibid* at pages 51-57 ("i. Exceptional Access: A Backdoor By Any Other Name?").

what constitutes a "systemic vulnerability," including what constitutes a "vulnerability," "secure information," "authentication," "encryption," or "other data protections."[51] Governments have advanced problematic and limited definitions of these concepts when seeking to justify surveillance over-reach at the cost of cybersecurity.[52] This has been specifically the case where systematic capabilities are intended to be deployed against individual targets. For example, the US FBI sought to compel Apple to create an interface that would have let the government bypass secure device encryption on every person's iPhone. This was not characterized as a "vulnerability" on the government's presumption that it will only be used on specific phones lawfully seized by police.[53]

38. The existence of this capability on its own creates a risk that it could be co-opted by bad actors. It is not enough that police intend to only use it on a case-by-case basis against specific targets. As the head of the UK's National Security Cyber Centre recently underscored, "companies that don't see cybersecurity as a priority are 'no longer just naïve,' but are 'failing to grasp the reality of today's world'."[54] With some cyber threat actors now possessing "eye-watering level[s] of sophistication,"[55] the same is also true for government agencies that still hold out hope or hubris that surveillance-driven compromises in companies' secure networks will not be exploited by commercial or state-backed threat actors.

39. Second, the safeguard only operates to protect an ESP's own services. It does not apply if an ESP is being obligated to create systemic vulnerabilities in *other providers'* electronic services, which the initial ESP can be required to do under SAAIA.[56] A free university, library, or airport WiFi network could therefore be obligated, for example, to develop the capability to install spyware on any mobile

---

[51] SAAIA, s 2(1).

[52] Lex Gill, Tamir Israel, and Christopher Parsons, "Shining a Light on the Encryption Debate: A Canadian Field Guide," Joint Research Publication, Citizen Lab & the Canadian Internet Policy & Public Interest Clinic (May 2018), online: <https://citizenlab.ca/wp-content/uploads/2018/05/Shining-A-Light-Encryption-CitLab-CIPPIC.pdf>; Bruce Schneier, "Why You Should Side with Apple, Not the FBI, in the San Bernardino iPhone Case," *Washington Post* (18 February 2026), online: <https://www.washingtonpost.com/posteverything/wp/2016/02/18/why-you-should-side-with-apple-not-the-fbi-in-the-san-bernardino-iphone-case/>; Charlie Savage, "Justice Dept Revives Push to Mandate a Way to Unlock Phones," *New York Times* (24 March 2018), online: <https://www.nytimes.com/2018/03/24/us/politics/unlock-phones-encryption.html>.

[53] Spencer Ackerman, Sam Thielman & Danny Yadron, "Apple case: judge rejects FBI request for access to drug dealer's iPhone," *Guardian* (29 February 2016), online: <https://www.theguardian.com/technology/2016/feb/29/apple-fbi-case-drug-dealer-iphone-jun-feng-san-bernardino>; Bruce Schneier, "Why You Should Side with Apple, Not the FBI, in the San Bernardino iPhone Case," *Washington Post* (18 February 2026), online: <https://www.washingtonpost.com/posteverything/wp/2016/02/18/why-you-should-side-with-apple-not-the-fbi-in-the-san-bernardino-iphone-case/>; Office of the Inspector General, "A Special Inquiry Regarding the Accuracy of FBI Statements Concerning its Capabilities to Exploit an iPhone Seized During the San Bernardino Terror Attack Investigations," Oversight and Review Division 18-03 (March 2018), online: <https://oig.justice.gov/reports/2018/o1803.pdf> [https://web.archive.org/web/20200218060830/https://oig.justice.gov/reports/2018/o1803.pdf].

[54] Mason Boycott-Owen, "UK intelligence: 100 nations have spyware that can hack Britain," *Politico* (22 April 2026), online: <https://www.politico.eu/article/u-k-intelligence-100-nations-have-spyware-that-can-hack-britain/>.

[55] *Ibid*.

[56] See e.g. SAAIA, s 7(5): "The electronic service provider is not required to comply with a provision of the order, with respect to an electronic service, if compliance with that provision would require the provider to introduce a systemic vulnerability related to that service or prevent the provider from rectifying such a vulnerability" (emphasis added). Under SAAIA, proposed ss 5(2) and 7(1), the government may "make regulations respecting the obligations" of service providers. The primary limitation on these "obligations" is that they would advance the purpose of the SAAIA, which is to "ensure that electronic service providers can facilitate the exercise of authorities to access information." There is no requirement that obligations imposed on a particular service provider will facilitate authorized access to information related to that service.

device that connects to it.[57] Police would need a court order to use this capability to install spyware on any particular target,[58] but the resulting vulnerability it creates would be in the targeted phones, not in the WiFi network, so the systemic vulnerability exception would not apply.

40. Third, the term "systemic vulnerability" only applies if the vulnerability creates a substantial risk that secure information might be accessed by "a person who does not have any right or authority to do so."[59] It therefore fails to take into account the threat that foreign intelligence and other agencies might compromise Canadian systems further to authority issued in their national law. Foreign intelligence agencies frequently target technical surveillance capabilities imposed through regimes such as that proposed by the SAAIA.[60]

41. Fourth, systemic vulnerabilities only relate to a specific set of "electronic protections," defined as "authentication, encryption and any other prescribed type of data protection." As a result, no "other data protections" are included within the scope of the term unless they are explicitly prescribed through a regulation.[61] As drafted, the "security vulnerability" limitation would therefore do nothing to mitigate deeply problematic mechanisms such as client-side scanning obligations—which amount to installing algorithmic tools on every single customer's private messaging application, to monitor content and posts that they share—because the systemic vulnerabilities these tools create are not in encryption or authentication mechanisms but in other types of data protections.[62]

42. Fifth, the systemic vulnerability mechanism has limited application in mitigating significant cybersecurity threats created by the SAAIA's mandatory data retention regime. The limitation only applies to the risk that "secure information" will be accessed by unauthorized persons. This is not responsive to the type of systemic threat that the mandatory data retention regime can pose to cybersecurity or human rights. For example, virtual private networks ("VPNs") are a critical privacy and security tool relied on by journalists, human rights defenders, political dissidents, members of vulnerable and equity-denied communities, activists resisting authoritarian repression, lawyers, and human rights and security researchers around the world.

---

[57] WiFi networks would qualify as ESPs under the proposed SAAIA and have been listed as anticipated targets of comparable surveillance capability regimes: Paul Karp, "Spies with that? Police can snoop on McDonald's and Westfield wifi customers," *Guardian* (28 May 2019), online: <https://www.theguardian.com/business/2019/may/28/spies-with-that-police-can-snoop-on-mcdonalds-and-westfield-wifi-customers>; Australia, Department of Home Affairs, "The Assistance and Access Act - An Interim Guide for: Security, Intelligence and Law Enforcement" (26 July 2019, documents released under the Freedom of Information Act 1982 (Cth), FA 19/06/00892) at page 20, online: <https://www.homeaffairs.gov.au/foi/files/2019/fa190200278-document-released.PDF> ("Examples of designated communications providers: McDonald's; Westfield or other free wifi providers").

[58] House of Commons, Standing Committee on Access to Information, Privacy and Ethics, *Study of Device Investigation Tools Used by the Royal Canadian Mounted Police (RCMP)*, Testimony of Royal Canadian Mounted Police, Dave Cobey, Technical Case Management Program, Technical Investigation Services (8 August 2022).

[59] SAAIA, s 2(1).

[60] United States, National Security Agency, "Exploiting Foreign Lawful Intercept (LI) Roundtable," TOP SECRET//SI/REL TO USA, FVEY," <https://christopher-parsons.com/wp-content/uploads/2023/01/nsa-exploiting-foreign-lawful-intercept-li-roundtable.pdf>, document published in James Bamford, "A Death in Athens," *Intercept* (28 September 2015), online: <https://theintercept.com/2015/09/28/death-athens-rogue-nsa-operation/>. For a summary, see Christopher Parsons, "Exploiting Foreign Lawful Intercept (LI) Roundtable," online: *Technology, Thoughts & Trinkets* <https://christopher-parsons.com/resources/the-sigint-summaries/nsa-summaries/#exploiting-foreign-lawful-intercept-li-roundtable>.

[61] SAAIA, proposed s 2(1), "electronic protection means authentication, encryption and any other prescribed type of data protection" (emphasis added).

[62] Hal Abelson, et al, "Bugs in our Pockets: The Risks of Client-Side Scanning," (2024) 10(1) Journal of Cybersecurity; Maxime Deryck, Diane Leblanc-Albarel, and Bart Preneel, "White-Box Attacks on PhotoDNA Perceptual Hash Function," (2026) Paper 2026/486, online: <https://eprint.iacr.org/2026/486>.

These security tools anonymize the location and identity of people including by strictly limiting what traffic data they retain. Requiring VPNs to retain traffic data regarding people using their services would fundamentally compromise the privacy and security that these tools offer, but would not render "secure information" accessible to unauthorized persons. As a result, the systemic vulnerability limitation may not be engaged, despite a systemic vulnerability being, in fact, introduced.

A.2.ii. Necessity and Proportionality

43. In addition to the systemic vulnerability limitation, the SAAIA also includes a number of factors that need to be considered when its powers are exercised.[63] As with nearly all other elements of Bill C-22, these factors appear designed to give the government the maximum amount of flexibility in justifying whatever surveillance requirements it wishes to put in place. The standards are therefore deficient in a number of ways.

44. First, the factors in question must consider the impact of each specific obligation imposed rather than of the regulation or order itself. As currently framed, a harm created by a specific obligation might be justified by reference to benefits anticipated from another obligation packaged in the same regulation or order.

45. Second, the factors fail to take into account the wide-ranging collateral harms the SAAIA threatens. The government need only consider the negative impacts of obligations to users of the specific electronic service being targeted rather than the broader harms to society or to users of other electronic services.[64]

46. Third, the SAAIA fails to impose an objective standard that the government must meet to issue the order in question rather than simply requiring the government to "take [them] into account."[65] Powers under the SAAIA should only be exercised if the government is able to demonstrate reasonable grounds to believe that every factor is established.[66] Reasonable grounds to believe is a well-established objective standard that is used throughout the *Criminal Code*, the *CSIS Act*, and the *CSE Act*, including where decision-makers are required to consider competing factors.

47. Fourth, SAAIA only requires that the factors be considered at the time an order or regulation is issued. There is no obligation to consider their applicability on an ongoing basis or when imposing specific conditions onto a specific electronic service provider through a compliance order.[67] Nor does the SAAIA require additional review once an obligation is authorized,

---

[63] SAAIA, s 5(3) (the factors are: benefits to the administration of justice; feasibility of compliance for core providers; costs incurred by core providers; potential impact on providers' users; potential impact on privacy protection and cybersecurity; and "any other factor" considered relevant).

[64] SAAIA, ss 5(3)(d) and 7(3)(d).

[65] SAAIA, at s 5(3) and 7(3).

[66] *Hunter v Southam*, [1984] 2 SCR 145 at 167-168 ("History has confirmed the appropriateness of this requirement as the threshold for subordinating the expectation of privacy to the needs of law enforcement"); *R v TELUS Communications Inc*, 2013 SCC 16 at paras 19, 55-56 (regarding the need for strict application of threshold conditions for authorization).

[67] By contrast, under the Australian regime, all technical capability notices must include an expiry date and no order can be issued for longer than 1 year (that is to say, the order itself lasts for one year, distinguished from the duration of data retention required by the order), and must then be reissued (and, by extension, reassessed): Australia, *Telecommunications and Other Legislation*

providing no scrutiny mechanism if the original circumstances under which the order or regulation was issued have changed.

48. Fifth, the factors as formulated fail to impose a clear justification framework, relying instead on an open-ended list of criteria. A clear justification framework would prohibit any obligation from being imposed unless the government can demonstrably establish there are reasonable grounds to believe that:

    a. the obligation in question is strictly necessary to the investigation of a serious offence as defined in section 467.1(1) of the *Criminal Code* or to the security of Canada as defined in s. 2 of the *CSIS Act* and cannot be achieved by less intrusive means;[68]
    b. any potential impact including specifically to cybersecurity and to the right to privacy is demonstrably proportionate to the objectives of the obligation;
    c. it is demonstrably feasible for all impacted electronic service providers to comply with the obligation and that the costs to be incurred by electronic service providers or the government are proportionate to the objectives of the obligation; and
    d. the obligation in question does not require an ESP to do anything that can be accomplished through an existing power.[69]

    The list of factors should be closed (i.e., should not include any other factor that the government may wish to consider). We **recommend** the above justification framework replace the current list of considerations in sections 5(3) and 7(3) of SAAIA.

49. SAAIA also lacks the following explicit limits on the obligations that can be imposed on ESPs, which we consider necessary to add. These limits are critical, but if implemented selectively or piecemeal, will fail to remedy the overarching problems arising from SAAIA's overbreadth (as discussed in Part A.1 above). Specifically, we **recommend** adding the following safeguards to the Act:

    a. Narrow the definition of "electronic service provider" to only mean telecommunications carriers;
    b. Limit the application of SAAIA so that it can only obligate telecommunications carriers to develop wiretapping capabilities and clarify that these rules cannot require a "specific design of equipment, facilities, services, features or system configurations";[70]

Amendment (Assistance and Access) Act 2018, No. 148, 2018, sections 317TA(1A)("An expiry date specified in a technical capability notice must not be later than 12 months after the notice was given.").

[68] See, for example, Australia, *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*, No. 148, 2018, section 317T: "Technical Capability Notices … (2) The specified acts or things must: … be directed towards ensuring that the designated communications provider is capable of giving listed help…in relation to … a relevant objective. (3) For the purposes of this section, relevant objective means: (a) enforcing the criminal law, so far as it relates to serious Australian offences; or (b) assisting the enforcement of the criminal laws in force in a foreign country, so far as those laws relate to serious foreign offences; or (c) safeguarding national security."

[69] Australia, *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*, No. 148, 2018, s 317ZH (a technical capability notice cannot require a service provider to do anything that would otherwise require a warrant); *Criminal Code*, RSC , s 4887.01(c): "there is no other provision in this or any other Act of Parliament that would provide for a warrant, authorization or order permitting the technique, procedure or device to be used or the thing to be done." See also: *R v TELUS Communications Inc*, 2013 SCC 16 at para 81.

[70] Communications Assistance for Law Enforcement Act (CALEA), encoded at 47 USC 1002(b)(1): "This subchapter does not authorize any law enforcement agency or officer—(A) to require any specific design of equipment, facilities, services, features, or system configurations to be adopted by any provider of a wire or electronic communication service, any manufacturer of telecommunications equipment, or any provider of telecommunications support services; or (B) to prohibit the adoption of any equipment, facility, service, or feature by any provider of a wire or electronic communication service, any manufacturer of telecommunications equipment, or any provider of telecommunications support services.

c. Add the following provision to ss 5 and 7 of SAAIA: "No order or regulation shall be made that would have the effect of degrading, removing, defeating or bypassing any technical safeguard including encryption";
d. Limit the ability of the government to redefine key terms in this limitation through regulations (s. 47(1)(c));
e. Require regulations (s. 5) and orders (s. 7) expire after one year;
f. Remove the data retention regime because any indiscriminate retention or preservation is unconstitutional. Alternatively:
    i. limit it to preservation of data already under a service provider's control for 30 days;
    ii. limit the application of the regime to telecommunications carriers;
    iii. specify what categories of data can be required to be preserved in the text of the statute; and
    iv. ensure that these exclude any type of tracking data as defined in s. 487.011 of the *Criminal Code*, with the possible exception of requiring telecommunications carriers to preserve cell tower interaction records;
g. Prohibit companies from using or disclosing mandatorily retained or preserved data for any reason other than responding to state requests that relate to investigations of serious offences or to activities that threaten the security of Canada;
h. Require companies to delete retained or preserved information once the retention or preservation window closes unless a preservation order is issued under the *Criminal Code*;
i. Limit obligations imposed through the SAAIA to an ESP's own services; and
j. Add a provision to the SAAIA establishing that ESPs cannot be compelled to deceive or mislead their customers or the public.[71]

A.3. Lack of Judicial Authorization & Control

50. Courts are the primary vehicle for authorizing most surveillance activities carried out by CSIS and the police. Yet under the SAAIA, obligations that dwarf most powers in the *Criminal Code* in terms of intrusiveness can be imposed without judicial authorization or appeal. The primary vehicle of independent oversight and input in the SAAIA is through judicial or quasi-judicial review only. This is particularly problematic in light of the potential prohibitions of disclosure that an order has been issued, setting up a regime of secrecy. The result is a national surveillance system that might far outstrip current legal regimes in both scope and intrusiveness, and that relies on an oversight framework created for the extra-ordinary foreign intelligence context rather than for domestic policing.

