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

Updated Summary

Submitted to the Senate Standing Committee on National Security, Defence and Veteran Affairs (SECD) in its study of Bill C-22, *An Act respecting lawful access*

November 19, 2026

AUTHORS

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
Cynthia Khoo | Senior Fellow, Citizen Lab, Munk School of Global Affairs & Public Policy, University of Toronto

Updated Summary

NOTE: This submission is an updated supplement to a detailed analysis which was prepared for 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*. This submission includes updated and additional recommendations which draw heavily from the initial analysis, but we note that we continue to maintain our recommendations from the originally published detailed analysis.[1]

1. Bill C-22, the *Lawful Access Act*, proposes a range of new surveillance authorizations and enacts a broad-ranging regime for imposing surveillance obligations onto electronic service providers, including building technical capabilities they may not already have and the obligation to record sensitive metadata and all users of a service and keep it for up to six months.

2. Modifications to Bill C-22 during the attenuated study it received before the House of Commons failed to address core concerns raised by the proposal. Several deeply concerning issues remain, and more than one aspect of the bill remains almost certainly constitutionally fatal and inconsistent with Canada's international human rights obligations.

3. In this submission, we provide targeted analysis and recommendations focused on aspects of Bill C-22 with pressing and far-reaching implications. 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of the destructive consequences of Bill C-22, our core recommendation is that the offending elements of the bill be withdrawn.

4. Elements of part 1 of Bill C-22 are enabling legislation for international information-sharing agreements, yet the government has not provided parliament with the details necessary to understand how Bill C-22 will interact with these agreements. The government should comply with its own treaty-implementation transparency policy before any of the bill's provisions related to a foreign data-sharing agreements move forward.

5. At a time of escalating and unprecedented digital security threats, part 2 of Bill C-22 is designed to prioritize surveillance at the cost of every person's cybersecurity. We are at an inflection point where powerful commercial spyware and AI-fueled cyber attack capabilities that threaten even the most advanced state-backed cybersecurity agencies in the Five Eyes alliance are becoming available to an increasing number of threat actors. Canada's networks are being probed, targeted, and tested for weaknesses on a daily basis. Yet instead of putting cybersecurity first, Bill C-22 will weaken the integrity and security of the digital tools we all rely on most.

6. While the government has stated that part 2 of Bill C-22 is intended to align Canada with its international counterparts, this is simply not the case. Part 2 of Bill C-22 falls short of international human rights standards and conflicts with binding decisions of the European human rights system while extending well beyond what our Five Eye partners have in place. Indeed, Bill C-22 has drawn criticism from European civil society groups and businesses, who have called on government leaders to limit Bill C-22's blanket metadata retention regime and threats to encryption.[2] This misalignment jeopardizes Canada's ongoing attempts to foster greater partnerships with Europe, including its emphasis on a new digital integration agreement. Indeed, the Court of Justice of the European Union has in the past rejected agreements between Canada and the EU where Canada's framework failed to meet EU human rights standards.[3]

---

[1] Cynthia Khoo, Tamir Israel & Kate Robertson, "(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/ ("Citizen Lab/CCLA Analysis of Bill C-22").

[2] United Nations, Office of the High Commissioner for Human Rights, Advisory Service on Digital Technologies, Comments on Canadian draft Bill C-22", November 3, 2026, https://ccla.org/wp-content/uploads/2026/11/2026.11.03-UN.OHCHR-C22.Assessment.pdf; "Open letter from European civil society organisations on encryption and privacy threats in Canada's Bill C-22", (September 2026), https://www.accessnow.org/press-release/encryption-and-privacy-threats-in-canadas-bill-c-22/; and "Canadian and European Tech Warns Bill C-22 Would Undermine Privacy and Security", Chamber of Progress (September 2026), https://progresschamber.org/news/canadian-and-european-tech-warns-bill-c-22-would-undermine-privacy-and-security/.

[3] Opinion 1/15, July 26, 2017 (CJEU, Grand Chamber); "Open letter from European civil society organisations on encryption and privacy threats in Canada's Bill C-22", (September 2026), https://www.accessnow.org/press-release/encryption-and-privacy-threats-in-canadas-bill-c-22/; and Kate Robertson, "The Lawful Access Act threatens to blow a hole in Canada's national security", *The Globe and Mail*, 9 October 2026, https://www.theglobeandmail.com/opinion/article-the-lawful-access-act-threatens-to-blow-a-hole-in-canadas-national/.

7. We elaborate on these concerns below, drawing heavily on our more comprehensive analysis of Bill C-22 as initially presented in parliament.

SAAIA Creates an Untenable Risk to Privacy & Cybersecurity

8. Part 2 of Bill C-22 would enact the *Supporting Authorized Access to Information Act* ("SAAIA"). The proposed SAAIA would create a surveillance by design regime by which the government can impose any technical obligation onto any electronic service provider ("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 under which the government could compel any ESP to access, record, and keep sensitive metadata within their reach on every person in Canada or abroad for up to six months.

9. Our core recommendation is therefore to entirely withdraw Part 2 of the bill so that it can be reconsidered. Below, we recommended some amendments to SAAIA that should be viewed as a last-resort measure provided in the spirit of harm reduction and to better ensure that the government's stated objective of aligning Canada with its Five Eye counterparts extends to incorporating the safeguards and limitations in these other regimes alongside their powers. It should not be taken as an indicator that Part 2 is acceptable.

