(Un)Forced Errors: Analysis of Proposed Surveillance Law Expansion under Bill C-22, *An Act respecting lawful access*

Executive Summary

Submitted to the House of Commons Standing Committee on Public Safety and National Security (SECU) in its study of Bill C-22, *An Act respecting lawful access*

June 2, 2026

AUTHORS

Cynthia Khoo | Senior Fellow, Citizen Lab, Munk School of Global Affairs & Public Policy, University of Toronto
Tamir Israel | Director, Privacy, Surveillance & Technology Program, Canadian Civil Liberties Association (CCLA)
Kate Robertson | Senior Research Associate, Citizen Lab, Munk School of Global Affairs & Public Policy, University of Toronto

Executive Summary

NOTE: This submission is an executive summary of a detailed analysis of Bill C-22, *An Act respecting lawful access*.[1] The full submission can be read at: https://citizenlab.ca/research/analysis-of-proposed-surveillance-law-expansion-under-bill-c-22

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"), and enacts a broad-ranging regime for imposing surveillance obligations onto electronic service providers, including building technical capabilities they may not already have. The bill effectively reintroduces what were formerly Parts 14 and 15 of Bill C-2, the *Strong Borders Act*, with modifications. While the government made efforts to address some of the problematic elements of Bill C-2, several deeply concerning issues remain, and other concerns have been exacerbated by the broadening of certain elements of the earlier proposed legislation. More than one aspect of the bill is almost certainly constitutionally fatal.

2. In this submission, we provide targeted analysis and recommendations focused on aspects of Bill C-22 with pressing and far-reaching implications. Due to the stringent timeline imposed on the House of Commons Standing Committee on Public Safety and National Security's ("SECU") legislative study of the bill, the analysis provided in this submission is far from exhaustive. Indeed, there are highly problematic elements of this legislative proposal that are not addressed in this analysis at all, in light of the time constraints.

3. In fact, the extreme fast-tracking of this bill by the government is itself cause for concern and reason to question whether the committee process is capable of remedying the legislative proposal's many flaws. 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 the technical surveillance capability regime proposed in Part 2 of this bill was subject to no less than 173 amendments before being passed.[2] Yet the government has allotted barely three weeks to the committee's study of this bill. The government's failure to confirm in advance the interaction between Bill C-22 and pending international information-sharing agreements as it is required to do is a further procedural flaw that has severely impeded the effective legislative study of this proposal.

4. While the submission provides amendments that might mitigate some of the destructive consequences of Bill C-22, our core recommendation is that the offending elements of the Bill be withdrawn. The government must also comply with its own treaty-implementation transparency policy prior to any of the bill's provisions related to a foreign data-sharing agreement moving forward.

SAAIA Creates an Untenable Risk to Privacy & Cybersecurity

5. In **Part A** of our submission, we address how Bill C-22 would enact the *Supporting Authorized Access to Information Act* ("SAAIA") under Part 2 of the bill. The proposed SAAIA would create a surveillance capability regime by which the government can impose any obligation onto any electronic service provider

---

[1] Cynthia Khoo, Kate Robertson & Tamir Israel, "(Un)forced Errors: Analysis of Proposed Surveillance Law Expansion under Bill C-22, An Act respecting lawful access", Joint Analysis: *Citizen Lab & Canadian Civil Liberties Association*, (June 2026), <https://citizenlab.ca/research/analysis-of-proposed-surveillance-law-expansion-under-bill-c-22/>.

[2] 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>.

("ESP") for the purpose of facilitating lawful use of surveillance authorizations. These obligations could include requiring ESPs to change how they operate or to embed surveillance tools in their services. In addition to this surveillance capability regime, SAAIA also includes a mandatory metadata retention regime that the government could potentially use to require any ESP to access, record, and keep sensitive metadata within their reach on every person in Canada or abroad for up to one year.

6. 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 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. With a growing arsenal of "AI"-based[3] surveillance techniques on the horizon, SAAIA's potential for intrusiveness will grow apace.