51. For example, police currently require judicial authorization to compel a company to preserve personal information they already have regarding a specific person for 90 days.[72] By contrast, under the SAAIA, police will be able to force the same company to keep the same information on every single customer for up to a full year without judicial authorization. Similarly, under the

[71] Australia, *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*, No. 148, 2018, s 317E(2): "Paragraph (1)(j) does not apply to: (a) making a false or misleading statement; or (b) engaging in dishonest conduct."

[72] *Criminal Code*, RSC 1985, c C-46, s 487.013. Similarly, if CSIS wishes to retain personal data of people in Canada already under its control but which is not directly and immediately related to activities that represent a threat to the security of Canada, it must obtain judicial authorization from the Federal Court: *Canadian Security Intelligence Service Act (Re)*, 2022 FC 645 at paras 9-19.

Criminal Code, police require a general warrant to install spyware on a specific target's mobile device. By contrast, under the SAAIA, companies such as Apple and Google might be compelled to create an interface providing police with direct access to mobile devices running on iOS or Android. While either situation requires additional judicial approval (an authorization under Part VI of the *Criminal Code*) to use the installed capability in order to intercept private communications,[73] SAAIA would nevertheless bypass the existing general warrant requirement for the initial installation of the spyware on people's mobile devices.

52. The primary vehicle for independent scrutiny proposed in the SAAIA is judicial review. Regulations issued under section 5 by the Governor in Council and compliance orders issued by a designated person under section 24 can be judicially reviewed before the Courts.[74] Orders issued by the Minister of Public Safety under section 7 must be quasi-judicially reviewed by the Intelligence Commissioner before coming into effect.[75]

53. Judicial review is no substitute for independent authorization or full appellate review of SAAIA requirements. In judicial review, an independent entity assesses whether the decision-maker (in this instance, the Minister, the Governor in Council, or a designated person) was reasonable in making its decision based on the evidence that was before them at the time rather than whether the decision is in fact correct.[76] Because the focus of the judicial review inquiry is on the initial decision, the review is highly deferential and, moreover, any evidence that was not before the initial decision-maker is generally inadmissible.[77] By contrast, when a court authorizes police or CSIS surveillance activity, the government makes its case to the court but the actual weighing of competing factors is conducted by an independent decision-maker.[78] Challenges of *ex parte* judicial authorizations and even appeals of those challenges are conducted with heavier scrutiny

---

[73] House of Commons, Standing Committee on Access to Information, Privacy and Ethics, *Study of Device Investigation Tools Used by the Royal Canadian Mounted Police (RCMP)*, Testimony of Royal Canadian Mounted Police, Dave Cobey, Technical Case Management Program, Technical Investigation Services (8 August 2022).

[74] SAAIA, s 17.

[75] "The [*Intelligence Commissioner Act*] requires the Intelligence Commissioner to review whether the Minister's conclusions are reasonable. I will therefore apply the reasonableness standard, as applied in judicial reviews of administrative action": CSE-2025-09, Intelligence Commissioner Decision and Reasons in relation to a Cybersecurity Authorization for Activities on Non-federal Infrastructures pursuant to subsection 27(2) of the *Communications Security Establishment Act* and section 14 of the *Intelligence Commissioner Act*, date redacted.

[76] *Canada (Minister of Citizenship and Immigration) v. Vavilov*, 2019 SCC 6; *Canada (Attorney General) v Canadian Civil Liberties Association*, 2026 FCA 6, leave to appeal sought, SCC File No 42261; and CSE-2025-09, Intelligence Commissioner Decision and Reasons in relation to a Cybersecurity Authorization for Activities on Non-federal Infrastructures pursuant to subsection 27(2) of the *Communications Security Establishment Act* and section 14 of the *Intelligence Commissioner Act*, date redacted. Note that "quasi-judicial review" is functionally the same as judicial review, but conducted by an independent quasi-judicial tribunal rather than by a court: *Spasoja v Canada (Citizenship and Immigration)*, 2014 FC 913, in general and at paras 27-32 in particular. See also: *Parizeau c Barreau du Québec*, 2011 QCCA 1498.

[77] *Canada (Attorney General) v Canadian Civil Liberties Association*, 2026 FCA 6, leave to appeal sought, SCC File No 42261 at paras 62 and 140: "As for admissibility, evidence that was not before the decision-maker at the time of its decision is generally inadmissible." For the purpose of an order-in-council issued under section 5 of the *SAAIA*, the relevant decision-maker would be Cabinet and for the purpose of a ministerial order issued under section 7 of the proposed SAAIA (2026 FCA 6 at para 130), the relevant decision maker would be the Minister of Public Safety. Note that with respect to section 5 orders, there is a risk that important information may be further shielded from consideration due to cabinet confidence (2026 FCA 6 at at para 129).

[78] *Hunter et al v Southam Inc*, [1984] 2 SCR 145 at pages 161-165 ("B) Who Must Grant the Authorization?") (Ministers are not typically capable of "acting judicially" to meet the requirement for independent authorization of a search or seizure under section 8 of the *Charter*). Warrantless searches or seizures are presumptively unreasonable under section 8: *R v Duarte* [1990] 1 SCR 30; *R v Spencer*, 2014 SCC 43 at para 68; *R v Vu*, 2013 SCC 60.

than judicial review.[79] As a result, the SAAIA lacks independent judicial authorization or an effective appeal mechanism. Nor can the availability of judicial review be considered a "safeguard" for the purpose of assessing the SAAIA's constitutionality.[80] Ultimately, the SAAIA lacks effective judicial control.

54. Under section 8 of the *Charter*, any search or seizure that interferes with a reasonable expectation of privacy in the absence of judicial authorization is presumptively unreasonable.[81] Under the SAAIA, companies will be compelled to significantly expand their access to and retention of sensitive personal information with the explicit purpose of making that information available to the state upon request.[82] Section 8 is clearly engaged and, as a result, the absence of judicial authorization and control is a constitutional defect.

55. Heavy reliance on judicial review is particularly problematic in light of the nature of the inquiry the SAAIA requires and the secrecy with which many obligations will be imposed. As described above, the SAAIA relies on the government's balancing of a list of considerations.[83] This type of open-ended balancing exercise is highly immunized from scrutiny through a judicial review process that is limited to assessing whether the decision-maker acted reasonably or not.

56. Many SAAIA obligations will also be imposed in secret and without any input from relevant stakeholders, or will simply lack sufficient public-facing details to support a judicial review challenge before the courts. This is because SAAIA relies heavily on an oversight framework designed for the foreign intelligence context, so many of the decisions and reports relied upon as transparency mechanisms will be opaque (for instance, through vague descriptions and redactions). This opacity is compounded by the SAAIA's blanket restriction on any public discussion by ESPs regarding obligations they are facing, which builds in an additional layer of expansive secrecy.[84] While there will always be some details relating to these capabilities that cannot be made public, broad stakeholder engagement and detailed public descriptions should be the default, subject to confidentiality requirements only where these are strictly necessary to avoid compromising investigative techniques.

---

[79] *R v Garofoli*, [1990] 2 SCR 1421 (when challenging an authorization in court, defendant may cross-examine); *R v Araujo*, 2000 SCC 65 at para 40 (questions of fact); *R v Vu*, 2013 SCC 60 at paras 12-18.

[80] *Canadian Council for Refugees v. Canada (Citizenship and Immigration)*, 2023 SCC 17 at para 77: "The general availability of judicial review therefore cannot save otherwise unconstitutional legislation. For this reason, I consider it unhelpful to view judicial review as a form of 'safety valve' or statutory safeguard." See also Australia, Parliamentary Joint Committee on Human Rights, Human Rights Scrutiny Report (4 December 2018) at paras 2.178-2.181, online (PDF): <https://www.aph.gov.au/-/media/Committees/Senate/committee/humanrights_ctte/reports/2018/Report_13/Report_13_of_2018.pdf>: "Questions therefore arose in the context of the current bill insofar as the power to give a technical assistance notice or request, or technical capability notice, is not exercised by a judge, nor does a judge supervise its application. … Therefore, in terms of ensuring the impact on individual rights is proportionate for the purposes of international human rights law, the availability of judicial review for providers does not appear to be an adequate safeguard"; see also Australian Government, Independent National Security Legislation Monitor, Dr James Renwick, "Trust but Verify: A report concerning the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* and related matters" (2020) 3rd INSLM, 9th Report, at page 15: "A key safeguard in Schedule 1 is the general limitation that TANs and TCNs must be reasonable and proportionate. … But those factors should be weighed up by someone independent of the Government or the agency. That should also be so when determining whether complying with the notice is not 'practicable', not 'technically feasible', or would create a 'systemic weakness' or 'systemic vulnerability'."

[81] *Hunter v Southam Inc*, [1984] 2 SCR 145.

[82] SAAIA, ss 5(2)(d) and (7(2).

[83] See discussion in Part A.2.ii above.

[84] SAAIA, s 15.

57. We therefore **recommend**:

    a. Requiring authorization by the Federal Court as a precondition for the issuance of any regulation, order, or compliance order under the SAAIA and encoding a full right to *de novo* review before the federal court for any relevant stakeholder;
    b. Amending s. 15 of SAAIA so that information may be kept confidential only to the extent it is demonstrably necessary to preserving the integrity of an investigative technique; and
    c. Requiring public notification of all orders at least 30 days before they come into effect.

B. Constitutional Protection of "Publicly Available Information"

58. Clause 11 of Bill C-22 amends section 487.0195 of the *Criminal Code* to state expressly that "no production order or warrant, or confirmation of service demand... is necessary for a peace officer or public officer to receive, obtain and act on any information that is available to the public."[85] The associated heading is "Publicly available information." As currently drafted, this provision creates a framework that flies in the face of decades of Supreme Court of Canada jurisprudence recognizing that public information is not categorically exempt from section 8 protection. It would strip untold volumes and ranges of sensitive data of constitutional protection from warrantless searches by law enforcement, even where individuals retain a reasonable expectation of privacy in that data.

59. Moreover, it is unclear why this provision is necessary. Where publicly available information is *not* subject to a reasonable expectation of privacy, longstanding police powers already exist; the addition of this provision thus only causes needless confusion. Law enforcement may already gather public information while executing policing duties, if the act of gathering that information does not interfere with *Charter* interests such as privacy, equality, or civil liberties, nor violates statutory privacy laws. Conversely, where publicly available information *is* subject to a reasonable expectation of privacy, the proposed s. 487.0195(4) would be unconstitutional under s. 8 of the *Charter*, due to being a warrantless power, and therefore presumptively unreasonable.

60. Worse than unnecessary, the provision is misleading. The phrase "for greater certainty" is meant to indicate that the legislation simply codifies the existing state of the law.[86] That could not be further from the truth, as the subsections below will explain. If this amendment in Bill C-22 is enacted as drafted, it would represent a quietly deceptive upending of a foundational pillar of Canadian constitutional privacy law.

61. For these and other reasons detailed below, we **recommend** that the amendment concerning "information available to the public" or "publicly available information" ("PAI"), which we will treat as interchangeable concepts herein, be removed from the bill. Failing that, we **recommend** adding language expressly clarifying that PAI, for the purposes of Bill C-22, does not include information in which there is a reasonable expectation of privacy; personal information that has been unlawfully collected or disclosed; nor commercially available information ("CAI"). Each of these categories are discussed in greater detail below. This section concludes with a discussion of how the PAI provision in Bill C-22 could interact with other privacy law regimes (e.g., private sector privacy law) to drastically undermine both constitutional privacy and consumer data privacy rights in Canada.

[85] Bill C-22, cl 11, s 487.0195(4).

[86] *R v Spencer*, 2014 SCC 43 at para 73.

B.1. Reasonable Expectation of Privacy in Public

62. The Bill C-22 *Charter* statement suggests that the government justifies the PAI provision and lack of definition with the notion, "Where information is available to the public, a person will usually have no reasonable expectation of privacy in it."[87] This betrays a paucity of understanding of the relevant law in Canada, where it is well settled that reasonable expectation of privacy does inhere in many kinds of information that may be considered publicly available, and a person's reasonable expectation of privacy is not negated by the mere fact that they or their information appear in public.[88]

63. The PAI provision as drafted conflicts with bedrock principles in Canadian constitutional law, as far as reasonable expectations of privacy are concerned. Whether there is such reasonable expectation depends on the "totality of the circumstances," where public availability is only one of many relevant factors in a context-sensitive and normative analysis.[89] Bill C-22 treats public availability as the sole determinative factor, disregarding both context and the required normative approach.

64. The provision also treats privacy as an all-or-nothing concept, despite repeated rulings to the contrary by the Supreme Court of Canada: "being in a public or semi-public space does not automatically negate all expectations of privacy with respect to observation or recording."[90] As Justice La Forest noted, quoting US legal scholar Melvin Gutterman, "In a variety of public contexts, we may expect to be casually observed, but may justifiably be outraged by intensive scrutiny. In these public acts we do not expect to be personally identified and subject to extensive surveillance, but seek to merge into the 'situational landscape'."[91] Deeming all PAI automatically searchable and seizable without a warrant destroys the very premise of such a landscape, and with it the notion of privacy as anonymity, which the Supreme Court has recognized is one of the core components of the right to privacy protected by section 8 of the *Charter*.[92]

65. Lastly, the proposed legislation would embed the prohibited "risk analysis" approach to privacy, which "reduc[es] the inquiry to whether the person put themselves at risk of the intrusion they experienced."[93] As the current PAI provision stands, any person in Canada relinquishes their right to be protected from unreasonable search by the state of their personal information the moment they step foot outside onto public streets, or participate in society in an online public space. Police conduct carried out in reliance on the proposed framework in the bill would likely not withstand constitutional scrutiny in the courts.

---

[87] "Bill C-22: An Act respecting lawful access" (Charter Statement) (24 April 2026), online: *Department of Justice Canada* <https://www.justice.gc.ca/eng/csj-sjc/pl/charter-charte/c22_2.html>.

[88] *R v Jarvis*, 2019 SCC 10 at para 41; *R v Wong*, [1990] 3 SCR 36 at page 62 (Lamer J, concurring); *R v Wise*, [1992] 1 SCR 527, 1992 CanLII 125 (SCC) at pages 40-42 (La Forest J, dissenting).

[89] *R v Tessling*, 2004 SCC 67 at paras 19, 42; *R v Cole*, [2012] 3 SCR 34 at paras 39-40; *R v Jarvis*, 2019 SCC 10, at paras 60, 68.

[90] *R v Jarvis*, 2019 SCC 10, at para 61; see also *R v Jones*, 2017 SCC 60 at para 41.

[91] *R v Wise*, [1992] 1 SCR 527, 1992 CanLII 125 (SCC) at page 41.

[92] *R v Spencer*, 2014 SCC 43 at paras 41-45.

[93] *R v Jarvis*, 2019 SCC 10 at para 64; see also *R v Marakah*, 2017 SCC 59 at para 68; and *R v Duarte*, [1990] 1 SCR 30 at page 48.

66. Deeming all PAI as automatically legally subject to warrantless search carries especially troubling implications in light of the myriad ways that personal information is mass collected and routinely disclosed through the proliferation of digital technologies and industries such as AI-based surveillance tools, social media platforms, data brokers, algorithmic profiling, and law-enforcement-oriented commercial surveillance vendors. All of these tools and systems are designed to maximally collect, use, and disclose personal information that is in public view (whether virtual or physical), much of which would be considered information to which a reasonable expectation of privacy still attaches. This includes, for example, biometrics information based on one's face, voice, or walking gait;[94] location data, often revealing one's daily routines;[95] potential medical conditions, behavioural patterns, or psychological state inferred from social media activity;[96] genetic genealogical information,[97] or the contents of personal conversations held in public spaces.[98]

67. The Supreme Court of Canada has noted:

> 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.... Aggregation "creates synergies. When analyzed, aggregated information can reveal new facts about a person that she did not expect would be known about her when the original, isolated data was collected" ... The ubiquity of the Internet means we must increasingly consider "the ways in which different data sets in combination with other data sets affect privacy rights."... Not only does the Internet keep an accurate permanent record, it has concentrated this mass of data in the hands of third parties, investing these third parties with immense informational power. It has given large private corporations the ability to collect vast stores of user information and to aggregate that data into sharp images of their users' online activity....[99]

The Court's observations apply with even greater force when one combines with the Internet the further accumulative drive and intrusiveness of technologies advertised under the banner of "AI."[100] One's personal information either being necessarily PAI as a condition of participating in today's digitized society, or turned into PAI without one's knowledge or consent, is increasingly becoming the general rule of modern life, rather than an exception that may be relied upon as a

---

[94] Office of the Privacy Commissioner of Canada, "Guidance for processing biometrics – for federal institutions" (2025), online: <https://www.priv.gc.ca/en/privacy-topics/health-genetic-and-other-body-information/biometrics/gd_bio _fed-final/>.