10. Overall, SAAIA provides the government with maximum flexibility, minimal restrictions, and minimal judicial and public scrutiny–an unacceptable combination and one that makes the proposed legislation unfit for purpose. It effectively grants the government carte blanche to prioritize surveillance over the security of our most fundamental digital tools for decades to come, and to do so in secret. Its unparalleled breadth is intended to capture every current or future digital entity, and to provide the government with maximum flexibility to impose any obligation on these. Notably, SAAIA is not limited to communications providers, but applies to any digital entity, including operating systems and other entities.[4] For example, the bill's application to developers of AI chatbots opens the door to "compelling AI agents to work for the police rather than for users,"[5] and forcing retention of metadata concerning how AI agents are being used by individual users. Nothing in the bill would prevent companies such as OpenAI from turning around and commercializing the data collected about individual users. Given the long term implications of this regime, it is critical to get it right.

11. In light of the severe threat SAAIA poses to privacy, cybersecurity and encryption, the legislation in its current form has received a cross-cutting chorus of opposition. Calls to fix SAAIA have come from:

    - civil liberties groups,[6]
    - other civil society and human rights groups including those dedicated to journalism, education, health, labour, migrant justice, and gender equality;[7]
    - the legal community;[8]

---

[4] By contrast, surveillance by design regimes in the US and New Zealand are limited to imposing "lawful intercept" (wiretapping) obligations onto phone and Internet providers, whereas surveillance by design regimes in the UK and Australia are limited in application to communications providers. See, e.g. UK, IPA 2016, ss 261(10)-(11).

[5] Kate Robertson, "The Lawful Access Act threatens to blow a hole in Canada's national security", *The Globe and Mail*, 9 October 2026, https://www.theglobeandmail.com/opinion/article-the-lawful-access-act-threatens-to-blow-a-hole-in-canadas-national/.

[6] Canadian Civil Liberties Association & Researchers at Citizen Lab, International Civil Liberties Monitoring Group, OpenMedia, British Columbia Civil Liberties Association, Amnesty International; Ligue des droits et libertés, Canadian Muslim Public Affairs Council, Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic, the Centre for Free Expression, Canadian Constitution Foundation, Privacy & Access and Council of Canadians, and the David Asper Centre for Constitutional Rights.

[7] Canadian Association of Journalists, Canadian Life and Health Insurance Association, Canadian Association of University Teachers (CAUT), Canadian Anti Monopoly Project (CAMP), Canadian Council for Refugees, LEAF, Migrants' Rights Network, Migrant Workers' Alliance for Change, Canadian Labour Congress, Clinique pour law justice migrante, the Ontario Council of Agencies Serving Immigrations (OCASI) and the Community Justice Collective (CJC), Crypto Québec, and Chayn.

[8] The Canadian Bar Association; David Fraser, Partner, McInnes Cooper; Dr. Michael Geist, Canada Research Chair in Internet and E-Commerce Law, Professor of Law, Faculty of Law, University of Ottawa; Prof. Robert Diab, Professor, Faculty of Law, Thompson Rivers University; Michael Karanicolas, Associate Professor of Law and Palmer Chair in Public Policy & Law, Schulich School of Law, Dalhousie University; Lisa Austin, Professor of Law, Jackman Law, University of Toronto; Steve Coughlan, Professor of Law, Schulich School of Law, Dalhousie University; Teresa Scassa, Canada Research Chair in Information Law and Policy, University of Ottawa; Matt Malone, Balsillie

- providers of secure digital tools, cybersecurity mitigation services, technology companies, and open source technical tools, internet companies, internet associations and technical standards bodies;[9]
- cybersecurity experts and technologists;[10]
- digital rights groups and experts from the EU and around the world;[11]
- independent regulators;[12]
- U.S. congressional committees and a U.S. senator;[13] and
- the UN Office of the High Commissioner for Human Rights.[14]

The legislation's threat to cybersecurity has been a particular focal point for criticism, with the importance of ensuring the bill is not later used to weaken or bypass encryption a key recurring theme.[15] The Canadian public is similarly opposed to this element of SAAIA, with a recent survey finding that people in Canada overwhelmingly believe they have the right to private conversations and that they are broadly opposed to allowing law enforcement access to encrypted messages.[16] Bill C-22 in its current form continues to pose an untenable threat to encryption.

12. Governments today generally recognize the importance of cybersecurity and encryption.[17] 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–these are not hypothetical examples, but concrete proposals that have been advanced by Canadian and other government agencies at various points in time.[18] When initially advanced, these proposals are never presented as a "backdoor" or an attempt to

---

Scholar, Balsillie School of International Affairs; Katie Szilagyi, Associate Professor of Law, University of Manitoba; Matthew Dylag, Assistant Professor of Law, Schulich School of Law, Dalhousie University; Suzie Dunn, Assistant Professor of Law, Schulich School of Law, Dalhousie University.