7. SAAIA's data retention mechanism is almost certainly unconstitutional. It lets the government obligate any ESP to keep metadata indiscriminately without any need to demonstrate that the person is involved in any wrongdoing. Metadata is not defined, but is at the least likely to include a record of who each person interacted with, detailed tracking of every single person's movements, and an overview of every application a person has used. Metadata can be extremely sensitive. One analysis that was limited to people's call records found that "there are significant privacy impacts associated with telephone metadata" which "trivially gives rise to…sensitive inferences", including political perspectives, religious views and more.[4] Canadian privacy laws place strict limits on what metadata companies can collect,[5] but SAAIA would override these limitations while placing no limits on when that data might be accessed or for what purpose.

8. The government has presented SAAIA as necessary to align Canada with its Five Eye partners. But half of Canada's Five Eye partners have nothing approaching SAAIA. New Zealand and the United States ("US") do not have mandatory data retention requirements at all, and have surveillance capability regimes that are limited to imposing wiretapping obligations on Internet access and telephone companies.[6]

---

[3] For purposes of this submission, 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/>.

[4] 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>.

[5] 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>.

[6] 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>.

9. Two of the Five Eyes, Australia and the United Kingdom (UK) do have regimes that approach SAAIA's breadth. But 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.[7] As a result of this order, Apple has removed a critical encryption safeguard for iCloud backups ("Advanced Data Protection") for any Apple devices connecting from the UK. While Australian laws cannot be challenged for violating human rights in court, the Parliamentary Joint Committee on Human Rights held that the Australian surveillance capability regime was "incompatible with [human] rights" due to being "unlikely to constitute a proportionate limitation on the rights to privacy and freedom of expression" in its mandatory assessment of the legislative proposal.[8]

10. Even narrower surveillance 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.[9] 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.[10] 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.[11] Technical modifications made in compliance with these obligations are also notoriously difficult to secure. When the US National Security Agency (NSA) tested equipment that complied

---

[7] 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/>.

[8] 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>.

[9] "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>.

[10] 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>.

[11] 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-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/>.

with the US surveillance capability law, CALEA,[12] it found that "every single switch it tested had a security flaw".[13] The NSA and other foreign intelligence agencies have also recognized that surveillance capability regimes are lucrative targets for exploitation,[14] making these requirements even more difficult to implement in a secure manner.

11. Governments today generally recognize the importance of cybersecurity and encryption.[15] 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.[16] 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.

12. Against this backdrop, SAAIA represents a troubling framework through which the government will be able to impose its evolving surveillance priorities. In light of the speed at which the study of Bill C-22 is proceeding, our core recommendation is to entirely withdraw Part 2 of the bill. As presented, SAAIA 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 an oversight framework that is designed for foreign intelligence and, as a result, is heavily shielded from stakeholder input, judicial control and public accountability. 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.

Provisions on publicly available information & voluntary disclosure are inconsistent with Canadian Charter jurisprudence

13. In **Parts B and D** of this submission, we recommend that the provisions that purport to clarify the law, "for greater certainty", regarding "publicly available information" and the "voluntary provision" of information both be removed from the bill. Both provisions involve 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

---

[12] Communications Assistance for Law Enforcement Act (CALEA), 47 USC 1002.

[13] 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>.

[14] 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>.

[15] 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/>.

[16] 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>.

jurisprudence. In the event these provisions are not removed, again we provide suggested amendments, purely as a mitigatory measure.

14. Bill C-22 proposes to add a provision to the *Criminal Code* that indicates "for greater certainty" that law enforcement do not require a production order or warrant for information that is available to the public. By treating the public character of information as determinative of any constitutionally protected privacy interest, the provision creates a framework that flies in the face of decades of Canadian *Charter* jurisprudence, which has consistently recognized public information is not categorically exempt from section 8 protection.

15. Embedding this framework in the *Criminal Code* 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. This approach raises additional problems for failing to exclude information that was initially collected or became public through unlawful means. A number of Canadian police agencies were found to have used Clearview AI's intrusive facial recognition application even though the company's facial recognition database was created in violation of Canada's privacy laws.[17] As more and more of our personal information becomes publicly available, as a condition of participating in today's digitized society, and often without our knowledge or consent,[18] it is all the more crucial that the bill not embed a framework premised on the notion that no privacy protection exists for information in public view.