[95] Office of the Privacy Commissioner of Canada, *Joint investigation into location tracking by the Tim Hortons App*, PIPIEDA Findings #2022-001 (1 June 2022), online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2022/pipeda-2022-001/>.

[96] *R v Bykovets*, 2024 SCC 6 at paras 76-77.

[97] Kate Robertson, "Investigative Genealogy and the *Charter*: Consent, the Immutability of DNA, and Canada's Arriving Future," (2025) 73(4) CLQ 471.

[98] Momin Qureshi, "Toronto police won't implement controversial ShotSpotter tech," *CityNews* (14 February 2019), online: <https://toronto.citynews.ca/2019/02/14/toronto-police-shotspotter/>.

[99] *R v Bykovets*, 2024 SCC 6 at paras 73-75 (citations omitted).

[100] See e.g. Meredith Whittaker, "AI agents are coming for your privacy, warns Meredith Whittaker," *Economist* (9 September 2025), online: <https://www.economist.com/by-invitation/2025/09/09/ai-agents-are-coming-for-your-privacy- warns-meredith-whittaker>; Joe Wilkins, "Millions of Private ChatGPT Conversations Are Being Harvested and Sold for Profit," *Futurism* (18 December 2025), online: <https://futurism.com/artificial-intelligence/ai-chatbot-data-scraping>; and Jay Stanley, "Machine Surveillance is Being Super-Charged by Large AI Models" (21 March 2025), online: *ACLU* <https://www.aclu.org/news/privacy-technology/machine-surveillance-is-being-super-charged-by-large-ai-models>.

coarse proxy for the presence or absence of a reasonable expectation of privacy. This makes it all the more crucial that the bill not presumptively create a framework premised on the notion that PAI lacks constitutional protection as a foregone conclusion.[101]

B.2. Unlawful Collection or Disclosure of Personal Information

68. The current reference to PAI in Bill C-22 also does not account for personal information that has become public through unlawful means, or which was originally collected unlawfully before being disclosed. The history of the Internet's role in society has doubled as an unfortunately rich history of consequential data breaches. Prominent examples include: the data breach of the Canvas instructional platform, affecting millions of post-secondary students including in Canada;[102] the exposure of 70,000 Discord users' government identification photos and other personal information, by hackers of a third-party age-verification company the platform used;[103] an Alberta separatist group leaking the personal information of millions of voters in the province;[104] and unauthorized access to 143 million people's personal information after Equifax was subjected to a cybersecurity attack, including Canadian social insurance numbers.[105] The constitutional right to privacy should not be made dependent on the operations and information security practices and competence of any given company or institution.

69. As for illegal collection, the Citizen Lab and CIPPIC noted in an analysis of legislation proposed in 2017, Bill C-59, *An Act respecting national security matters*, that "it is well documented that many of the companies that accumulate [personal] data for commercial or even noncommercial distribution are not operating in compliance with Canadian data protection laws."[106] One does not have to strain to find particularly salient examples from recent years in joint investigations completed by Canada's federal and provincial privacy commissioners, all of which concluded with findings of illegal activity by the entity in question. These include the facial recognition company Clearview AI;[107] the social

---

[101] "While evolving technologies may make it easier, as a matter of fact, for state agents or private individuals to glean, store and disseminate information about us, this does not necessarily mean that our reasonable expectations of privacy will correspondingly shrink." *R v Jarvis*, 2019 SCC 10 at para 63.

[102] Jessica Wong, "A cyberattack hit universities worldwide, including top Canadian schools. Here's what we know," *CBC* (9 May 2026), online: <https://www.cbc.ca/news/canada/canvas-cyber-attack-canadian-universities-9.7193648>.

[103] Robert Booth, "Hack of age verification firm may have exposed 70,000 Discord users' ID photos," *Guardian* (9 October 2025), online: <https://www.theguardian.com/media/2025/oct/09/hack-age-verification-firm-discord-users-id-photos>.

[104] Jack Farrell & Lisa Johnson, "Scope of how many people accessed leaked voter list may be incomplete: Elections Alberta," *Global News* (13 May 2026), online: <https://globalnews.ca/news/11848082/elections-alberta-the-centurion-project-access-list/>.

[105] Office of the Privacy Commissioner of Canada, *Investigation into Equifax Inc. and Equifax Canada Co.'s compliance with PIPEDA in light of the 2017 breach of personal information*, PIPEDA Findings #2019-001 (9 April 2019), online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2019/pipeda-2019-001/>.

[106] Lex Gill, Tamir Israel, Bill Robinson & Ronald Deibert, "Analysis of the *Communications Security Establishment Act* and Related Provisions in Bill C-59 (*An Act respecting national security matters*), First Reading (December 18, 2017)," Joint Report by the Citizen Lab and Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC) (December 2017) at page 53, online (PDF): <https://citizenlab.ca/wp-content/uploads/2017/12/C-59-Analysis-1.0.pdf>.

[107] Office of the Privacy Commissioner of Canada, *Joint investigation of Clearview AI, Inc*, PIPEDA Findings #2021-001 (2 February 2021), online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001>.

media platform TikTok;[108] the AI company and operator of ChatGPT, OpenAI;[109] the network of pornography platforms by Aylo (formerly Mindgeek);[110] and the national coffee chain, Tim Hortons.[111] Designating personal information that became public by way of illegal and violative business practices as "publicly available" for the purpose of warrantless state search would represent compounding injustices, effectively adding a constitutional injury on top of the one already given by the private sector, *because* one was injured by the private sector.

B.3. Commercially Available Information

70. For similar reasons as those applying to unlawfully collected or disclosed personal information, under no circumstances should PAI be defined to include commercially available information ("CAI"). We rely on the following definition of CAI:

> [CAI is] information that is available commercially, through a commercial transaction with another party. The acquisition may occur on a one-time or subscription basis, and may involve the [state actor] directly ingesting the CAI or obtaining a license agreement that affords a continuing right of access. CAI typically is acquired for a fee, but … also includes information offered at no cost if it is the type of information that is normally offered for sale – e.g., a free trial offering of CAI.[112]

Further, CAI may include, but is not limited to, data or services sold exclusively to law enforcement or other government actors. In fact, the more pertinent subset of CAI may be found in the growing field of data brokers, surveillance vendors, and other personal-data-reliant companies—many operating in legal grey areas at best, or in outright defiance of applicable laws—

[108] Office of the Privacy Commissioner of Canada, *Joint investigation of TikTok Pte Ltd*, PIPEDA Findings #2025-003 (23 September 2025), online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2025/pipeda-2025-003/>.

[109] Office of the Privacy Commissioner of Canada, *Joint Investigation of OpenAI OpCo, LLC*, PIPEDA Findings #2026-002 (6 May 2026) online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/ investigations-into-businesses/2026/pipeda-2026-002/>.

[110] Office of the Privacy Commissioner of Canada, *Investigation into Aylo (formerly MindGeek)'s Compliance with PIPEDA*, PIPEDA Findings #2024-001 (29 February 2024), online: <https://www.priv.gc.ca/en/opc-actions-and-decisions /investigations/investigations-into-businesses/2024/pipeda-2024-001/>

[111] Office of the Privacy Commissioner of Canada, *Joint investigation into location tracking by the Tim Hortons App*, PIPIEDA Findings #2022-001 (1 June 2022), online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations /investigations-into-businesses/2022/pipeda-2022-001/>.

[112] Senior Advisory Group Panel on Commercially Available Information, "Report to the Director of National Intelligence" (27 January 2022) at page 11 (emphasis omitted), online: *US Office of the Director of National Intelligence* <https://www.dni.gov/files/ODNI/documents/assessments/ODNI-Declassified-Report-on-CAI-January2022.pdf>.

offering their services and datasets to the general public, whether on an individual basis,[113] at the enterprise level,[114] or simply to anyone who can pay.[115]

71. Canadian law enforcement agencies have shown that they have no qualms purchasing or otherwise obtaining access to CAI in the course of their work, in ways later determined to be in violation of Canadian privacy law.[116] Even worse, some members of law enforcement use their access to such tools to engage in forms of intimate partner abuse or other technology-facilitated gender-based violence.[117] Governments' demonstrated inability to restrain or prevent this kind of endemic misconduct suggests that such abuses will only increase alongside law enforcement's access to increased surveillance powers.

72. At a fundamental level, considering CAI to be non-protected PAI amounts to enabling state actors to buy their way out of having to respect the Constitution, representing an end-run around section 8 of the *Charter*. This point has been made with particular starkness in the United States, where there is not even the minimum protection of a federal consumer privacy law, with one historical legislative attempt to close this loophole entitled the "Fourth Amendment Is Not For Sale Act."[118] Likewise, constitutional privacy rights in Canada are not a commodity to be bought and sold.

73. An additional pressing concern with including CAI in the definition of PAI is that of building perverse incentives into government and the law. The Citizen Lab and CIPPIC wrote nine years ago:

> [T]here is also a risk that [including CAI in PAI for the purpose of warrantless search by CSE] will signal to these private sector actors that the Canadian government is in

---

[113] See e.g. Cynthia Khoo, Kate Robertson & Ron Deibert "Installing Fear: A Canadian Legal and Policy Analysis of Using, Developing, and Selling Smartphone Spyware and Stalkerware Applications" (June 2019), online: *Citizen Lab* <https://citizenlab.ca/research/installing-fear-a-canadian-legal-and-policy-analysis-of-using-developing-and-selling-smartphone-spyware-and-stalkerware-applications/>; and Lorenzo Franceschi-Bicchierai, "Hacked, leaked, exposed: Why you should never use stalkerware apps," TechCrunch (9 February 2026), online: <https://techcrunch.com/2026/02/09/hacked-leaked-exposed-why-you-should-stop-using-stalkerware-apps/>.

[114] See e.g. Adam Molnar, "Surveillance and Algorithmic Management at Work: Capabilities, Trends, and Legal Implications" (March 2025), online: *Information and Privacy Commissioner of Ontario* <https://www.ipc.on.ca/en/resources/research-hub/surveillance-and-algorithmic-management-at-work>; and Coworker.org, "Little Tech Goes Global: The Expansion of AI and Workplace Surveillance" (June 2025), online: <https://home.coworker.org/little-tech-goes-global/>.

[115] See e.g. Joseph Cox, "This Company Built a Private Surveillance Network. We Tracked Someone With It," *Vice Motherboard* (17 September 2019), online: <https://www.vice.com/en/article/i-tracked-someone-with-license-plate-readers-drn/>.

[116] See e.g. Office of the Privacy Commissioner of Canada, *Joint investigation of Clearview AI, Inc*, PIPEDA Findings #2021-001 (2 February 2021), online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/>; and Office of the Privacy Commissioner of Canada, *Investigation of the RCMP's collection of open-source information under Project Wide Awake* (Special report to Parliament) (15 February 2024), online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/202324/sr_pa_20240215_rcmp-pwa/>.

[117] See e.g. Alexander Quon, "Regina officer charged with violating privacy act by snooping in police database 67 times," *CBC News* (14 May 2026), online: <https://www.cbc.ca/news/canada/saskatchewan/clinton-duquette-charged-privacy-9.7200310>; Christopher Ingraham, "Police Have Reportedly Used License Plate Readers to Stalk Romantic Interests at Least 16 Times in Recent Years" (27 April 2026), online: *Institute for Justice* <https://ij.org/police-have-reportedly-used-license-plate-readers-to-stalk-romantic-interests-at-least-14-times-in-recent-years/>; and Joint Submission by Citizen Lab and Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC), "Submission to the UN Special Rapporteur on Violence Against Women, its Causes, and Consequences" (3 November 2017) at page 5, online: <https://citizenlab.ca/submission-un-special-rapporteur-violence-women-causes-consequences/>.

[118] US, Bill HR 4639, *Fourth Amendment Is Not For Sale Act*, 118th Cong, 2023; see also Emile Ayoub & Elizabeth Goitein, "Closing the Data Broker Loophole" (13 February 2024), online: *Brennan Center for Justice* <https://www.brennancenter.org/our-work/research-reports/closing-data-broker-loophole> .

> the market for new kinds of information about Canadians and persons in Canada. These companies—which are already heavily invested in sophisticated methods, sources, and technologies relating to the collection, aggregation and analysis of personal information—could be incentivized to create and collect forms of Canadian data that they would have never previously sought to capture or exploit, but that that could be of particular interest to the CSE [or other law enforcement agencies]. Growing demand from a well-funded agency such as the CSE [or RCMP] for commercial available Canadian data could send a signal—including to criminal groups—that it is in the market for such information, however acquired.[119]

74. The Canadian government and privacy commissioners already struggle to hold major technology companies to account, as well as protect vulnerable individuals and the general public from harms arising from the unlawful or unethical collection, use, and disclosure of their personal data.[120] Meanwhile, the Canadian public has been long awaiting updates to the *Personal Information Protection and Electronic Documents Act* ("PIPEDA"), so that they are better protected against increasingly brazen private sector privacy violations, and has also been clamouring for long overdue legislation to regulate, hold liable, and provide protections from freewheeling AI companies, who also play fast and loose with personal data.[121] Against this backdrop, it is unfathomable that the federal government is proposing to set up a legal regime where one or more arms of the government itself would, indirectly, incentivize or benefit from such companies continuing their privacy-invasive practices and business models.

B.4. Interaction with Other Regimes in Canadian Privacy Law

75. The dramatic expansion of non-protected PAI in Bill C-22, for the purpose of warrantless search and seizure, is also misaligned with and would introduce confusion and destabilization in Canadian privacy law regimes governing the private sector and public agencies outside of law enforcement. Where these privacy laws address PAI, its definition has been developed through years of interpretation and guidance from privacy commissioners and the courts, with a view to protecting privacy rights in the context of commercial practices and government operations, respectively. The proposed provision in Bill C-22 could prompt a weakening of privacy protection for personal information across the board, where it is considered PAI. This weakening would moreover occur in an era where both technology companies and Canadian law

---

[119] Lex Gill, Tamir Israel, Bill Robinson & Ronald Deibert, "Analysis of the *Communications Security Establishment Act* and Related Provisions in Bill C-59 (*An Act respecting national security matters*), First Reading (December 18, 2017)," Joint Report by the Citizen Lab and Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC) (December 2017) at page 54, online (PDF): <https://citizenlab.ca/wp-content/uploads/2017/12/C-59-Analysis-1.0.pdf>.

[120] See Part B.2 above, in particular examples cited; Sean Boynton, "OpenAI's handling of Tumbler Ridge shooter info opens regulation questions," *Global News* (24 February 2026), online: <https://globalnews.ca/news/11687903/openai-tumbler-ridge-shooting-duty-to-inform/>; and Madison McLauchlan, "Grok's non-consensual sexual images highlight gaps in Canada's deepfake laws," *Betakit* (8 January 2026), online: <https://betakit.com/groks-non-consensual-sexual-images-highlight-gaps-in-canadas-deepfake-laws/>.

[121] See e.g. Madison McLauchlan, "Evan Solomon teases new AI laws as experts warn Canada is behind international peers," *Betakit* (24 October 2025), online: <https://betakit.com/evan-solomon-teases-new-ai-laws-as-experts-warn-canada-is-behind-international-peers/>; Sean Boynton, "Ottawa's 'refreshed' AI strategy delayed to next year, minister says," *Global News* (3 December 2025), online: <https://globalnews.ca/news/11558465/canada-artificial-intelligence-strategy-update-delay-minister/>; and Dale Smith, "Death on the order paper," *CBC National* (14 January 2025), online: <https://nationalmagazine.ca/en-ca/articles/law/hot-topics-in-law/2025/death-on-the-order-paper>.

enforcement have repeatedly collaborated with each other in contravention of both constitutional and private sector privacy law, infringing Canadian communities' constitutional privacy and other human rights, as well as their consumer privacy and data protection rights.