[9] Signal, the Canadian Chamber of Commerce, Apple Inc., Google Inc., Meta Platforms Inc., Shopify, Psiphon, Windscribe, Proton (Proton VPN, Protonmail), NordSecurity (NordVPN, NordPass), Coinbase Canada, Figment Inc., Tailscale Inc., Tuta, Kape Technologies Plc (ExpressVPN, Private Internet Access), the Rum Group (Rumble), Association for Competitive Technology, TECHNATION Canada, Canadian American Business Council, the Chamber of Progress, Réseau Koumbit, and the Business Software Alliance (whose members include Cohere, Salesforce, Cisco and OpenAI), and the Software & Information Industry Association, the Internet Architecture Board, the Information Technology Industry Council, the Internet Infrastructure Coalition, Mozilla, DuckDuckGo, the Tor Project, and Canada-based Tucows (and others already listed in footnote 8); and internet.works (which includes eBay, Dropbox, Discord, Etsy, Expedia, Flickr, Intuit, Pintrest, Reddit, Roblox, Tripadvisor, Yelp, Zoom and others).

[10] The Global Encryption Coalition, the Cybersecurity Advisors Network, Tech Workers Coalition Canada, Technologists for Democracy, Susan Landau, Ian Goldberg, Peter Swire, Michael Specter, and Douglas Stebila.

[11] European civil society organizations, including Access Now, ARTICLE 19, European Digital Rights (EDRi), Bits of Freedom, Digitalcourage, Electronic Frontier Norway, Epicenter.works – for digital rights, ESWA, Homo Digitalis, Initiative für Netzfreiheit, IT-Pol Denmark, Liga voor Mensenrechten vzw, Open Rights Group, Osservatorio Nessuno OdV, SHARE Foundation, Stop Killing the Internet; and other digital rights groups and experts around the world, including the Electronic Frontier Foundation; the Internet Society, the Center for Democracy & Technology, Fight for the Future, Global Partners Digital, and Cory Doctorow.

[12] The Office of Privacy Commissioner of Canada and the Intelligence Commissioner.

[13] Chairs of the U.S. House Judiciary and Foreign Affairs Committees, and U.S. Senator Ron Wyden.

[14] Office of the High Commissioner for Human Rights, OHCHR Advisory Service on Digital Technologies Comments on Canadian draft Bill C-22 (the Lawful Access Act), 3 November 2026, https://ccla.org/wp-content/uploads/2026/11/2026.11.03-UN.OHCHR-C22.Assessment.pdf.

[15] For example, the Privacy Commissioner of Canada recommended an explicit prohibition on "any action that would render systemic methods of authentication or encryption less effective." The encrypted messaging provider, Signal, testified that the law "must prohibit degrading or bypassing encryption", and had given examples of surveillance measures "that do not directly touch encryption but that negate the very purpose of encryption." Apple Inc. testified that the bill should be amended to "explicitly prohibit any requirement that would weaken, bypass, or undermine end-to-end encryption." United Nations, Office of the High Commissioner for Human Rights, Advisory Service on Digital Technologies, Comments on Canadian draft Bill C-22", November 3, 2026, https://ccla.org/wp-content/uploads/2026/11/2026.11.03-UN.OHCHR-C22.Assessment.pdf.

[16] Center for Democracy & Technology, "Canadians Oppose Key Surveillance Powers in Bill C-22 and Want Strong Protections for Encrypted Communications", May 19, 2026, https://cdt.org/insights/canadians-oppose-key-surveillance-powers-in-bill-c-22-and-want-strong-protections-for-encrypted-communications/.

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

[18] Hal Abelson, Ross Anderson, Steven M Bellovin, Josh Benaloh, Matt Blaze, Jon Callas, Whitfield Diffie, Susan Landau, Peter G Neumann, Ron L Rivest, Jeffrey I Schiller, Bruce Schneier, Vanessa Teague & Carmela Troncoso, "Bugs in our Pockets: The Risks of Client-Side Scanning", (2024) 10(1) *J of Cybersecurity* 1, https://doi.org/10.1093/cybsec/tyad020; 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) https://citizenlab.ca/wp-content/uploads/2018/05/Shining-A-Light-Encryption-CitLab-CIPPIC.pdf, pp 19-21.

compromise encryption, but rather as a mechanism for various government agencies to access secure data on a case-by-case basis without collateral harm. 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.

13. Against this backdrop, SAAIA represents a problematic framework through which the government will be able to impose its evolving surveillance priorities in secret and at the cost of every person's cybersecurity. SAAIA's framework is particularly problematic for its combination of an open-ended scope of application with flexible, ill-defined safeguards and inadequate oversight. In particular, SAAIA's oversight framework is heavily shielded from stakeholder input, judicial control and public accountability due to its nature as a mechanism for foreign intelligence oversight rather than one of domestic judicial authorization. Safeguards introduced by the government to date as protections for encryption do more to confirm the risk that encryption will be compromised or weakened than to ensure that this critical safeguard will remain intact.[19]

14. SAAIA's data retention mechanism has also received extensive criticism and is almost certainly unconstitutional. While SECU's study of the bill amended the time period to six months (from one year) and added a general necessity requirement, this change does not address the core issue, which is that the government can obligate any ESP to keep a person's metadata indiscriminately without any need to demonstrate that the person is involved in any wrongdoing.

15. The government's ability to impose and justify these obligations in secret is particularly concerning. Governments have consistently overstated the need for metadata while consistently understating its highly intrusive potential when justifying similar mechanisms in secret.[20] A 5 year audit of a US program mandating retention of phone call logs for national security purposes found, for example, that the program had yielded just one single significant investigation and only generated unique information that the FBI did not already possess on two occasions.[21] This independent assessment contributed to the program's eventual abandonment fourteen years after it was secretly initiated and less than six years after it was publicly disclosed by whistleblower Edward Snowden.[22]

16. Governments also frequently understate how sensitive metadata is when allowed to advance surveillance proposals in secret. Metadata is not defined in SAAIA, but at the least includes a record of every person's digital interactions and phone records, detailed tracking of every single person's movements, and an overview of every application a person has used.[23] This type of metadata is highly revealing. For example, one analysis that was limited to people's call records demonstrated that "there are significant privacy impacts associated with telephone metadata" which "gives rise to…sensitive inferences", including political perspectives, religious views and more.[24]

---

[19] See paras 25-26 below.