16. Another provision in Bill C-22 indicates "for greater certainty" that no authorization is required for police to receive information that is being voluntarily or proactively disclosed. This provision is similarly out of line with existing *Charter* jurisprudence, particularly in relation to third party consent (where one person is consenting to a search or seizure of another person's information). Canadian case law has consistently rejected third-party consent as a means of waiving section 8 protections. The categorical framework put in place by Bill C-22 poses a particularly dire threat to privacy if commercial service providers are permitted to waive the privacy rights of their users and proactively disclose their personal information to police.

Bill C-22's connection to international data-sharing agreements must be disclosed

17. Finally, in **Part C** of this submission, we outline how 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. 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

---

[17] 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>; 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 *Clearview AI Inc v British Columbia (Information and Privacy Commissioner)*, 2026 BCCA 67.

[18] See e.g. 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>; 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>; 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>; and 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/>.

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.

18. 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."[19]

19. 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.[20] The agreement would be established under a piece of US legislation called the Clarifying Lawful Overseas Use of Data Act ("CLOUD Act").

20. Canadian officials have previously linked the proposed surveillance reforms, when they were presented in Bill C-2, to the United States.[21] However, the federal government has not provided the public or Parliament with an explanation concerning why the United States has been pressing Canada to pass the surveillance reforms in Bill C-2 that have now been re-introduced in Bill C-22 almost a year later.

21. 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", and noted that they look forward to Canada's "prompt collaboration" on reaching a CLOUD Act agreement.

22. Our analysis identifies numerous areas of overlap between Part 1 of Bill C-22's proposed provisions and anticipated areas of law reform required to advance Canada's ability to enter into one or both of the above treaties. We then discuss a host of constitutional and human rights issues that would arise from either or both agreements, or from the general prospect of Canadian service providers sharing the personal data of those in Canada with foreign law enforcement entities as envisioned in the bill.

23. The foremost issue is that Canadian constitutional law provides stronger protection for human rights than that of many signatories to the 2AP, including the United States. This is particularly the case with respect to protection of privacy rights, freedom of expression, and the right to equality and freedom from discrimination, all of which are guaranteed under the *Charter*. Entering into a Canada-US CLOUD Act agreement would threaten to water down Canada's constitutional standards. Joining the 2AP would mean playing a role in diluting international human rights standards, while also enabling Canadian law enforcement agencies to enter into secret agreements with their foreign counterparts to ignore the few privacy protections in the treaty. Through either, Canada could become complicit in human rights violations perpetrated by the US or other foreign governments that criminalize activities that are lawful or constitutionally protected under Canadian law.

---

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

[20] 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>.

[21] 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 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 FISA warrants, the Patriot Act". 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> .

24. In addition, the personal information of targeted individuals in Canada would be handed over to legal regimes with weaker privacy laws or which do not consider themselves legally obligated to protect that person, their human rights, or their information. These treaties also provide no legal recourse or remedy for those whose privacy or other constitutional rights are violated in the process of Canada transferring their personal data to foreign law enforcement agencies, or for violative consequences resulting from that transfer.

25. 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 the people whose information it is—will remain protected, once shared with foreign entities, at the level guaranteed by Canadian constitutional, human rights, and privacy laws. This is despite the fact that 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*.

26. We therefore 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 consequential repercussions of what Bill C-22 appears to be laying the groundwork for, including a more closely interlocked law enforcement system and legal regime with the US. The Canadian government should be required to provide full transparency regarding Canada's potential adoption of both the 2AP and a Canada-US CLOUD Act agreement. In the event the government persists in either or both of these agreements, we recommend several necessary safeguards that must be added as amendments to Bill C-22, to ensure a minimum baseline of human rights protections applies to any data-sharing with foreign law enforcement.

Conclusion

27. Bill C-22 contains significant flaws and its legislative study has been marred by procedural defects that have impeded any meaningful attempt to address those flaws through the legislative process. As this submission demonstrates, many of the provisions Bill C-22 would enact will have far-reaching implications, with detrimental impacts that could be in effect for decades to come, even if any of these provisions are repealed as the result of inevitable constitutional challenges. In addition to those overarching concerns, this analysis offers 18 recommendations in respect of the draft legislation, which we consider to be integral to addressing the proposed bill's sweeping scope, its correspondingly significant risks to constitutional and human rights, transparency and accountability deficits in the legislation, and the dangers it poses to cybersecurity and encryption in Canada's information and communication networks.

Table of Recommendations

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: 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 a. provides services in Canada; or b. 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. 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. 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.