76. First, PIPEDA (and substantially similar provincial legislation[122]) address PAI by establishing that businesses do not need consent to collect, use, or disclose "information that is publicly available and is specified by the regulations."[123] The regulations set out discrete, narrowly defined categories of information, including telephone and business directories, government and statutory registries, court records, and personal information appearing in traditional publications, such as a magazine, book, or newspaper (provided the information came from the individual themselves).[124] These categories have over time come to define what constitutes PAI in private sector privacy law, for the purposes of legally engaging with personal information in the absence of consent.[125] The notably narrow scope of the PAI exception in PIPEDA and its provincial counterparts, and associated jurisprudence, reflects the understanding that there are myriad kinds of personal information that may be in public view or accessible by the public, but are not, by virtue of that, no longer protected by privacy law.[126]

77. Second, while the federal *Privacy Act* does not define PAI,[127] the legislation has undergone no substantive modernization since its enactment in 1983,[128] leaving an extensive gap between the legislation and its applicability to present-day threats to privacy arising from digital technologies. In fact, a *Privacy Act* modernization discussion paper by the Department of Justice specifically highlights the need to update the Act's approach to PAI: "These developments suggest a need to reconsider our reliance on practical obscurity where the legal treatment of publicly available personal information is concerned. Introducing a definition that seeks to protect individuals' reasonable expectations in context is one possible approach."[129] Multiple decisions from the Office of the Privacy Commissioner of Canada have meanwhile affirmed that section 69(2) of the *Privacy Act* does not make it open season

---

[122] *Personal Information Protection Act*, SBC 2003, c 63; and *Personal Information Protection Act*, SA 2003, c P-6.5.

[123] *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5, ss 7(1)(d), 7(2)(c.1), 7(3)(h.1) [PIPEDA].

[124] *Regulations Specifying Publicly Available Information*, SOR/2001-7, s 1 (2000).

[125] See generally Teresa Scassa, "Privacy and Publicly Available Personal Information" (2013) 11:1 CJLT 1; and Andrea Slane, "Information Brokers, Fairness, and Privacy in Publicly Accessible Information" (2018) 4 CJCCL 1.

[126] *Ibid* (Scassa), at 20 ("Expanding the scope of what is 'publicly available information' to capture such things as activity in public view seems to equate 'public' information with 'publicly available' information. There is much information that is public, yet that is not excluded from the consent requirements of data protection legislation."); see also *Alberta (Information and Privacy Commissioner) v United Food and Commercial Workers, Local 401*, 2013 SCC 62 at para 27 ("It goes without saying that by appearing in public, an individual does not automatically forfeit his or her interest in retaining control over the personal information which is thereby exposed."); Office of the Privacy Commissioner of Canada, *Google Inc WiFi Data Collection*, PIPEDA Report of Findings #2011-001 (6 June 2011) at paras 18 and 21, online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2011/pipeda-2011-001>; and Office of the Privacy Commissioner of Canada, "Interpretation Bulletin: Publicly Available Information" (11 December 2015), online: <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_06_pai/>.

[127] It states only, "Sections 7 and 8 [regarding use and disclosure] do not apply to personal information that is publicly available." *Privacy Act*, RSC, 1985, c P-21, s 69(2); for judicial interpretation, see *Lukács v Canada (Transport, Infrastructure and Communities)*, 2015 FCA 140 at para 69; and *Martin v Canada (Health)*, 2016 FC 796 at paras 57-60.

[128] Treasury Board Secretariat, "*Privacy Act* modernization" (2 April 2026), online: *Government of Canada* <https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/access-information/privacy-act-modernization-policy-approaches.html>.

[129] "*Privacy Act* Modernization: A Discussion Paper: 3. Greater certainty for Canadians and government: delineating the contours of the Privacy Act and defining important concepts" (2021) at page 5, online (PDF): *Department of Justice Canada* <https://www.justice.gc.ca/eng/csj-sjc/pa-lprp/dp-dd/modern_3.html>.

on all personal information that is in public view, especially in today's digitized society.[130] It would be incongruous and regressive for Bill C-22 to enshrine in the *Criminal Code* an undefined reference to PAI that has been already recognized as outdated and inadequate even in the context of the *Privacy Act*.

78. Third, multiple prominent Parliamentary committee studies, federal and provincial privacy commissioner investigations and special reports to Parliament, and years of academic research—including by the Citizen Lab[131]—have demonstrated a troubling pattern of Canadian law enforcement taking advantage of outdated and inadequately enforced private sector privacy laws to engage in constitutionally questionable conduct with respect to warrantless access to personal information. For instance, the House of Commons Standing Committee on Access to Information, Privacy and Ethics (ETHI) has put forward reports concerning use of ODITs by the RCMP[132] and use by the federal government of digital forensic tools on mobile devices.[133] Similarly, the Office of the Privacy Commissioner of Canada has delivered two special reports to Parliament that should cast a sobering light on what Bill C-22 purports to do with PAI, concerning the RCMP's use of intrusive social media monitoring tools under "Project Wide Awake,"[134] and police use of facial recognition technologies across Canada.[135]

---

[130] "There has been an exponential growth in the availability of personal information about individuals over the last two decades. The idea that the government could collect and use any personal information that can be purchased or accessed online without a fulsome assessment of the legality of the vendor's practices cannot be accepted as it would fail to recognize and give effect to the privacy rights of Canadians." Office of the Privacy Commissioner of Canada, *Investigation of the RCMP's collection of open-source information under Project Wide Awake* (Special report to Parliament) (15 February 2024) at para 35, online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/202324/sr_pa_20240215_rcmp-pwa/>; see also Office of the Privacy Commissioner of Canada, *Aboriginal Affairs and Northern Development Canada wrongly collects information from First Nations activist's personal Facebook page* (29 October 2013), online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-federal-institutions/2012-13/pa_201213_01> ("Under the Act, restrictions on the collection of personal information apply, whether the personal information is available publicly or not."); and Office of the Privacy Commissioner of Canada, *Canada Post's collection and use of personal information for marketing purposes not compliant with the Act* (Complaint under the *Privacy Act*) (12 May 2023) at paras 41, 44, online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-federal-institutions/2022-23/pa_20230512_cpc>.

[131] See e.g. Lex Gill & Petra Molnar, "Bots at the Gate: A Human Rights Analysis of Automated Decision Making in Canada's Immigration and Refugee System" (26 September 2018), online (PDF): Citizen Lab and International Human Rights Program, University of Toronto <https://citizenlab.ca/research/bots-at-the-gate-human-rights-analysis-automated-decision-making-in-canadas-immigration-refugee-system/>; and Kate Robertson, Cynthia Khoo & Yolanda Song, "To Surveil and Predict A Human Rights Analysis of Algorithmic Policing in Canada" (1 September 2020), online: Citizen Lab and International Human Rights Program, University of Toronto <https://citizenlab.ca/research/to-surveil-and-predict-a-human-rights-analysis-of-algorithmic-policing-in-canada/>.

[132] House of Commons, Standing Committee on Access to Information, Privacy and Ethics, "Device Investigative Tools Used By The Royal Canadian Mounted Police And Related Issues" (November 2022), online: <https://www.ourcommons.ca/DocumentViewer/en/44-1/ETHI/report-7/>.

[133] House of Commons, Standing Committee on Access to Information, Privacy and Ethics, "Federal Government's Use of Technological Tools Capable of Extracting Personal Data from Mobile Devices and Computers" (19 June 2025), online: <https://www.ourcommons.ca/DocumentViewer/en/45-1/ETHI/report-1/>.

[134] Office of the Privacy Commissioner of Canada, *Investigation of the RCMP's collection of open-source information under Project Wide Awake* (Special report to Parliament) (15 February 2024), online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/202324/sr_pa_20240215_rcmp-pwa/>.

[135] Office of the Privacy Commissioner of Canada, *Police use of Facial Recognition Technology in Canada and the way forward* (Special report to Parliament on the OPC's investigation into the RCMP's use of Clearview AI and draft joint guidance for law enforcement agencies considering the use of facial recognition technology) (10 June 2021), online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/202021/sr_rcmp/>

79. These reports all highlight the difficulties that regulators and lawmakers face in conducting effective investigation and oversight of, let alone providing consequences or remedies to, recalcitrant technology companies flouting Canadian privacy law, and law enforcement availing itself of the personal information spoils resulting from that flouting. The legal reforms required to close these privacy protection loopholes have yet to occur. Yet, while facing an ascendence of AI companies posing a potentially existential threat to privacy as we know it,[136] Bill C-22 instead threatens to expand those loopholes and make them permanent. This would be a constitutional and human rights misstep of staggering proportions.

C. Foreign Law Enforcement Access to Canadian Data

80. Bill C-22 proposes to introduce new provisions which would expand the circumstances in which foreign law enforcement authorities can obtain access to data in Canada (and conversely, in which domestic law enforcement authorities can obtain access to data outside of Canada). In summary, there are three scenarios to be considered. First, Bill C-22, on its own, opens new legal processes involving cross-border access to data, such as processes changing how foreign law enforcement authorities can access subscriber information and transmission data. The second and third scenarios involve how Bill C-22 is positioned to enable Canada to enter data-sharing treaties with foreign states, either in whole or in part (as set out in Part C.1 and C.2). In this Part C, we focus on the constitutional and human rights risks related to the latter two scenarios, but note those risks are not exclusive to those treaties, as problems can arise even in respect of Bill C-22's provisions alone.

C.1. Bill C-22 and the Second Additional Protocol to the Budapest Convention

81. When the predecessor to Bill C-22 (Bill C-2, the *Strong Borders Act*) was previously introduced in 2025, Department of Justice staff acknowledged during the question-and-answer stage of a technical briefing that the intent of certain provisions was to enable Canada to implement an international data-sharing treaty known as the "Second Additional Protocol" to the Budapest Convention on Cybercrime ("2AP"). Staff at the briefing acknowledged that other cross-border "cooperation" tools were foreseeable.

82. However, the federal government did not provide the general public or Parliament with notice or information about these plans. Nearly one year later, the federal government has declined again to provide Parliament with clarity—despite the fact that Bill C-22 again introduces reforms related to requests for information "under an international agreement or arrangement to which Canada and [a] foreign state are parties."[137]

83. The 2AP is a multilateral law enforcement data-sharing treaty. For countries that adopt it, it is designed to bypass the traditional mutual legal assistance processes that facilitate domestic court oversight of foreign law enforcement demands for information. If Canada were to ratify the

[136] See e.g. Beatrice Nolan, "AI agents are an 'existential threat' to secure messaging, Signal's president Whittaker says," *Fortune* (27 November 2025), online: <https://fortune.com/2025/11/27/ai-agents-are-an-existential-threat-to-secure-messaging-signals-president-whittaker-says/>.

[137] Bill C-22, Part 1, cl 7, proposed s 487.0181(4).

treaty, it would very likely prompt "a significant increase in the volume of requests for communication-related information by foreign and Canadian investigative entities, with a corresponding impact on the right to privacy."[138] The United States is a signatory of the treaty and would potentially be making requests for Canadian data under the framework.

84. There are multiple provisions in Bill C-22, amending the *Criminal Code* and the *Mutual Legal Assistance in Criminal Matters Act* ("MLACMA"[139]), that appear designed to enable Canada to implement the 2AP treaty:

Second Additional Protocol	Bill C-22
Article 8 would require that Canada pass a law authorizing Canadian courts to enforce an order from foreign authorities for either subscriber information or transmission data.	Clause 29 of Bill C-22 would amend the *Mutual Legal Assistance in Criminal Matters Act* to pass a law authorizing Canadian courts to enforce of an order from foreign authorities for either subscriber information or transmission data.
Article 8(6)(a)(i) of the 2AP would require that foreign orders compelling the production of subscriber be enforced within twenty days for subscriber information.	Bill C-22 proposes under section 22.07(5)(b) of MLACMA to obligate that Canadian providers must comply with foreign orders within twenty days for subscriber information.
Article 8(6)(a)(ii) of the 2AP would require that foreign orders compelling the production of subscriber be enforced within forty-five days for transmission data.	Bill C-22 proposes under section 22.07(5)(a) of MLACMA to obligate Canadian providers to comply with foreign orders within forty-five days for transmission data.
Article 7 of the 2AP would require Canada to empower its competent authorities to issue an order to be submitted directly to a foreign entity in a foreign state in order to obtain the disclosure of subscriber information. Article 8 of the 2AP would require Canada to empower its authorities to issue an order that could be served upon a foreign entity to disclose subscriber information or transmission data with the assistance of the foreign state.	Section 487.018 in Bill C-22 would enact an international production request, which empowers a judge to authorize a police officer to request subscriber information or transmission data from a foreign entity. The request "may include any information that is required by the foreign entity, by the foreign state in which the foreign entity is located or under an international agreement or arrangement to which Canada and the foreign state are parties." The federal government has not explained whether s. 487.018 is contemplated in relation to Article 7, or just Article 8 of the 2AP (if Canada intends to reserve on Article 7). In either event, the only international agreements

[138] Michael Maddock, "Consultation on the Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence" (12 April 2024) at page 3, online (PDF): *Information and Privacy Commissioner of Ontario* <https://www.ipc.on.ca/en/media/4301/download?attachment>.

[139] *Mutual Legal Assistance in Criminal Matters Act*, RSC 1985, c 30 (4th Supp) [MLACMA].

	being considered by Canada which involve "direct" access to foreign entities are the 2AP and the CLOUD Act treaty model with the United States (discussed below).
Article 9 would require Canada to amend its law to enable designated Canadian law enforcement to directly facilitate requests for subscriber information, transmission data, tracking data, and stored communications data if foreign authorities indicate in the request "sufficient facts to demonstrate that there is an emergency and how the data sought relate to it." Generally, the purpose of the provision is to enable authorities to bypass the requirements and safeguards of existing mutual assistance channels.	Section 487.11 of Bill C-22 expands the exigent circumstances power under the *Criminal Code* to include the warrantless power to seize subscriber information, transmission data, and tracking data. Section 487.0195(3) of Bill C-22 would authorize the warrantless disclosure of information to law enforcement "if the person or telecommunications service provider…is required by law, including a law of a foreign state, to provide it." This provision, on the whole, is vague and capable of being interpreted in multiple ways.

C.2. Bill C-22 and Canada-US Negotiations of a CLOUD Act Agreement

85. Bill C-22 is also being tabled at a time when it is widely known that the Canadian government has been in closed-door negotiations with the United States over a potential bilateral law enforcement data-sharing agreement between the two countries.[140] The agreement would be established under a piece of US legislation called the Clarifying Lawful Overseas Use of Data Act ("CLOUD Act").

86. A CLOUD Act agreement would require Canada to reform its laws to permit US law enforcement to directly issue demands for personal data held by Canadian technology service providers. The United States would introduce corresponding law reforms for Canadian law enforcement. If the deal proceeds, US surveillance activities covered by the agreement would no longer be subjected to oversight from Canadian authorities or courts. Canada would be relinquishing a core component of Canada's sovereignty under international law.

87. In May 2026, leaders of the House Judiciary and Foreign Affairs committees in the US Congress sent a letter to Canada's Minister of Public Safety about Bill C-22. The letter describes CLOUD Act discussions between Canada and the US as still "ongoing." The letter expressed concern that an agreement had not yet been reached, and directed that "[w]e look forward to your prompt collaboration" on the issue.

88. Canadian officials have also linked the proposed surveillance reforms, when they were presented in Bill C-2, to the United States. In July 2025, an unnamed Canadian government official—reported to have direct knowledge of trade negotiations between the US and Canada—informed *Politico* that the

[140] US Department of Justice, "United States and Canada Welcome Negotiations of a CLOUD Act Agreement" (22 March 2022), online: <https://www.justice.gov/archives/opa/pr/united-states-and-canada-welcome-negotiations-cloud-act-agreement>.

US wished for Canada to pass Bill C-2 in order to enhance law enforcement cooperation with the US. The official stated that "[a]t the heart of what the U.S. wants is to join arms in law enforcement with Canada, with the same kind of toolkit that they use: intercepts under [the *Foreign Intelligence Surveillance Act of 1978* ("FISA")] warrants, the Patriot Act."[141] One of this brief's authors has drawn in more detail the following connections between Bill C-22 and a potential CLOUD Act agreement:

> In the absence of public transparency [including explanations about why the US is leaning on Canada to pass these surveillance reforms], observers are left to read between the lines. And in those lines are signs that the US pressure and interest in seeing Bill C-22 pass very likely arises from the fact that one of the consequences of passing the legislation is that it would lay the necessary groundwork for concluding a CLOUD Act agreement between Canada and the US.
>
> For example, as previously forecast,[142] to enter a CLOUD Act agreement, Canada will need to expand the authority of Canadian judges issuing production orders (a court-ordered demand for information) to digital information stored outside Canada's borders. This type of reform is now being proposed in Bill C-22.
>
> Similarly, Bill C-22's new proposal to create a court order that can compel subscriber information through watered-down privacy protections would also move the ball up the field toward a CLOUD Act agreement. Canadian law currently affords stronger privacy safeguards toward subscriber information than US law does. While only government officials can tell us what a CLOUD Act agreement between Canada and the US would entail, CLOUD Act agreements are generally about lifting legal restrictions that would prevent companies from disclosing data to law enforcement on the other side of the border. For example, the UK–US CLOUD Act agreement includes targeted and expedited access to subscriber information with fewer protections compared to other types of information. Other parts of Bill C-22 also overlap with additional areas where Canadian protections are stronger than those afforded under the US constitution.
>
> In all likelihood, these areas of overlap are not incidental but part of a broader effort to harmonize Canadian law with American surveillance expectations ahead of a potential Canada–US CLOUD Act agreement. This would explain why—as noted above—government officials on both sides of the border have discussed Canada's lawful access reforms in the context of Canada–US co-operation.[143]

89. Undoubtedly, Bill C-22 would not be the last step towards implementing a CLOUD Act agreement; indeed, the agreement itself has not yet been tabled. But this is precisely the problem, as the public and parliamentarians lack much needed transparency regarding the impact of a CLOUD Act agreement on Bill C-22's reforms, and vice versa.