[20] National Security Intelligence Committee of Parliamentarians, "Special Report on the Lawful Access to Communications by Security and Intelligence Organizations" (September 2025). By contrast, see: United States, Privacy and Civil Liberties Oversight Board, Section 215 Report on the Telephone Records Program, January 23, 2014; Charlie Savage, "NSA Phone Program Cost $100 Million but Produced Only Two Unique Leads", February 25, 2020, *New York Times*, https://www.nytimes.com/2020/02/25/us/politics/nsa-phone-program.html; Ellen Nakashima, "Repeated Mistakes in Phone Record Collection Led NSA to Shutter Controversial Program", June 26, 2019, *Washington Post*, https://www.washingtonpost.com/world/national-security/repeated-mistakes-in-phone-record-collection-led-nsa-to-shutter-controversial-program/2019/06/25/f256ba6c-93ca-11e9-b570-6416efdc0803_story.html.

[21] Charlie Savage, "NSA Phone Program Cost $100 Million but Produced Only Two Unique Leads", February 25, 2020, New York Times, https://www.nytimes.com/2020/02/25/us/politics/nsa-phone-program.html. See also: United States, Privacy and Civil Liberties Oversight Board, Section 215 Report on the Telephone Records Program, January 23, 2014.

[22] Glenn Greenwald, "NSA Collecting Phone Records of Millions of Verizon Customers Daily", June 5, 2013, *The Guardian*, https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order; Charlie Savage, "NSA Phone Program Cost $100 Million but Produced Only Two Unique Leads", February 25, 2020, New York Times, https://www.nytimes.com/2020/02/25/us/politics/nsa-phone-program.html.

[23] SAAIA, ss 2(1), 5(2)-(4); Citizen Lab/CCLA Analysis of Bill C-22, *supra* note 1, at p 11-12.

[24] 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), http://webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone-metadata/;

17. It is important to note that Bill C-22 does not only expose everyone's metadata to unconstitutional retention, but would also make all Internet users in Canada more vulnerable to privacy violations by private sector technology and Internet companies. Canadian privacy laws place strict limits on what metadata companies can collect,[25] but—on top of the ever-present possibility of data breaches—SAAIA would override these limitations while placing no limits on when that data might be accessed by the service providers themselves or for what purpose, meaning companies may use the data troves they collect under SAAIA for their own commercial purposes.

18. Despite rapid technological changes over the past decade, the government has indicated that the surveillance obstacles it needs to overcome relate primarily to telephone and Internet providers.[26] While the impetus to solve any potential future surveillance priority is understandable, government surveillance powers are frequently updated and rarely limited once adopted.[27] Applying SAAIA to telecommunications providers alone as a starting point would therefore be an important step in targeting the regime to stated law enforcement and national security needs and to mitigating the potential harm of the regime.

19. Indeed, the government's *Charter* compliance statement is a clear indication of the hazardous manner in which it intends to apply this regime. The statement argues that the right to privacy as protected by section 8 of the *Charter* is not even engaged when obligations are imposed on service providers despite unambiguous jurisprudence from the Supreme Court of Canada to the contrary.[28] This mis-statement of the law is a concerning indication of the manner in which the government intends to apply SAAIA and is particularly concerning in light of the secretive framework that the government will be able to use to advance its legal arguments.

20. 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 do not have mandatory data retention requirements at all, and both countries have limited regimes that can only impose "lawful intercept" (i.e. wiretapping) requirements on telephone and Internet providers.[29] By contrast, SAAIA

Written Testimony of Ed Felten, House of Representatives, Subcommittee on Crime and Federal Government Surveillance of the Committee on the Judiciary (2 October 2013), *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.

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

[26] SECD Proceedings, Testimony of Gary Anandasangaree, P.C., M.P., Minister of Public Safety, and of Richard Bilodeau, Assistant Deputy Minister, National and Cyber Security Branch, November 2, 2026.

[27] The list of lawful access proposals that have become law in recent years includes: Bill C-13, *Protecting Canadians from Online Crime Act*, 41st Parliament, 2nd Session, Royal Assent December 9, 2014; Bill C-51, *Anti-terrorism Act, 2015*, 41st Parliament, 2nd Session, received Royal Assent on June 18, 2015; Bill C-59, *National Security Act, 2017*, 42nd Parliament, 1st Session, received Royal Assent on June 21, 2019; Bill S-4, *An Act to amend the Criminal Code and the Identification of Criminals Act and to make related amendments to other Acts (COVID-19 response and other measures)*, 44th Parliament, 1st Session, received Royal Assent on December 15, 2022; Bill C-16, *Protecting Victims Act*, 1st Session, 54th Parliament, received Royal Assent on June 18, 2026; Bill C-12, 45th Parliament, *Strengthening Canada's Immigration System and Borders Act*, 1st Session, received Royal Assent on March 26, 2026; Bill C-70, *Countering Foreign Interference Act*, 44th Parliament, 1st Session, received Royal Assent, June 20, 2024.

[28] See *Charter Statement on Bill C-22*, Tabled in the House of Commons, April 24, 2026, "Part 2 – Supporting Authorized Access to Information Act", which does not identify any section 8 implications arising from SAAIA's metadata retention provisions. However, see Citizen Lab/CCLA Analysis of Bill C-22, supra note 1, at p 12, citing *R v Laroche*, 2002 SCC 72, paras 33, 50-55, where the Supreme Court held that 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; *R v Hollaman*, 2025 BCCA 315; *R v Pham*, 2025 BCCA 324 at para 103, leave to appeal granted, SCC File No 42101; *R v Khairullah*, 2025 ABCJ 14. See also, Office of the High Commissioner for Human Rights, OHCHR Advisory Service on Digital Technologies Comments on Canadian draft Bill C-22 (the Lawful Access Act), 3 November 2026, https://ccla.org/wp-content/uploads/2026/11/2026.11.03-UN.OHCHR-C22.Assessment.pdf, p 5-6.

[29] National Security Intelligence Committee of Parliamentarians, "Special Report on the Lawful Access to Communications by Security and Intelligence Organizations" (September 2025), p 15 (Table 2.1).

includes a sweeping metadata retention regime and allows the government to impose any obligation on any digital service provider, including operating systems and systems with no communicative element at all, in secret.

21. Two of the Five Eyes, Australia and the United Kingdom (UK), have regimes that approach SAAIA's breadth. But the UK regime is currently being challenged after a secret government order requiring Apple to remove critical end to end encryption protections from its iCloud backups was leaked to the public in violation of the law's secrecy provisions.[30] It is unclear how an order compelling access to iCloud backups that are end-to-end encrypted is compatible with the UK's legal framework, yet the result of this order is that Apple devices in the UK are now deprived of a critical safeguard available to devices anywhere else in the world.[31] 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.[32] Far from addressing these constitutional defects in the UK and Australian regimes, SAAIA not only imports but even expands the breadth of both regimes while failing to include many of their essential safeguards and limitations.

22. It should be clear that all technical surveillance capability regimes, regardless of breadth, present a significant threat to cybersecurity. The US and New Zealand regimes, for example, are limited to imposing "lawful intercept" obligations onto telecommunications carriers. These obligations are far narrower in scope and complexity than those imposed in SAAIA, but still create lucrative targets that are difficult to secure.[33] For example, when the US National Security Agency (NSA) tested equipment that complied with CALEA, the US lawful intercept law,[34] it found that "every single switch it tested had a security flaw".[35] The most recently discovered compromise, attributed to Salt Typhoon, an advanced persistent threat actor with ties to

---

[30] Privacy International, "PI Apple TCN Challenge", 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), 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] UKIPTrib 1, 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), 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), https://www.washingtonpost.com/technology/2025/02/07/apple-encryption-backdoor-uk/.

[31] *Podchasov v Russia*, App No 33696/19, Feb 13, 2024, (ECtHR 3rd Section), paras 56-57, 77 and 79.

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

[33] "CCLA and Coalition of Coalitions Call for Withdrawal of Bill C-2", (11 July 2025), *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), 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*, https://spectrum.ieee.org/the-athens-affair; Susan Landau, "CALEA Was a National Security Disaster Waiting to Happen", *Lawfare* (13 November 2024), 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) https://www.congress.gov/119/meeting/house/118335/witnesses/HHRG-119-JU08-Wstate-LandauS-20250605.pdf, p 8; 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), 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.

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

[35] Susan Landau, "The Large Immortal Machine and the Ticking Time Bomb", (2013) 11(1) *J on Telecom & High Tec L* 1, archived, p 3: "When several large switch manufacturers submitted CALEA-compliant switches to the NSA for testing – a requirement prior to use in Department of Defense systems – the NSA found security problems with the CALEA-compliant implementation on every single switch submitted for testing."; Testimony of Susan Landau, House of Representatives, Subcommittee on Crime and Federal Government Surveillance of the Committee on the Judiciary (5 June 2025) https://www.congress.gov/119/meeting/house/118335/witnesses/HHRG-119-JU08-Wstate-LandauS-20250605.pdf, p 8.

the government of China, commandeered "lawful intercept" backdoors built into U.S. Internet service providers under CALEA with disastrous implications.[36]

SAAIA's Safeguards and limitations are inadequate

23. SAAIA does not include any effective safeguards for encryption and other cyber security mechanisms. There is no requirement on the government's part to establish, based on reasonable grounds, that the privacy implications of an ESP's obligation are proportionate or that an obligation is strictly necessary to investigations of serious offences or national security activity. Instead, there is an open-ended set of factors that the government must take into account when imposing obligations.[37] SAAIA includes two specific additional safeguards—one against the creation of systemic vulnerabilities and one against obligations to decrypt end-to-end encryption.[38] Neither of these exceptions are sufficient to safeguard encryption.