---

[141] Mickey Djuric, Mike Blanchfield, and Nick Taylor-Vaisey, "Stars, stripes and side-eye," *Politico* (4 July 2025), online: <https://www.politico.com/newsletters/canada-playbook/2025/07/04/stars-stripes-and-side-eye-00439998>.

[142] Jessica Jahn, "Canada's Future CLOUD Act Agreement with the United States," International Centre for Criminal Law Reform and Criminal Justice Policy (ICCLR) (29 March 2022), online: <https://icclr.org/2022/03/29/canadas-future-cloud-act-agreement-with-the-united-states/>.

[143] Kate Robertson, "Trump Wants to Tap Your Phone. Ottawa Might Let Him," *Walrus* (25 May 2026), online: <https://thewalrus.ca/trump-wants-to-tap-your-phone-ottawa-might-let-him/>.

C.3. Transparency Regarding Treaty-Implementing Legislation Is Obligatory

90. The Government of Canada's *Policy on Tabling of Treaties in Parliament* requires that the federal government must provide Parliament with notice and a published explanation before it can table legislation that is part of the implementation of a treaty with a foreign country. The policy better democratizes Canada's treaty-making processes, and enables parliamentarians to study legislative provisions while understanding *how those provisions will actually be used*. Otherwise, the public and parliamentarians are left with "an incomplete picture about legislation being studied—despite international treaties often carrying far-reaching consequences for the security, constitutional rights, and human rights of people in Canada and around the world."[144]

91. In particular, the Government of Canada's policy states:

> For treaties that require implementing legislation before the government can proceed to ratification, acceptance, approval or accession ("ratification"), the government will:
>
> - Observe a waiting period of at least twenty-one sitting days before the introduction of the necessary implementing legislation in Parliament;
> - Will allow Members of Parliament the same opportunities to debate, present and vote on motions, as for those treaties which do not require implementing legislation;
> - Will subsequently introduce the implementing legislation for these treaties; and
> - Seek, only when the legislation is adopted, the authorization from the Governor in Council to express consent to be bound by the treaty.[145]

92. When tabling a treaty, the federal government must also provide Parliament with an "explanatory memorandum," which details matters regarding why the treaty is in the national interest; policy considerations; a description of how the treaty will be implemented in Canadian law, including any legislation required; and a discussion of the treaty's federal, provincial, and/or territorial implications, including whether the treaty will impact matters within provincial jurisdiction. The policy requires the government to consult with provinces and territories when preparing the memorandum.

93. Even if implementing foreign law-enforcement data-sharing treaties is only part of the purpose of the legislation, the public and parliamentarians still require transparency. The policy does not exempt the government from compliance just because there might be more than one ostensible purpose behind treaty-implementing provisions.[146]

94. The above steps have not been taken in this case, leading to a significant procedural and democratic deficit instilled in Bill C-22 from the outset. That alone should give pause to any Member of Parliament purporting to meaningfully represent their constituents' interests, before passing this bill absent the required treaty-implementing transparency documentation from the federal government.

---

[144] *Ibid*.

[145] Government of Canada, *Policy on Tabling of Treaties in Parliament* at 6.2(b) (emphasis added), online: <https://www.treaty-accord.gc.ca/procedures.aspx?lang=eng>.

[146] *Ibid*.

C.4. Constitutional and Human Rights Risks of Cross-Border Data-Sharing Agreements

95. Both the 2AP and a prospective CLOUD Act agreement raise significant constitutional and human rights risks that parliamentarians must be in a position to understand and study before they can carefully consider the implications of Bill C-22's proposed powers. As noted above, this brief is only able to provide partial submissions on this issue given the absence of much-needed transparency. Some of the problems that arise are common to both data-sharing treaties, while others relate only to one or the other; each will be specified as applicable.

C.4.i. Reasonable Suspicion Standard

96. A central issue that expert scholars and civil society have raised in respect of Part 1 of Bill C-22, is that the legislation would dilute the threshold for law enforcement access to subscriber information from "reasonable belief" to "reasonable suspicion." Consideration of this issue must also include recognition that part of the very reason that Bill C-22 is lowering standards of privacy protection for subscriber information is likely for the purpose of accommodating foreign surveillance laws that already permit access to subscriber information under less protective thresholds.[147] For example, if Bill C-22 passes, US law enforcement would become able to access subscriber information in Canada through this same lower standard—and potentially without even Canadian judicial oversight if a CLOUD Act agreement is reached.

97. Recent events in the United States are instructive regarding the dangers of lowering privacy protections for subscriber information in order to cater to foreign surveillance standards:

> Far from a theoretical concern, there are already reports of an alarming pattern of abuse of powers by US authorities to seize subscriber information behind anonymous online speech that is critical of the current US administration. Earlier this month, *Wired* reported that the Department of Homeland Security demanded that Google disclose the subscriber and location data of a Canadian—located in Canada—who expressed opinions against Immigration and Customs Enforcement online.
>
> The government defends the changes in Bill C-22 on the grounds that access to subscriber information by Canadian or foreign law enforcement authorities will still be supervised by Canadian court judges. But that may no longer be the case if a CLOUD Act deal goes ahead. Moreover, inappropriate demands for subscriber information may be challenging to detect, even for the courts. For example, in the case involving the Canadian who had publicly condemned ICE killings of civilians earlier this year, the US demand for subscriber information was obscured into an investigation of a purported customs law violation.
>
> Obscuring controversial methods is, unfortunately, not an isolated occurrence. Two weeks ago, a US court issued a ruling regarding the Department of Justice's attempt to

[147] See Parts C.1 and C.2 above. See also Michael Geist, "Scoping in the Tech Giants: Bill C-22's International Production Order and the Shift to a Less Privacy-Protective Cross-Border Disclosure System," *michaelgeist.ca* (31 March 2026), online: <https://www.michaelgeist.ca/2026/03/scoping-in-the-tech-giants-bill-c-22s-international-production-order-and-the-shift-to-a-less-privacy-protective-cross-border-disclosure-system/>.

> force a US hospital to disclose transgender youth health records under the guise of an investigation for fraud-related charges. The court expressed significant concern, noting that the department wields "immense prosecutorial authority and discretion" but that it had "proven unworthy of this trust at every point in this case."
>
> The department had misrepresented and withheld information from multiple courts "in an obvious effort to shield its recent investigative tactics," had engaged in forum shopping to move to a court "that DOJ deems friendly to its political positions," and its representatives were found to have misrepresented salient facts while under oath.[148]

The above events involve the very parts of the US government with which Canadian law enforcement would likely be cooperating under a foreign data-access agreement. This raises concerns both for the degree to which, if any, Canadian personal information would be protected once it is transferred to the US (discussed further in Part C.5 below), as well as regarding the extent to which US agencies and law enforcement would respect the terms of any such agreement, in particular those aimed at protecting constitutional and human rights.

C.4.ii. Human Rights Violations, Chilling Effects, and Transnational Repression

98. In addition to lowering the threshold standard to reasonable suspicion, other aspects of the 2AP would increase the danger that subscriber information or transmission data will be disclosed to foreign law enforcement in inappropriate circumstances, and where it would interfere with human rights such as the freedom of expression, freedom from discrimination, and the right to privacy:

> Article 8 sets limits regarding the amount of supporting information that is required [to] have a foreign request for subscriber information or transmission data enforced. It contains no requirements mandating that all material facts be fully, frankly, and fairly described—information that is essential for meaningful scrutiny and oversight. The explanatory reports even describe that any summary of facts should be "brief." All additional information is treated as optional.
>
> …under international human rights standards, prior review by the independent judicial authority is required to establish that there are sufficient factual and legal grounds to justify the invasion of privacy—a key safeguard against arbitrary and unreasonable interferences. It cannot be an exercise of proforma rubber stamping. The [2AP's] direct requirement or encouragement of providing <u>less information</u> to requested States and service providers (including in some cases even prohibiting information from being shared with service providers), directly undermines this review function.[149]

99. These risks are intolerable given the fact that the Supreme Court of Canada has made clear that access to subscriber information that links a person with anonymously undertaken online activities

[148] Kate Robertson, "Trump Wants to Tap Your Phone. Ottawa Might Let Him," *Walrus* (25 May 2026), online: <https://thewalrus.ca/trump-wants-to-tap-your-phone-ottawa-might-let-him/>.

[149] Kate Robertson and Verónica Arroyo, "Expediting Human Rights Abuses: A Constitutional and Human Rights Analysis of the Second Additional Protocol to the Budapest Convention on Cybercrime," Citizen Lab, Munk School of Global Affairs & Public Policy, University of Toronto (March 2024) at paras 37 and 53 (emphasis added), online (PDF): <https://citizenlab.ca/wp-content/uploads/2025/06/PDF-copy-June-2025-Submission.pdf>.

engages "significant privacy interests."[150] Not only would a reasonable suspicion standard lower the threshold of belief to suspicion only, domestic or foreign law enforcement would only be required to show that the information would merely "assist" in the investigation of any offence. This is a very low standard of relevance. The proposed law would leave it open to law enforcement to describe *some* basis for showing how that data would "assist" in an investigation, even if the person whose subscriber information is at issue is innocent of any wrongdoing.

100. The US court ruling this month censuring the US DOJ's improper tactics and misrepresentations in its pursuit of identity information (and other health data) underscores the broader danger that Bill C-22's diluted privacy thresholds increase the risk of censorship, discrimination, chilling effects, human rights violations, or other forms of transnational repression from foreign surveillance actors. States may abuse the expedited data-sharing regime to track, de-anonymize, and surveil protesters and human rights dissidents living in Canada or elsewhere.

101. In this way, the 2AP has been the subject of significant criticism by human rights organizations around the world: "[I]f the 2AP is adopted as a global standard, it would contribute to the elimination and diminishment of protections that are critical to mutual legal assistance treaties and norms. As a result, 'much of the world's population may be left vulnerable to arbitrary and abusive data collection practices by domestic law enforcement agencies.'"[151]

C.4.iii. Myriad Issues with 2AP Not Reflected in Bill C-22

102. Bill C-22 would implement specific provisions like Article 8 of the 2AP, but implementing Article 8 of the 2AP would mean Canada is ratifying the *treaty as a whole* (subject to the availability of some reservations), including components that aren't explicitly reflected in Bill C-22. For example, in Citizen Lab's submission to Canada's Department of Justice on the 2AP,[152] the authors urge attention toward Articles 12 and 14(1), which authorize data transfers between states and foreign law enforcement authorities under other secretive agreements or "arrangements," or between the law enforcement authorities of multiple states directly. Article 14(1) explicitly permits states to *agree to ignore* even the weak data protection requirements in Article 14. Rather than "establishing high standards, the protocol prioritizes law enforcement access at almost every turn."[153]

103. The problems with 2AP are too lengthy to exhaust in this brief. For a more thorough analysis, we refer to the above-mentioned Citizen Lab submission to the Department of Justice.[154]

---

[150] *R v Spencer*, 2014 SCC 43 at para 50.

[151] Kate Robertson and Verónica Arroyo, "Expediting Human Rights Abuses: A Constitutional and Human Rights Analysis of the Second Additional Protocol to the Budapest Convention on Cybercrime," Citizen Lab, Munk School of Global Affairs & Public Policy, University of Toronto (March 2024), online: <https://citizenlab.ca/wp-content/uploads/2025/06/PDF-copy-June-2025-Submission.pdf> (pdf).

[152] *Ibid*.

[153] Tamir Israel & Katitza Rodriguez, "On New Cross-Border Cybercrime Policing Protocol, a Call for Caution," *Just Security* (13 May 2022), online: <https://www.justsecurity.org/81502/on-new-cross-border-cybercrime-policing-protocol-a-call-for-caution/>.

[154] Kate Robertson and Verónica Arroyo, "Expediting Human Rights Abuses: A Constitutional and Human Rights Analysis of the Second Additional Protocol to the Budapest Convention on Cybercrime," Citizen Lab, Munk School of Global Affairs & Public Policy, University of Toronto (March 2024), online (PDF): <https://citizenlab.ca/wp-content/uploads/2025/06/PDF-copy-June-2025-Submission.pdf>.

C.4.iv. CLOUD Act Agreement Represents Constitutional and Human Rights Minefield

104. Bill C-22's reforms "overlap with some of the exact areas that Canada's constitutional protection provides greater protection against unreasonable surveillance than that of the US constitution."[155] Perhaps most significantly is the United States' third-party doctrine, which deprives individuals in the US of constitutional privacy protections if their information is shared with a third party. The United States is now struggling with a decades-old doctrine that is inappropriate for the digital age: "Fifty years later, smartphones are now ubiquitous, each loaded to the hilt with third-party apps hoovering up reams of private data about the most intimate and sensitive aspects of our daily lives."[156]

105. Conversely, Canada's Supreme Court rejected the premises of the US third-party doctrine decades ago, and Canadian jurisprudence ever since has maintained that "[o]ur approach is distinct from the United States."[157] As a result, the Canadian government faces "a veritable minefield of incompatibilities and contradictions between Canada's constitutional and human rights frameworks, and those of the U.S."[158] Those differences were anticipated to be the root of prohibitive incompatibilities between the two countries in reaching a potential CLOUD Act agreement."[159] Bill C-22's reforms (see, for example, Parts B and D of this brief) are symptomatic of how Canada's distinct approach is already deteriorating under pressure from the United States.

106. Moreover, since Canada began negotiations with the United States, the Supreme Court of the United States consequentially ruled in 2024 that the US President wields power over criminal law investigations "that neither Congress nor the courts can touch."[160] This legal interpretation has ushered in serious threats to the rule of law in the United States, and has added to the now growing list of fundamental constitutional differences with the United States. These changes "point to a structural deterioration that will persist long after [President Trump] leaves office."[161] In Canada, it is a core constitutional principle that the justice system must remain free of political interference from the executive branch. But if Canada accedes to a CLOUD Act agreement, Bill C-22's new and unprecedentedly expansive powers "would end up in the hands of the US President and 'his lawyers'."[162]

---

[155] Kate Robertson, "Unspoken Implications: A Preliminary Analysis of Bill C-2 and Canada's Potential Data-Sharing Obligations Towards the United States and Other Countries," Citizen Lab, Munk School of Global Affairs & Public Policy, University of Toronto (16 June 2025), online: <https://citizenlab.ca/research/a-preliminary-analysis-of-bill-c-2/>.

[156] Cynthia Khoo and Kate Robertson, "Canada-U.S. Cross-Border Surveillance Negotiations Raise Constitutional and Human Rights Whirlwind under U.S. CLOUD Act," Citizen Lab, Munk School of Global Affairs & Public Policy, University of Toronto (24 February 2025), online: <https://citizenlab.ca/research/canada-us-cross-border-surveillance-cloud-act/>.

[157] *R v Bykovets*, 2024 SCC 6 at para 47.

[158] Cynthia Khoo and Kate Robertson, "Canada-U.S. Cross-Border Surveillance Negotiations Raise Constitutional and Human Rights Whirlwind under U.S. CLOUD Act," Citizen Lab, Munk School of Global Affairs & Public Policy, University of Toronto (24 February 2025), online: <https://citizenlab.ca/research/canada-us-cross-border-surveillance-cloud-act/>.

[159] *Ibid*.

[160] Jack Goldsmith, "The President's Favorite Decision: The Influence of Trump v. U.S. in Trump 2.0," *Lawfare* (10 February 2025), online: <https://www.lawfaremedia.org/article/the-president-s-favorite-decision--the-influence-of-trump-v.-u.s.-in-trump-2.0>.

[161] Kate Robertson, "Trump Wants to Tap Your Phone. Ottawa Might Let Him," *Walrus* (25 May 2026), online: <https://thewalrus.ca/trump-wants-to-tap-your-phone-ottawa-might-let-him/>.