24. Under SAAIA, service providers need not comply with any obligation if they are of the view that it would have the effect of introducing or keeping in place a "systemic vulnerability" in electronic protections including encryption.[39] The "systemic vulnerability" exception allows companies to weaken or compromise encryption if the government is of the view that the resulting measures will mostly be employed by lawfully authorized government officials. It effectively encodes the concept of "exceptional access", which is based on the faulty premise that security bypass tools can be safeguarded so that only the government will employ them. This notion has been demonstrated as false by the technical community on numerous occasions, as summarized by a number of the world's leading cybersecurity experts:

> Since strong encryption became available to the public nearly half a century ago, intelligence and law enforcement agencies around the world have sought to limit its use. The first attempts were to restrict access to encryption devices. When the invention of the PC made encryption widely available in software, attempts were made to require backdoors that would provide governmental access to decryption. These proposals were effectively abandoned in most democratic countries by the end of the 20th century. Since then, several national intelligence and law enforcement agencies have instead worked to enlist vendors as surrogates to provide access to encrypted traffic, whether using technical vulnerabilities or covert court-ordered access. … However, when actually analyzing CSS systems…from a security perspective, it becomes apparent that the promise of a technologically limited surveillance system is in many ways illusory. … In this paper, we explore answers to these questions. In the end, we find no design space for solutions that provide substantial benefits to law enforcement without seriously risking the privacy and security of law-abiding citizens.[40]

---

[36] Internet Society, "Open Letter: Bill C-22, An Act Respecting lawful access", 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), 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), *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), 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), https://www.theglobeandmail.com/politics/article-lawful-access-bill-could-threaten-encryption-deter-investment-chamber/.

[37] SAAIA, ss 5(3) and 7(3). By contrast, see SAAIA, s 5(4.1). CCLA/CitLab analysis.

[38] SAAIA, ss 5(5), 7(5) and 2(4).

[39] SAAIA, ss 5(5), 7(5) and 2(1) "systemic vulnerability" and "electronic protection".

[40] Hal Abelson, Ross Anderson, Steven M Bellovin, Josh Benaloh, Matt Blaze, Jon Callas, Whitfield Diffie, Susan Landau, Peter G Neumann, Ron L Rivest, Jeffrey I Schiller, Bruce Schneier, Vanessa Teague & Carmela Troncoso, "Bugs in our Pockets: The Risks of Client-Side Scanning", (2024) 10(1) J of Cybersecurity 1, https://doi.org/10.1093/cybsec/tyad020; Erica Portnoy, "Why Adding Client-Side Scanning Breaks End-to-End Encryption, November 1, 2019, Electronic Frontier Foundation, https://www.eff.org/deeplinks/2019/11/why-adding-client-side-scanningbreaks-end-end-encryption; High Commissioner for Human Rights, "Apple-FBI Case Could Have Serious Global Ramifications for Human Rights", March 4, 2016, https://www.ohchr.org/en/press-releases/2016/03/apple-fbi-case-could-have-serious-global-ramifications-human-rights-zeid; Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/29/32, May 22, 2025, https://undocs.org/A/HRC/29/32, para 8; Peter Swire, Ian Goldberg, Michael Specter, Douglas Stebila, "Explaining Concerns About Bill C-22 Based on Experience with Prior Encryption Proposals and Lawful Access Regimes Elsewhere", Cross-Border Data Forum, October 30, 2026, https://www.crossborderdataforum.org/explaining-concerns-about-bill-c-22-based-on-experience-with-prior-encryption-proposals-and-lawful-access-regimes-elsewhere/.

25. An additional safeguard indicates that obligations under SAAIA cannot compel a service provider to decrypt communications unless the service provider already possesses the information necessary to decrypt the information.[41] While compelling service providers to decrypt end-to-end encryption is one legal obligation that governments can impose to facilitate access to encrypted data, modern attempts to weaken encryption rarely rely on decryption mandates.[42] For this reason, every stakeholder that sought protection for encryption called for an amendment that would explicitly prohibit any measure that would weaken, bypass, or compromise encryption.

26. Collectively, these two safeguards do not impede the government's ability to secretly impose obligations that weaken, bypass or circumvent encryption particularly in light of the wide-ranging types of obligations that can be imposed under SAAIA.[43] For example, under SAAIA:

- a secure email provider can be compelled to develop a system-wide tool that can be used to covertly reset any account's password to facilitate police access to the encrypted information on the account;[44]
- a secure messaging service can be compelled to create a tool that would allow for the creation of invisible accounts and to covertly add these accounts to group chats;[45]
- a secure cloud backup service can be compelled to impose content scanning tools onto end devices so that content that is responsive to an authorized production order can be remotely identified, organized and extracted before it is encrypted and backed up;[46] or
- a secure mobile device operating system provider can be compelled to create dedicated software that will bypass password entry limits to facilitate brute force access to an encrypted device.[47]

---

[41] SAAIA, 2(4): "No obligations under this Act are to be construed as compelling an electronic service provider to decrypt, or to ensure that an authorized person is able to decrypt, any information that is encrypted by a person to whom the electronic service provider provides services, unless the encryption was provided by the electronic service provider and the provider possesses the information necessary to decrypt the information."

[42] See discussion at Citizen Lab/CCLA Analysis of Bill C-22, *supra* note 1, at p 15. See also High Commissioner for Human Rights, "Apple-FBI Case Could Have Serious Global Ramifications for Human Rights", March 4, 2016, https://www.ohchr.org/en/press-releases/2016/03/apple-fbi-case-could-have-serious-global-ramifications-human-rights-zeid; and Office of the High Commissioner for Human Rights, OHCHR Advisory Service on Digital Technologies Comments on Canadian draft Bill C-22 (the Lawful Access Act), 3 November 2026, https://ccla.org/wp-content/uploads/2026/11/2026.11.03-UN.OHCHR-C22.Assessment.pdf, p 6.

[43] SAAIA, ss 7(1) and 5(2)(a) (impose any obligations respecting technical capabilities relating to the extracting and organizing of information that is authorized to be accessed and to providing access to such information to authorized persons) and (b) (obligate the installation, use and operation of any device, equipment or other thing that may enable an authorized person to access information).

[44] *R v Strong*, 2020 ONSC 7528, para 100.c; 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, https://www.homeaffairs.gov.au/foi/files/2019/fa190200278-document-released.PDF, pp 21-23: ("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").

[45] Internet Society, Fact Sheet: Ghost Proposals, March 24, 2020, https://www.internetsociety.org/resources/doc/2020/fact-sheet-ghost-proposals/; Mathew Green, "On Ghost Users and Messaging Backdoors", December 17, 2018, https://blog.cryptographyengineering.com/2018/12/17/on-ghost-users-and-messaging-backdoors/.

[46] For example, a content scanning tool could be used to remotely identify and extract all images or all messages from a particular application over a three-year period or a single account verification code: *R v Marek*, 2016 ABQB 18; *R v Jones*, 2011 ONCA 632, paras 42-50; *R v Strong*, 2020 ONSC 7528, para 100(b). See also: Privacy International, "PI Apple TCN Challenge," 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", October 1, 2025, https://privacyinternational.org/news-analysis/5685/second-orderuk-governments-new-secretorder-still-strikes-apples-security; *Apple v Secretary of State for the Home Department*, [2025] UKIPTrib 1, 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", February 14, 2025, https://www.hrw.org/news/2025/02/14/ukencryption-order-threatens-global-privacy-rights; Joseph Menn, "U.K. orders Apple to let it spy on users' encrypted accounts," Washington Post, February 7, 2025, https://www.washingtonpost.com/technology/2025/02/07/apple-encryption-backdoor-uk/; Hal Abelson, Ross Anderson, Steven M Bellovin, Josh Benaloh, Matt Blaze, Jon Callas, Whitfield Diffie, Susan Landau, Peter G Neumann, Ron L Rivest, Jeffrey I Schiller, Bruce Schneier, Vanessa Teague & Carmela Troncoso, "Bugs in our Pockets: The Risks of Client-Side Scanning", (2024) 10(1) *J of Cybersecurity* 1, https://doi.org/10.1093/cybsec/tyad020.

[47] *In re Search of an Apple iPhone Seized During the Execution of a Search Warrant*, 5:15-mj-00451, Order compelling Apple to Assist Agents in Search, February 6, 2016 (Calif Cent Dist, 2016), https://www.eff.org/document/apple-fbi-all-writs-first-magistrate-judge-order, paras 2-3.

None of these examples are hypotheticals as all have been proposed under similar regimes, yet each poses a severe threat to encryption and cybersecurity. In each of these instances, the service provider is not required to decrypt end-to-end encryption and the Canadian government would only compel deployment of the resulting capability against authorized targets. As a result, none of these proposals would be reliably excluded by existing exceptions in SAAIA despite the severe risk they pose to encryption and cybersecurity.

27. In addition, these two safeguards in SAAIA are not responsive to the types of threats posed to secure communications by the obligation to systematically retain metadata. Virtual Private Networks (VPNs), for example, are an important security tool that relies on a combination of encryption and retention limitations to facilitate secure and anonymous digital interactions.[48] SAAIA can be used to secretly compel VPNs to systematically retain metadata on users. Neither of SAAIA's core safeguards are engaged by retention requirements. A retention requirement would not require a VPN to "decrypt" any metadata at all.[49] While the obligation to retain *any* previously unretained metadata creates a significant threat of unauthorized access, this risk is not higher when the obligation is imposed on VPNs than on other types of providers even though the consequences of retention are far more severe.[50]

28. Finally, the framework for considering safeguards and limitations under SAAIA needs to be public by default and to the maximum extent possible. SAAIA currently relies on a framework that was designed to oversee foreign espionage and has proven highly resistant to public and judicial scrutiny in the absence of whistleblowers. It is not appropriate for addressing matters of primarily domestic surveillance.

29. SAAIA does not include any judicial authorization or appeal mechanisms, relying heavily instead on judicial and quasi-judicial review, a deferential mechanism that is limited to considering whether the government's decision is reasonable rather than determining independently whether an obligation should be imposed.[51] Judicial review provides limited ability to adduce new evidence and raise new considerations, in stark contrast to the standard process for authorizing domestic interference with the right to privacy.[52] As indicated in legislative assessments of Australia's technical surveillance capabilities regime, judicial review is not an adequate mechanism for ensuring these types of obligations are imposed in a manner that is necessary and proportionate:

> … 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.[53]

---

[48] See, for example, Marie Woolf, "Toronto-based VPN Provider Plans to Quit Canada Over Lawful-Access bill", Globe and Mail, October 4, 2026, https://www.theglobeandmail.com/politics/article-psiphon-vpn-provider-plans-to-quit-canada-overlawful-access-bill/; Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/29/32, May 22, 2025, https://undocs.org/A/HRC/29/32, para 23.

[49] SAAIA, s 2(4).

[50] SAAIA, s 2(1) "systemic vulnerability".