[162] *Ibid*.

C.5. Consequences of Sharing Canadian Personal Data with Foreign Entities

107. There are a number of troubling consequences that may arise once Canadian personal data is in the hands of foreign law enforcement or other state agencies, as would be facilitated by the 2AP and a Canada-US CLOUD Act agreement. At the outset is a misalignment in privacy laws making Canadian personal data more vulnerable to misuse and exploitation.[163] Both state and private actors in the US, for instance, are subject to fewer constraints that protect the right to privacy than in Canada, such as the lack of a federal consumer privacy law such as PIPEDA,[164] and the continued application of the third-party doctrine in constitutional privacy law, which Canadian jurisprudence has long abandoned (discussed in Part C.4 above). As a result of differing legal regimes, personal information is routinely collected, used, and disclosed in the US, and in other countries that have signed the 2AP, where it would likely be illegal if done in Canada, often in violation of additional human rights beyond privacy.

108. For example, US Immigration and Customs Enforcement ("ICE") relies on a panoply of surveillance technologies and systems, such as facial recognition and phone tracking software,[165] as well as home utilities data[166] and genetic and biometric databases,[167] to pursue immigrants for indiscriminate detention and deportation, and retaliate against protestors.[168] Law enforcement in the UK has implemented live facial recognition across cities despite deep human rights issues with its use.[169] Violative surveillance is also a core aspect of states engaging in digital transnational repression, including of dissidents who have made their home in Canada.[170]

---

[163] Kate Robertson and Verónica Arroyo, "Expediting Human Rights Abuses: A Constitutional and Human Rights Analysis of the Second Additional Protocol to the Budapest Convention on Cybercrime," Citizen Lab, Munk School of Global Affairs & Public Policy, University of Toronto (March 2024) at pages 25-31, online (PDF): <https://citizenlab.ca/wp-content/uploads/2025/06/PDF-copy-June-2025-Submission.pdf>.

[164] See e.g. Adi Robertson, "America desperately needs new privacy laws," *Verge* (22 February 2026), online: <https://www.theverge.com/column/882516/privacy-laws-america>; and Caitriona Fitzgerald, "America needs a strong privacy law. The SECURE Data Act isn't it" (4 May 2026), online: *Electronic Privacy Information Center (EPIC)* <https://epic.org/america-needs-a-strong-privacy-law-the-secure-data-act-isnt-it/>.

[165] Lauren Girgis, "How ICE is using technology, databases to track people," *Seattle Times* (13 February 2026), online: <https://www.seattletimes.com/seattle-news/law-justice/how-ice-is-using-technology-databases-to-track-people/>.

[166] Nina Wang et al, "American Dragnet: Data-Driven Deportation in the 21st Century" (May 2022), online: *Center on Privacy & Technology at Georgetown Law* <https://americandragnet.org/finding3> ("V. ICE exploits people's basic needs for heat, electricity and water by collecting utility records through opaque and unregulated data brokers").

[167] Stevie Glaberson, Emerald Tse & Emily Tucker, "Raiding the Genome: How the United States Government Is Abusing Its Immigration Powers to Amass DNA for Future Policing" (May 2024), online: *Center on Privacy & Technology at Georgetown Law* <https://www.law.georgetown.edu/privacy-technology-center/publications/raiding-the-genome/>; and Mizue Aizeki & Paromita Shah, "HART Attack: DHS's massive biometrics database supercharges surveillance & threatens rights" (May 2022), online: *Just Futures Law* <https://www.justfutureslaw.org/hart-attack>.

[168] Daphne Duret & Jesse Bogan, "'We Know Where You Live.' Protesters Say ICE Agents Retaliate With Threats, Investigations," *Marshall Project* (2 April 2026), online: <https://www.themarshallproject.org/2026/02/04/ice-immigration-intimidation-tactics-protesters>.

[169] Ella Kipling & Dominic Casciani, "Court challenge over Met Police's use of live facial recognition lost," *BBC* (21 April 2026), online: <https://www.bbc.com/news/articles/cq59x4vv954o>; and Peter Fussey & Daragh Murray, "Policing Uses of Live Facial Recognition in the United Kingdom" in Amba Kak, ed, *Regulating Biometrics: Global Approaches and Urgent Questions* (September 2020), online (PDF): AI Now Institute <https://ainowinstitute.org/wp-content/uploads/2023/09/regulatingbiometrics-fussey-murray.pdf>.

[170] See Noura Aljizawi et al, "Psychological and Emotional War: Digital Transnational Repression in Canada" (March 2022), online: Citizen Lab <https://citizenlab.ca/research/psychological-emotional-war-digital-transnational-repression-canada/>;

109. Meanwhile, private companies amass personal information to build ethically and legally questionable technologies facilitating algorithmic discrimination[171] and an astounding range of short-term and long-term harms associated with the use and deployment of software programs marketed as "AI."[172] The boundaries between government-held sensitive data and private sector access to that data have also increasingly broken down, such as through Elon Musk's "Department of Government Efficiency" in the US;[173] and data brokers and commercial surveillance vendors selling personal data back to police and intelligence agencies for monitoring and tracking people.[174]

110. Under the Bill C-22 provisions, as well as potential cross-border law-enforcement data-sharing agreements, personal information could be shared with foreign governments as a matter of incidental collection—for example, the private messaging history of a suspect with someone would also be the other person's private messaging history with them, even if the interlocutor is uninvolved with the activities being investigated. Yet, there do not appear to be data minimization or other protective obligations either built into Bill C-22 itself or placed on signatories within 2AP or a CLOUD Act agreement, which Canada or the individual or group in Canada whose privacy was violated would be able to enforce in practice.

111. It is far from clear that signatories such as the US would even adhere to such obligations, or respect Canadian jurisdiction or sovereignty in the event, given there has already been at least one reported instance of a US government agency requesting detailed information from Google about a Canadian man who criticized the US president online, despite no active substantive ties to the US.[175] The federal government has to date failed to explain why none of the above should be of concern to the Canadian public, or how it will ensure Canadian personal information—or indeed, the people whose information it is—will remain protected at the level guaranteed by Canadian constitutional, human rights, and privacy law even after being passed onto foreign governments with poor human rights records.

---

and Noura Aljizawi et al, "No Escape: The Weaponization of Gender for the Purposes of Digital Transnational Repression" (December 2024), online: Citizen Lab <https://citizenlab.ca/research/the-weaponization-of-gender-for-the-purposes-of-digital-transnational-repression/>.

[171] See e.g. Virginia Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor* (New York: St. Martin's Press, 2018); Safiya Noble, *Algorithms of Oppression* (New York: NYU Press, 2018); Ava Sasani, "As AI tools get smarter, they're growing more covertly racist, experts find," *Guardian* (16 March 2024), online: <https://www.theguardian.com/technology/2024/mar/16/ai-racism-chatgpt-gemini-bias>; and Reece Rogers & Victoria Turk, "OpenAI's Sora Is Plagued by Sexist, Racist, and Ableist Biases," *Wired* (23 March 2025), online: <https://www.wired.com/story/openai-sora-video-generator-bias/>.

[172] "Open Letter to the Minister of Artificial Intelligence and Digital Innovation from Civil Society Organizations and Individuals Opposing 'National Sprint' Consultation on AI Strategy" (31 October 2025) at pages 2-4, online (PDF): *People's Consultation on AI* <https://www.peoplesaiconsultation.ca/open-letter/>.

[173] Makena Kelly et al, "Inside Elon Musk's 'Digital Coup'," *Wired* (13 March 2025), online: <https://www.wired.com/story/elon-musk-digital-coup-doge-data-ai/>.

[174] See e.g. Byron Tau, "How the Pentagon Learned to Use Targeted Ads to Find Its Targets—and Vladimir Putin," *Wired* (27 February 2024), online: <https://www.wired.com/story/how-pentagon-learned-targeted-ads-to-find-targets-and-vladimir-putin/>; and Wolfie Christl et al, "Uncovering Webloc: An Analysis of Penlink's Ad-based Geolocation Surveillance Tech" (April 2026), online: *Citizen Lab* <https://citizenlab.ca/research/analysis-of-penlinks-ad-based-geolocation-surveillance-tech/>.

[175] Chris Iorfida, "Canadian sues U.S. Homeland Security, which allegedly sought his Google data after critical social media posts," *CBC News* (6 May 2026), online: <https://www.cbc.ca/news/world/us-dhs-aclu-lawsuit-canadian-john-doe-9.7187851>.

C.6. Lack of Remedy for Human Rights Violations

112. The enactment of provisions that would empower or potentially compel a Canadian service provider to send transmission data, subscriber information, or other personal information to a foreign state raises grave issues of justiciability and enforcement with respect to protecting the privacy and other human rights of individuals whose data is transferred. As currently drafted, in proposed section 487.0181 of the *Criminal Code* and section 22.07 in MLACMA, Bill C-22 includes no remedies or recourse to vindicate one's human rights being violated by a foreign state actor as a result of receiving personal data from Canada. This is especially concerning given the wide range of signatories to 2AP, some of whom have shown flagrant disregard or overt hostility towards human rights and the rule of law, but which would be granted these production order powers for Canadian data under the 2AP.

113. The US (also a 2AP signatory) would obtain even broader cross-border data access should a CLOUD Act agreement come to pass.[176] CLOUD Act agreements with both the UK and Australia have explicitly refused to establish any rights or remedies for individuals or organizations whose data is subject to seizure under each agreement.[177]

114. Taking the US as just one example, there are several ways in which legal protection for Canadian privacy rights are lost once Canadian data crosses the border. First, a 2017 Presidential executive order removed what little protection may have been granted under the US Privacy Act, "explicitly exclud[ing] individuals who are not United States citizens or permanent residents from privacy protections."[178] Second, the US has long maintained that it is not subject to international human rights obligations, such as those under the International Covenant on Civil and Political Rights ("ICCPR"), in the case of non-US citizens outside its borders being surveilled by US law enforcement.[179] Quoting an earlier Citizen Lab analysis, "It seems a contradiction in

---

[176] See for example the scope of data accessible under the Australia-US CLOUD Act agreement: "Covered Data means the following types of data when possessed or controlled by a private entity acting in its capacity as a Covered Provider: content of an electronic or wire communication; computer data stored or processed for a user; traffic data or metadata pertaining to an electronic or wire communication or the storage or processing of computer data for a user; and Subscriber Information when sought pursuant to an Order that also seeks any of the other types of data referenced in this definition." *Agreement between the Government of the United States of America and the Government of Australia on Access to Electronic Data for the Purpose of Countering Serious Crime* ("Australia-US CLOUD Act agreement"), United States and Australia, 15 December 2021, at Art 1(4) (emphasis omitted), online: <https://www.justice.gov/criminal/criminal-oia/cloud-act-agreement-between-governments-us-and-australia>.

[177] *Agreement between the Government of the United State of America and the Government of the United Kingdom of Great Britain and Northern Ireland on Access to Electronic Data for the Purpose of Countering Serious Crime* ("UK-US CLOUD Act agreement"), United States and United Kingdom, 3 October 2019, at Art 3(4), online: <https://www.justice.gov/criminal/criminal-oia/cloud-act-agreement-between-governments-us-united-kingdom-great-britain-and-northern>; and *Agreement between the Government of the United States of America and the Government of Australia on Access to Electronic Data for the Purpose of Countering Serious Crime* ("Australia-US CLOUD Act agreement"), United States and Australia, 15 December 2021, at Art 3(6), online: <https://www.justice.gov/criminal/criminal-oia/cloud-act-agreement-between-governments-us-and-australia>.

[178] House of Commons, Standing Committee on Access to Information, Privacy and Ethics, "Protecting Canadians' Privacy at the U.S. Border" (December 2017) at page 16, online (PDF): <https://www.ourcommons.ca/Content/Committee/421/ETHI/Reports/RP9264624/ethirp10/ethirp10-e.pdf>.

[179] "The United States also notes its longstanding position that the ICCPR only applies to individuals who are both within the territory of the State Party and within that State Party's jurisdiction in line with Article 2(1) of the ICCPR." "United States Response to OHCHR Questionnaire on "The Right to Privacy in the Digital Age" (2014), online: *United Nations Office of the High Commissioner for Human Rights* <https://www.ohchr.org/sites/default/files/Documents/Issues/Privacy/United_States.pdf>; see also Kevin Jon Heller, "Does the ICCPR Apply Extraterritorially?," *OpinioJuris* (18 July 2006), online: <https://opiniojuris.org/2006/07/18/does-the-iccpr-apply-extraterritorially/>; and Harold Hongju Koh, "Memorandum Opinion on the Geographic Scope of the International

terms to task a U.S. judge with the vital responsibility of protecting the rights of people whom U.S. courts are simply not bound to protect, according to the U.S.'s own laws."[180]

115. In fact, it was for similar reasons that the Court of Justice of the European Union ("CJEU") not just once, but twice, struck down the US's adequacy status under the EU General Data Protection Regulation ("GDPR").[181] This was due to the US's foreign intelligence laws, which also do not recognize the privacy rights of non-US citizens outside the US. As one commentator noted, "when personal data is transferred to the US, the data subject loses control of that data to the US intelligence community."[182] Thus, EU data subjects could not be said to retain equivalent protection or rights as under the GDPR once their data was shared with even non-state actors in the US, a result the CJEU recognized as untenable under EU law. By extension, Canada entering into a data-sharing agreement with the US such as that contemplated under the CLOUD Act may result in its own adequacy status with the EU being threatened.

116. If Bill C-22 passes, a Canadian resident's personal information could be shared with US law enforcement under circumstances constituting an illegal search in Canadian law, but under the proposed regime, that person would have neither legal rights in the US nor legal recourse in Canada, to challenge or be remedied for that violation. They have simply lost what is meant to be a fundamental human right and constitutional guarantee under the *Charter*. Bill C-22 grants only the receiving electronic service provider the right to challenge a request believed to be unlawful or inappropriate, placing what in most cases would be a commercial business in the seat of a judicial arbiter over someone's human rights.

C.7. Recommendations to Protect Human Rights in Cross-Border Data Sharing

117. As a result of the above, we **recommend** that SECU's study of Part 1 of Bill C-22 be suspended until the government provides full transparency regarding its intentions concerning the Second Additional Protocol (2AP), and a Canada-US CLOUD Act agreement. In order for the government to understand how either agreement would impact or shed light on the potential repercussions of Bill C-22's provisions, the federal government must also commit to complying with the *Policy on Tabling of Treaties in Parliament*.

118. If the provisions in Bill C-22 regarding sharing personal information with foreign entities remain, then we **recommend** emphatically that the bill be amended to add several necessary safeguards. These guardrails are critical to mitigating some of the risk of privacy or other human rights violations in the context of sharing personal information with foreign governments, whether in

---

Covenant on Civil and Political Rights," Office of the Legal Adviser, United States Department of State (19 October 2010) at page 55, online (PDF): *Just Security* <https://www.justsecurity.org/wp-content/uploads/2014/03/state-department-iccpr-memo.pdf> (A US Department of State legal memo analyzing the US position and concluding that it "stands in significant tension with the treaty's object and purpose").

[180] Cynthia Khoo and Kate Robertson, "Canada-U.S. Cross-Border Surveillance Negotiations Raise Constitutional and Human Rights Whirlwind under U.S. CLOUD Act," *Citizen Lab, Munk School of Global Affairs & Public Policy, University of Toronto* (24 February 2025), online: <https://citizenlab.ca/research/canada-us-cross-border-surveillance-cloud-act/>.

[181] *Schrems v Data Protection Commissioner*, C-362/14 [2015]; and *Data Protection Commissioner v Facebook Ireland Ltd, Maximilian Schrems and intervening parties*, C-311/18 [2020].

[182] PJ Blount, "*Schrems II* and the Data Protection Enforcement Gap" (31 August 2021), online: EU Law Enforcement <https://eulawenforcement.com/?p=8062>.

the context of international law-enforcement data-sharing treaties, or the C-22 sharing mechanisms on a standalone basis, even in the absence of a treaty. Provisions implementing the following mandatory safeguards should be added to Bill C-22 where it addresses data-sharing with foreign entities and mutual legal assistance: (i) a dual criminality requirement; (ii) exclusion of requests related to political offences or where politically motivated; (iii) exclusion of requests related to a discriminatory purpose on basis of protected characteristics; (iv) mandatory rule-of-law assessment and assessment of human rights track record; and (v) mandatory data deletion obligations and retention policies. Each of these will be briefly discussed below in turn.

C.7.i. Dual Criminality

119. Requests from foreign entities for personal information should be rejected if the suspected or investigated criminal offence in question is based on conduct that is not also a serious criminal offence under Canadian law. This requirement already exists in MLACMA for requests issued outside of a signed agreement,[183] which many foreign requests received if Bill C-22 passes are likely to be, as well as in at least one signed agreement.[184]

120. A dual-criminality requirement is necessary to prevent Canada's legal system from being used by foreign states to persecute people in countries "that overcriminalize protected expression and behavior in a manner inconsistent with international human rights law."[185] For example, more than 120 countries have criminalized seeking or obtaining an abortion—a constitutionally protected activity in Canada—with an associated prison sentence of up to ten years,[186] and the US state of Alabama tabled a bill in 2019 which would have sentenced doctors to 99 years in prison for performing an abortion.[187]

C.7.ii. Exclude Political Offences or If Politically Motivated

121. Bill C-22 should impose an obligation to reject foreign law enforcement requests for data where the investigation "relates to an offence of a political character" or is considered "related to a political offence or as being prosecuted for political reasons." This exception appears in a number of bilateral, multilateral, and regional agreements to which Canada is already a party.[188] The

[183] MLACMA, ss 6(1)-6(2).

[184] *Agreement between the Government of Canada and the Government of the Hong Kong Special Administrative Region of the People's Republic of China on Mutual Legal Assistance in Criminal Matters*, Canada and Hong Kong, 16 February 2001 (entered into force 1 March 2002) at Art 5(2)(d), online: <https://www.treaty-accord.gc.ca/Treaty_Docs/PDF/103865.pdf>; see also "Open Letter Regarding the United Nations Convention on Cybercrime" (10 December 2024) at page 7, online: <https://openmedia.org/assets/20241210-UNCC.Canada_.Letter_.pdf> (regarding suspension of bilateral agreement with Hong Kong).

[185] Human Rights Watch, "Comments on the Updated Draft Text of the UN Cybercrime Convention (Rev 3)" (July 2024) at page 7, online (PDF): <https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Reconvened_concluding_session/Written_submissions/OP8/HRW_comments_on_Rev3_20240729.pdf>.

[186] Julianne McShane, "Some people who seek abortions can face prison time in more than 120 countries, analysis shows," *NBC News* (21 March 2023), online: <https://www.nbcnews.com/health/womens-health/abortion-penalties-prison-time-around-world-rcna75760>.

[187] Debbie Elliott & Laurel Wamsley, "Alabama Governor Signs Abortion Ban Into Law," *NPR* (14 March 2019), online: <https://www.npr.org/2019/05/14/723312937/alabama-lawmakers-passes-abortion-ban>.

[188] See in-line citations in "Open Civil Society Letter Regarding the United Nations Convention on Cybercrime" (10 December 2024) at page 6, online: <https://openmedia.org/assets/20241210-UNCC.Canada_.Letter_.pdf> ("The draft Convention lacks a

Citizen Lab, through its research, has extensively documented over the years the many ways in which governments all over the world rely on various surveillance technologies and control over digital information and communications networks to repress political dissent or target their political opponents, as well as persecute dissidents, journalists, and human rights defenders.[189] Without this provision, Canadian electronic service providers and legal authorities could become complicit by aiding foreign governments in these aims.

C.7.iii. Exclude If Discriminatory Purpose on Basis of Protected Characteristics

122. Canadian receivers of requests to share data with foreign law enforcement must also be required to refuse a request if the "investigation has been initiated for the purpose of prosecuting, punishing, or discriminating in any way against an individual or group of persons for reason of sex, race, social status, nationality, religion, or ideology."[190] Without a required refusal provision on grounds of discrimination, Canada may be assisting authoritarian regimes in any number of abominable acts targeting vulnerable and historically marginalized communities, despite the right to equality and freedom from discrimination being a constitutional guarantee under our own laws.

123. For example, dozens of countries across the globe still criminalize homosexuality, while others criminalize non-conforming gender expression, effectively outlawing "expression of transgender identities."[191] In early 2026, Israel passed a purported anti-terrorism law that *de facto* applied the

---

political crimes exception, even though this exception is present in numerous other bilateral or regional agreements [pointing to agreements with Hong Kong, Thailand, and Uruguay; the *Budapest Convention*; and the *Inter-American Convention on Mutual Assistance in Criminal Matters*] that Canada has adopted").

[189] See e.g. Bill Marczak, John Scott-Railton & Sarah McKune, "Hacking Team Reloaded? US-Based Ethiopian Journalists Again Targeted with Spyware" (9 March 2015), online: *Citizen Lab* <https://citizenlab.ca/research/hacking-team-reloaded-us-based-ethiopian-journalists-targeted-spyware/>; Katie Kleemola, Masashi Crete-Nishihata & John Scott-Railton, "Targeted Attacks against Tibetan and Hong Kong Groups Exploiting CVE-2014-4114" (15 June 2015), online: *Citizen Lab* <https://citizenlab.ca/research/targeted-attacks-against-tibetan-and-hong-kong-groups-exploiting-cve-2014-4114/>; Bill Marczak & John Scott-Railton, "The Million Dollar Dissident: NSO Group's iPhone Zero-Days Used Against A UAE Human Rights Defender" (24 August 2016), online: *Citizen Lab* <https://citizenlab.ca/research/million-dollar-dissident-iphone-zero-day-nso-group-uae/>; John Scott-Railton et al, "Reckless Exploit: Mexican Journalists, Lawyers, and a Child Targeted with NSO Spyware" (19 June 2017), online: *Citizen Lab* <https://citizenlab.ca/research/reckless-exploit-mexico-nso/>; Bill Marczak et al, "The Kingdom Came to Canada How Saudi-Linked Digital Espionage Reached Canadian Soil" (1 October 2018), online: *Citizen Lab* <https://citizenlab.ca/research/the-kingdom-came-to-canada-how-saudi-linked-digital-espionage-reached-canadian-soil/>; Noura Aljizawi et al, "No Escape: The Weaponization of Gender for the Purposes of Digital Transnational Repression" (2 December 2024), online: *Citizen Lab* <https://citizenlab.ca/research/the-weaponization-of-gender-for-the-purposes-of-digital-transnational-repression/>; Noura Aljizawi et al, "Psychological and Emotional War: Digital Transnational Repression in Canada" (1 March 2022), online: *Citizen Lab* <https://citizenlab.ca/research/psychological-emotional-war-digital-transnational-repression-canada/>; Bill Marczak et al, "Virtue or Vice? A First Look at Paragon's Proliferating Spyware Operations" (19 March 2025), online: *Citizen Lab* <https://citizenlab.ca/research/a-first-look-at-paragons-proliferating-spyware-operations/>; Bill Marczak & John Scott-Railton, "Graphite Caught: First Forensic Confirmation of Paragon's iOS Mercenary Spyware Finds Journalists Targeted" (12 June 2025), online: *Citizen Lab* <https://citizenlab.ca/research/first-forensic-confirmation-of-paragons-ios-mercenary-spyware-finds-journalists-targeted/>; John Scott-Railton et al, "Not Safe for Politics: Cellebrite Used on Kenyan Activist and Politician Boniface Mwangi" (17 February 2026), online: *Citizen Lab* <https://citizenlab.ca/research/cellebrite-used-on-kenyan-activist-and-politician-boniface-mwangi/>; and Gary Miller & Swantje Lange, "Bad Connection: Uncovering Global Telecom Exploitation by Covert Surveillance Actors" (23 April 2026), online: *Citizen Lab* <https://citizenlab.ca/research/uncovering-global-telecom-exploitation-by-covert-surveillance-actors/>.

[190] *Inter-American Convention on Mutual Assistance in Criminal Matters*, 3 June 1996, E104683 (entered into force 14 April 1996) at Art 9(b).

[191] Human Rights Watch, "#Outlawed: 'The Love that Dare Not Speak Its Name'," online: <https://features.hrw.org/features/features/lgbt_laws/>; and Chris Geidner, "After a string of losses in its anti-trans project, DOJ turns to grand jury subpoenas in Texas," *Law Dork* (13 May 2026), online: <https://www.lawdork.com/p/after-a-string-of-losses-in-its-anti>.

death penalty exclusively to Palestinians, prompting an immediate "early warning and urgent action procedure" response from the UN Committee on the Elimination of Racial Discrimination.[192] Research by the Citizen Lab has shown that state actors leverage sexism, misogyny, and gendered online abuse against female political dissidents who have left their home countries, engaging in gender-based digital transnational repression.[193] The federal government cannot allow the Canadian legal system to be leveraged towards such ends, whether targeting people within or outside of Canada.

C.7.iv. Rule of Law and Human Rights Track Record Assessment

124. The MLACMA should be amended to require periodic assessments and suspension of information-sharing with any country that exhibits systematic disregard for the rule of law in the country or any pattern of human rights abuses. If a country is found to have exhibited breakdown in rule of law, or systematic human rights abuses, then Canadian electronic service providers should be prohibited from sharing data with them under the new law.

125. This recommendation is informed by the Rule of Law Framework[194] that the European Union established in 2014 "to resolve future threats to the rule of law in Member states before the conditions for activating the [much more drastic] mechanisms foreseen in Article 7 [of the Treaty of the European Union] would be met."[195] The Framework is meant to be activated under circumstances where a Member state's authorities are creating or allowing a situation that is "likely to systematically and adversely affect the integrity, stability or the proper functioning of the institutions and the safeguard mechanisms established at national level to secure the rule of law."[196] This includes threats to a country's "political, institutional and/or legal order… or its constitutional structure, separation of powers, the independence or impartiality of the judiciary, or its system of judicial review including constitutional justice where it exists."[197] The Framework has been activated in two cases to date, for Poland and Hungary.[198]

---

[192] United Nations Office of the High Commissioner of Human Rights, "Israel's discriminatory death penalty law marks grave human rights retrogression, UN anti-racism committee warns" (1 May 2026), online: <https://www.ohchr.org/en/press-releases/2026/05/israels-discriminatory-death-penalty-law-marks-grave-human-rights>; UN OHCHR Committee on the Elimination of Racial Discrimination, "Statement on the Adoption of the 'Death Penalty for Terrorists Law' in Israel" (29 April 2026), online: <https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=INT%2FCERD%2FSWA%2FISR%2F11496>.

[193] Noura Aljizawi et al, "No Escape: The Weaponization of Gender for the Purposes of Digital Transnational Repression" (2 December 2024), online: *Citizen Lab* <https://citizenlab.ca/research/the-weaponization-of-gender-for-the-purposes-of-digital-transnational-repression/>.

[194] European Commission, *Communication from the Commission to the European Parliament and the Council - A new EU Framework to strengthen the Rule of Law* (COM(2014) 0158 final), online: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52014DC0158>; see also "Rule of law framework," online: *European Commission* <https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/upholding-rule-law/rule-law/rule-law-framework_en>.

[195] European Parliament, Study for the Committee on Constitutional Affairs (AFCO) Committee, *The EU framework for enforcing the respect for the rule of law and the Union's fundamental principles and values* (January 2019) at page 7, online: <https://www.europarl.europa.eu/RegData/etudes/STUD/2019/608856/IPOL_STU(2019)608856_EN.pdf>.

[196] *Ibid* at page 20.

[197] *Ibid*.

[198] *Ibid* at pages 22-32.

C.7.v. Data Deletion and Retention Obligations

126. Foreign entities that obtain Canadian data through an international production order should be subject to data deletion obligations and associated data retention policies. This would be in accordance with core data minimization principles established in Canadian data protection and privacy legislation,[199] and provide baseline protection to those whose personal information is incidentally collected, but who themselves have nothing to do with the investigation, or who are ruled out early as suspects or persons of interest. Legal experts have noted that incidental collection is a key issue and persistent concern with respect to law enforcement engaging in collection of personal information across borders, such as in the case of section 702 of FISA, as amended, in the United States,[200] or in the context of the US-UK CLOUD Act agreement.[201]

127. Without this amendment, there does not appear to be anything in Bill C-22 to protect the privacy rights of those in Canada whose personal information is transferred to a foreign entity only by virtue of their having communicated with a person being investigated, or if they were wrongly suspected. For example, the *Privacy Act* permits law enforcement in Canada to disclose personal information to foreign governments or foreign law enforcement agencies "under an agreement or arrangement" with a foreign government or its institutions.[202] But as noted above in Part C.4.iii, if Canada were to ratify the 2AP, the treaty would permit Canada to enter into a secret agreement with a foreign government, or Canadian police agencies to make secret agreements with their counterparts across borders on their own, outside of judicial or other formal oversight. Any of these undisclosed arrangements could explicitly eliminate even the minimal data protections available under the treaty.

D. "Voluntary Disclosure" Imports Unconstitutional Third-Party Consent Doctrine

128. Section 487.0195(3) states that law enforcement may "receive any information from a person or a telecommunications service provider" if the person or TSP "without being asked for it, provides it voluntarily." As drafted, this provision could be interpreted to expand law enforcement's ability to engage in the warrantless seizure of information. Given its status as a purported interpretive clause, the provision fails to stipulate that *third parties* are not authorized to provide purported agreement to disclosure on behalf of another individual. In fact, the provision wrongly attempts to suggest that telecommunications providers have the purported authority to disclose *Charter*-protected

[199] See e.g. "PIPEDA Fair Information Principle 4 – Limiting Collection" (13 August 2020), online: *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/principles/p_collection/>.

[200] Brennan Center for Justice, "Reducing 'Incidental' Collection Under FISA Section 702: A Critical Protection for Americans" (October 2017), online (PDF): <https://www.brennancenter.org/sites/default/files/FISASection702ReducingIncidentalCollection.pdf>.

[201] Eddie B Kim, "U.S.-U.K. Executive Agreement: Case Study of Incidental Collection of Data Under the CLOUD Act" (2020) 15:3 Wash J L T & Arts 247.

[202] *Privacy Act*, RSC, 1985, c P-21, s 8(2)(f).

information about their customers to law enforcement. As this Part D outlines, that is not the law in Canada.

D.1. "Voluntariness" Must Not Replace the Law of Consent to Search or Seizure

129. To the extent that the provision is attempting to develop a framework for warrantless collection of private information under Canadian law, the provision is unconstitutional and incoherent at law. It attempts to take merely one part of the longstanding *Charter* law on consent to search or seizure (voluntariness), and tries to flip it into a freestanding authority for the warrantless collection of private information. This makes no sense. It is straightforwardly contrary to the *Charter* to suggest that voluntariness is enough to justify a warrantless search or seizure. Instead, warrantless searches and seizures can become lawful if justified by *consent*, which is well settled in Canadian law. To be valid, that consent must be not only voluntary, but also informed, and importantly, the consent must come from the rightholder whose information is at issue (authority to consent).

130. For example, s. 487.0195(3) would upset the law of consent for witnesses and victims of crime, who often provide sensitive information like their medical records in the course of criminal investigation. They do so after providing law enforcement with consent to the disclosure. However, s. 487.0195(3) would instead suggest that the collection of this information is lawful if the disclosure is merely *voluntary*. This would lower the well-established threshold of consent, and deprive victims of crime of the right to be informed of the consequences of sharing their personal information before consenting to its disclosure.

131. The proposed s. 487.0195(3) is also similar to s. 487.0195(1), but removes the caveat that prevents disclosure where the person is "prohibited by law from disclosing" it. This would create further confusion and uncertainty for information-holders who are bound by statutory obligations to protect information, such as personal health information or other private information. The removal of the caveat appears to invite disclosures of the private information of even a customer or patient, even where such disclosure would violate existing statutory law or regulations.

D.2. Existing Law Enforcement Powers to Receive Information

132. The proposed provision is also wholly unnecessary.

133. For decades in this country, law enforcement authorities have had ample and flexible authorities to receive and act upon information from informants, witnesses, and victims of crime in the course of an investigation. This is a core policing function, and it is inherently reflected in longstanding duties and authorities to receive and act upon information in the course of policing duties. Over time, these longstanding duties have become appropriately balanced by both *Charter* protections (such as where the search or seizure of information engages a reasonable expectation of privacy) and statutory privacy legislation (where personal or deidentified information is concerned). Decades of court rulings, *Criminal Code* reforms, *Privacy Act* investigations, and privacy legislation reforms have developed around this general structure in the balance between privacy rights and law enforcement objectives.

134. For example, it has always been the case in Canada that law enforcement officers have the authority to be informed of knowledge from witnesses or victims of crime,[203] and to use the information received to form grounds to pursue a wide array of search and seizure powers under common law and the *Criminal Code*.[204] Police also have the authority to act in exigent circumstances, and to preserve evidence that is at risk of being lost. Where there is no reasonable expectation of privacy in the information in question, police authorities are even broader, mediated only in accordance with statutory privacy protection where the information constitutes personal or deidentified information.

135. Enacting the proposed s. 487.0195(3) would create chaos in this longstanding balance of powers and privacy rights in Canada, scrambling decades of jurisprudence and law reforms. Quite rightly, the balancing exercise involved in the calibration of the above police powers above unfolded in a contextual and nuanced manner, given how receiving "information" from "persons" could refer to an extraordinarily broad continuum of state-civilian interactions.

136. For example, individuals share access to sensitive information with spouses, healthcare providers, landlords, employers, siblings, fitness or fertility tracking apps, and telecom or Internet service providers. In the 21st century, individuals often have little appreciation of the extent of the data trails they are leaving behind them, or the extent to which their electronic life is easily accessible to a computer-savvy roommate, for example. As the Supreme Court of Canada put it in just one of these spheres, "We are not required to accept that our friends and family can unilaterally authorize police to take things that we share."[205]

D.3. Third-Party Consent to Police Search or Seizure Is Unconstitutional

137. Valid, first-party consent is already lawful authority for law enforcement to receive "information" from a "person." However, as drafted, s. 487.0195(3) would be attempting to do an unconstitutional end-run around the Supreme Court of Canada's repeated rejection of third-party consent under the *Charter*. Third-party consent has roots in the US third-party doctrine (see Part C.4.iv above), which states that individuals abandon constitutional privacy protection for information that is voluntarily shared with a third party. Unlike the United States, since the 1990s, Canada's Supreme Court has rejected the premises of the third party doctrine, and declined to follow related US jurisprudence.[206] Years later in *R. v. Cole*, the Supreme Court also considered and declined to follow the related doctrine of third-party consent in US jurisprudence, and instead ruled that the protections in s. 8 cannot be waived through the consent of a third party.[207]

138. Over the years after the Supreme Court's ruling in *R. v. Cole*, several "variants" of third-party consent reappeared in lower courts in Canada, which "all blurred into the same result: that the

[203] *R v Lambert*, 2023 ONCA 689 at para 58; *R v Molyneaux*, 2020 PECA 2, at para 51.

[204] *R v Bykovets*, 2024 SCC 6 at para 86; *R v Cole*, [2012] 3 SCR 34 at para 73.

[205] *R v Reeves*, 2018 SCC 56 at para 44.

[206] *R v Duarte*, [1990] 1 SCR 30; *R v Wong*, [1990] 3 SCR 36.

[207] *R v Cole*, [2012] 3 SCR 34 at paras 75-79.

'consent' of one individual effectively negates s. 8 protection for another person."[208] These variants were all again rejected or not accepted in the subsequent Supreme Court of Canada decisions in *R. v. Reeves*, and *R. v. Bykovets*.[209]

139. Section 487.0195(3) represents yet another one of the unconstitutional "variants" by which the federal government, through Bill C-22, is attempting to circumvent the longstanding prohibition on third-party consent. This time, the provision is premised upon the incoherent—and previously rejected[210]—concept that law enforcement is not engaged in "state action" if they seize and/or search information that was voluntarily offered by a third party.[211]

140. Stipulating that law enforcement had not "asked" for the information does not mean that s. 8 *Charter* rights are not engaged. As the Court of Appeal for Ontario already described, this is "an artificial view of what state action entails," and one which is unnecessary given the wide array of police powers that the courts already turn to where third parties are cooperating with the police. The Attorney General of Ontario also previously urged the Supreme Court of Canada against this concept, cautioning that it would invite an inappropriate cat-and-mouse game:

> Police interactions with members of the public are far too nuanced to draw this kind of constitutional line. And, if this line were drawn, it would inevitably devolve into a cat-and-mouse game in which the investigating officer would tell the individual, "I'm not allowed to *ask* for access to your shared data, but if you were to *offer* access to me I would be very happy to accept..." This Court's interpretation of s. 8 should not invite this sort of game-playing.[212]

141. Parliament has already crafted a warrantless seizure power under s. 489(2) of the *Criminal Code*, to enable a seizure pending authority to carry out a search.[213] The warrantless provision requires reasonable grounds of belief. Law enforcement also have authorities to receive information from a person who is consenting to its disclosure, so long as the information is not the subject of a reasonable expectation of privacy of another person.[214] Even where the information does engage such reasonable expectation of privacy of another person, as described above, the law has already provided for numerous investigative options and powers through which police may receive information from victims and witnesses of crime, rendering the proposed provision in Bill C-22 superfluous as well as detrimental. By now attempting to suggest that all forms of "voluntary" disclosure—moreover third-

---

[208] Kate Robertson, "Investigative Genealogy and the Charter: Consent, the Immutability of DNA, and Canada's Arriving Future," (2025) 73(4) CLQ 471 at 502.

[209] *Ibid* at pages 500-503; *R v Reeves*, 2018 SCC 56, at paras 41, 44, 52-53; *R v Bykovets*, 2024 SCC 6 (where an IP address had been provided to police by a service provider voluntarily).

[210] See *R v Cole*, [2012] 3 SCR 34 (where it was unconstitutional for the police to search a computer that had been willingly provided by a school teacher's employer; the computer had been provided to the police without any police request for the computer and the taking of a computer constituted a seizure); *R v Dyment*, [1988] 2 SCR 417 (it was unconstitutional for a police officer to take a blood sample that a doctor had willingly provided; there was no evidence that the sample had been "requested" by the police); *R v Lambert*, 2023 ONCA 689 at paras 66-73.

[211] "Bill C-22: An Act respecting lawful access" (Charter Statement) (24 April 2026), online: *Department of Justice Canada* <https://www.justice.gc.ca/eng/csj-sjc/pl/charter-charte/c22_2.html>.

[212] Attorney General of Ontario, Factum of the Respondent (23 April 2018), *R v Reeves*, 2018 SCC 56 at para 86 (emphasis in original).

[213] *Criminal Code*, RSC 1985, c C-46, s 489(2).

[214] *R v Lambert*, 2023 ONCA 689 at paras 56-63.

party disclosure—can justify a warrantless search and seizure authority, s. 487.0195(3) is grossly overbroad, and would unjustifiably upend this important and contextually balanced area of law. In doing so, if s. 487.0195(3) were to pass, it would wreak havoc on many years of stable court jurisprudence until the provision is inevitably subject to constitutional challenge.

D.4. "Voluntary" Provision of Commercially Available Information

142. Enacting s. 487.0195(3) as drafted would also risk further opening Canada's floodgates to the growing array of data-mining and other expansive data collection and analytics practices by private-sector data brokers and surveillance vendors who "voluntarily" offer law enforcement sensitive data sets, or other forms of disclosures that the Supreme Court has previously ruled were unconstitutional.[215]

143. If the "voluntariness" provision is retained in Bill C-22, it must be defined to exclude the "voluntary" provision of any commercially available information ("CAI") by vendors, as defined in Part B.3 above. That definition includes the provision of CAI through free trials and demos, even if no money is exchanged nor any contract signed. Otherwise, privacy rights under section 8 would be subordinated to surveillance companies' profit motive to secure lucrative contracts with law enforcement, a clientele around which many such companies build significant parts of if not their entire business models.[216] For example, Toronto Police Service's use of Clearview AI's facial recognition software occurred through a free trial,[217] and Amazon Ring, in the US, "sent police ambassadors fliers and discount codes in return for promoting the company's products in their communities" and "gave participating police departments access to maps of active cameras."[218]

144. Companies may also conduct product demonstrations for law enforcement in ways that may be considered voluntarily providing information "without being asked," but which, however inadvertently, could result in warrantless searches of surveilled private or semi-private spaces. The company Flock, for instance, which sells automated license plate reader ("ALPR") cameras, used a city's live cameras to demonstrate their capabilities to prospective customers, without first ensuring that the cameras accessed for demonstrations would not be those placed in sensitive areas, such as locations specific to children or religious communities.[219]

---

[215] See *R v Cole*, [2012] 3 SCR 34 (where it was unconstitutional for the police to search a computer that had been willingly provided by a school teacher's employer; the computer had been provided to the police without any police request for the computer and the taking of a computer constituted a seizure); *R v Dyment*, [1988] 2 SCR 417 (it was unconstitutional for a police officer to take a blood sample that a doctor had willingly provided; there was no evidence that the sample had been "requested" by the police); *R v Lambert*, 2023 ONCA 689 at paras 66-73.

[216] See e.g. *Clearview AI Inc v British Columbia (Information and Privacy Commissioner)*, 2026 BCCA 67 at paras 61, 95-96.

[217] Nicole Brockbank, "Toronto police used Clearview AI facial recognition software in 84 investigations," *CBC* (23 December 2021), online: <https://www.cbc.ca/news/canada/toronto/toronto-police-report-clearview-ai-1.6295295>.

[218] Grace Griffin, "Ring says police partnerships help solve crimes. What does it mean for your privacy?" *WBUR* (30 September 2025), online: <https://www.wbur.org/hereandnow/2025/09/30/ring-police-partnerships>; see also Louise Matsakis, "Cops Are Offering Ring Doorbell Cameras in Exchange for Info," *Wired* (2 August 2019), online: <https://www.wired.com/story/cops-offering-ring-doorbell-cameras-for-information/>.

[219] Jason Koebler, "City Learns Flock Accessed Cameras in Children's Gymnastics Room as a Sales Pitch Demo, Renews Contract Anyway," *404 Media* (30 April 2026), online: <https://www.404media.co/city-learns-flock-accessed-cameras-in-childrens-gymnastics-room-as-a-sales-pitch-demo-renews-contract-anyway/>.

145. Beyond commercial entities, Part C.1 of this brief discussed how s. 487.0195(3) also combines clauses related to warrantless collection of information pursuant to the law of a foreign state. As noted there, the provision as a whole is vague, and capable of being interpreted in multiple ways.[220] It is also unclear why the provision is necessary or appropriate, given the absence of transparency regarding Bill C-22's relationship to potentially multiple data-sharing treaties. This provision should not pass until these drafting errors are remedied, and the ambiguities are satisfactorily resolved. These problems, combined with those reviewed in this Part D, impair the entirety of s. 487.0195(3).

146. As a result of the issues set out in this and all of the above subsections, we **recommend** that s. 487.0195(3) of Bill C-22 be removed from the bill, given it is unnecessary and would inherently destabilize the well-established law of consent to search. If the provision were to be retained, it must be amended by:

    a. replacing the concept of voluntary disclosure with consent to disclosure;
    b. adding a caveat to ensure that any disclosure is limited to that which is not prohibited by law; and
    c. add language to clarify that the "information" referred to in section 487.0195(3) does not include information in which a Canadian or person in Canada, other than the person providing the consent, has a reasonable expectation of privacy, unless the peace officer or public officer is authorized by law to receive that information without a production order, warrant, or confirmation of service demand made under section 487.0121.

[220] For example, it is unclear whether the proposed underlined phrasing modifies the voluntary provision clause of s. 487.0195(3), or also the "law of a foreign state" clause: ."..if the person, without being asked for it, provides it voluntarily or is required by law, including a law of a foreign state, to provide it" (emphasis added).

E. Table of Recommendations

147. We compile here all of our recommendations for Bill C-22 from Parts A through D above:

Recommendations for Part 2 (SAAIA)	
Rec. 1	Delete the definition of "electronic service" and replace the definition of "electronic service provider" in section 2(1) of the SAAIA with the following: a. electronic service provider means a person that, individual or as part of a group, is a telecommunications common carrier within the meaning of the Telecommunications Act that b. provides services in Canada; or c. carries on all or part of its business activities in Canada.
Rec. 2	Replace section 5(2) of SAAIA so that it can only obligate telecommunications carriers to develop wiretapping capabilities and clarify that these rules cannot require a "specific design of equipment, facilities, services, features or system configurations."
Rec. 3	Add the following sub-provision to sections 5 and 7 of SAAIA: (#) No order or regulation shall be made that would have the effect of degrading, removing, defeating or bypassing any technical safeguard including encryption.
Rec. 4	Delete paragraph 47(1)(c) of SAAIA.
Rec. 5	Replace the current text of section 5(3) of SAAIA with the following text: In making a regulation under subsection (2), the Governor in Council must demonstrate that there are reasonable grounds to believe that: a. the obligation in question is strictly necessary to the investigation of a serious offence as defined in section 467.1(1) of the *Criminal Code* or to the security of Canada as defined in section 2 of the *CSIS Act*; b. the objectives of the obligation imposed cannot be achieved by less intrusive means; c. any potential impact, including specifically to cybersecurity and to the right to privacy, is demonstrably proportionate to the objectives of the obligation; and d. the obligation does not require an ESP to do anything that can be accomplished through an existing power.
Rec. 6	Replace the current text of section 7(3) of SAAIA with the following text: In making an order under subsection (1), the Minister must demonstrate that there are reasonable grounds to believe that: a. the obligation is strictly necessary to the investigation of a serious offence as defined in section 467.1(1) of the *Criminal Code* or to the security of Canada as defined in section 2 of the *CSIS Act*; b. the objectives of the obligation imposed cannot be achieved by less intrusive means;

	c. <u>any potential impact, including specifically to cybersecurity and to the right to privacy, is demonstrably proportionate to the objectives of the obligation; and</u> d. <u>the obligation does not require an ESP to do anything that can be accomplished through an existing power.</u>
Rec. 7	Remove the following from sections 5(3) and 7(3) of SAAIA: "(f) any other factor that the Governor in Council considers relevant"
Rec. 8	Require regulations (s. 5) and orders (s. 7) to expire after one year.
Rec. 9	Remove the data retention regime by deleting s. 5(2)(d) of SAAIA. In the alternative, amend 5(2)(d) of SAAIA so as to: a. limit it to preservation of data already under a service provider's control for 30 days; b. limit the application of the regime to telecommunications carriers; c. specify what categories of data can be required to be preserved in the text of the statute; and d. ensure that these exclude any type of tracking data as defined in s. 487.011 of the *Criminal Code*, with the possible exception of requiring telecommunications carriers to preserve cell tower interaction records.
Rec. 10	Add an amendment to prohibit companies from using or disclosing mandatorily retained or preserved data for any reason other than responding to state requests that relate to investigations of serious offences or to activities that threaten the security of Canada.
Rec. 11	Require companies to delete retained or preserved information once the retention or preservation window closes unless a preservation order is issued under the *Criminal Code*.
Rec. 12	Limit obligations imposed through the SAAIA to an ESP's own services.
Rec. 13	Add a provision to the SAAIA establishing that ESPs cannot be compelled to deceive or mislead their customers or the public.
Rec. 14	Add the following amendments regarding Ministerial orders and regulations: a. require authorization by the Federal Court as a precondition for the issuance of any regulation, order, or compliance order under the SAAIA and encoding a full right to *de novo* review before the Federal Court for any relevant stakeholder; b. amend s. 15 of SAAIA so that information may be kept confidential only to the extent it is demonstrably necessary to preserving the integrity of an investigative technique; and c. require public notification of all orders at least 30 days before they come into effect.
Recommendations for Part 1	
Rec. 15	Remove the entirety of section 487.0195(4).

	In the alternative, add to section 487.0195(4) language expressly clarifying that the definition of "publicly available information" (PAI) excludes all of the following: a. information in which there is a reasonable expectation of privacy; b. personal information that has been unlawfully collected or disclosed; and c. commercially available information [defined as proposed in Part B.3 above].
Rec. 16	Remove the entirety of section 487.0195(3). In the alternative, amend section 487.0195(3) in the following ways: a. replace the concept of "voluntary" disclosure with "consent to disclosure"; b. add a caveat to ensure any such disclosure "is not prohibited by law"; and c. add language to clarify that the "information" referred to in section 487.0195(3) <u>does not include information in which a Canadian or person in Canada, other than the person providing the consent, has a reasonable expectation of privacy, unless the peace officer or public officer is authorized by law to receive that information without a production order, warrant, or confirmation of service demand made under section 487.0121</u>.
Recommendations for Foreign Law Enforcement Access to Data	
Rec. 17	The Government of Canada must issue a public explanation regarding its intentions concerning the Second Additional Protocol, a potential Canada-US CLOUD Act agreement, and how Bill C-22 relates to either or both of these agreements. The federal government must also commit to complying with the *Policy on Tabling of Treaties in Parliament*. Suspend SECU's study of Part 1 of the bill until after the government has completed the above.
Rec. 18	Amend the bill to add the following safeguards to sharing data with foreign entities, as discussed in Part C.7: a. dual criminality requirement; b. exclusion of political offences or if politically motivated; c. exclusion if discriminatory purpose on basis of protected characteristics; d. requirement to engage in rule-of-law assessment and assessment of human rights track record; and e. data deletion and retention obligations.