[51] *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 Citizen Lab/CCLA Analysis of Bill C-22, *supra* note 1, at p 18-20; United Nations, Office of the High Commissioner for Human Rights, Advisory Service on Digital Technologies, Comments on Canadian draft Bill C-22", November 3, 2026, https://ccla.org/wp-content/uploads/2026/11/2026.11.03-UN.OHCHR-C22.Assessment.pdf, at p 2-3.

[52] *Canada (Minister of Citizenship and Immigration) v. Vavilov*, 2019 SCC 6; *Canada (Attorney General) v Canadian Civil Liberties Association*, 2026 FCA 6, currently under appeal, SCC File No 42261. Contrast with the standard authorization framework: 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.

[53] Australia, Parliamentary Joint Committee on Human Rights, Human Rights Scrutiny Report (4 December 2018) https://www.aph.gov.au//media/Committees/Senate/committee/humanrights_ctte/reports/2018/Report_13/Report_13_of_2018.pdf, at paras 2.178-2.181. 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 p 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'."

SAAIA's heavy reliance on judicial review is compounded by the use of the intelligence commissioner–an independent body designed to oversee foreign espionage–as the mechanism for judicially reviewing presumptively secret orders issued under s 7 of SAAIA. Given its foreign espionage orientation, the Intelligence Commissioner operates under significant secrecy, without ability for broad stakeholder input.

30. This results in absurd outcomes–to compel a service provider to preserve metadata in relation to specific targets of investigations for 90 days, police require judicial authorization but to compel the same service provider to retain or preserve the same metadata on every single customer for 6 months no judicial authorization is required.[54] CSIS requires judicial authorization before it can retain bulk metadata already under its *own* control where there is no immediate national security need for that metadata,[55] but would not require judicial authorization to compel a service provider to retain the same metadata on every single person for up to 6 months.

31. SAAIA also lacks any mechanism for technical review of orders by an independent, non-governmental body. The UK's technical advisory board plays this function, ensuring that an independent, non-governmental body with deep technical expertise assess any obligation before it is put in place, and that would form part of the record justifying the adoption of any obligation.[56]

32. Finally, under SAAIA the government has full discretion to decide whether obligations and compliance orders are imposed in secret.[57] SAAIA must operate in a manner that is public by default, where information is withheld from the public only in situations where the government can demonstrate that its public disclosure will be injurious to national security or to law enforcement investigations. Public accountability for the use of the expansive powers SAAIA will put in place cannot be dependent on whistleblowers.[58]

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

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

34. 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.

35. 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

---

54 *Criminal Code*, RSC 1985, c C-46, s 487.013.

55 *Canadian Security Intelligence Service Act (Re)*, 2022 FC 645 at paras 9-19.

56 UK, IPA 2016, ss 245 and 253(6).

57 SAAIA, ss 7(1), (1.1), 14(c) and 15(1)(presumptively secret orders).

58 See, for example, *Privacy International et al v Secretary of State for the Home Department*, [2026] UKIPTrib 9, https://www.judiciary.uk/wp-content/uploads/2026/11/OPEN-Judgment-Apple-Inc.-and-Privacy-Int.-Ors.pdf; *Apple v Secretary of State for the Home Department*, [2025] UKIPTrib 1, https://investigatorypowerstribunal.org.uk/wp-content/uploads/2025/04/IPT-25-68-CH-Judgment.pdf; Privacy International, "PI Apple TCN Challenge," https://privacyinternational.org/legal-action/pi-apple-tcnchallenge; and Privacy International, "The Second Order: The UK Government's new secret order still strikes at Apple's security", October 1, 2025, https://privacyinternational.org/news-analysis/5685/second-order-uk-governments-new-secretorder-still-strikes-apples-security.

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.[59] 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,[60] 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.

36. 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

37. 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 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.

38. 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."[61]

39. 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.[62] The agreement would be established under a piece of US legislation called the Clarifying Lawful Overseas Use of Data Act ("CLOUD Act").

40. Canadian officials have previously linked the proposed surveillance reforms, when they were presented in Bill C-2, to the United States.[63] However, the federal government has not provided the public or Parliament

---

[59] Nicole Brockbank, "Toronto police used Clearview AI facial recognition software in 84 investigations", *CBC* (23 December 2021), 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), 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.

[60] See e.g. Office of the Privacy Commissioner of Canada, *Joint investigation of TikTok Pte Ltd*, PIPEDA Findings #2025-003 (23 September 2025), 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) 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), 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), https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2022/pipeda-2022-001/.

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

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

[63] 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.

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.

41. 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.

42. 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.

43. 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.

44. 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.

45. 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*.

46. 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.

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), https://www.politico.com/newsletters/canada-playbook/2025/07/04/stars-stripes-and-side-eye-00439998.

Conclusion

47. 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)		Rationale
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, as an 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.	Aligns SAAIA with our Five Eyes investigative partners (the US and New Zealand) by limiting the application of its surveillance by design regime to telecommunications carriers (phone, and internet companies including satellite.
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".	Aligns SAAIA with Five Eyes investigative partners (the US and New Zealand) by limiting its scope of obligations to lawful intercept capabilities (wiretaps) and with the US which prohibits imposing specific design obligations onto service providers (CALEA).
Rec 3	Amend section 5(2) to prevent the government from requiring service providers to provide direct access to infrastructure, software or data: 5(2) The Governor in Council may make regulations relating to the obligations of core providers, 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~~ by presenting lawful authority to a core provider; (b) the installation, use, operation, management, assessment, testing and maintenance of any device, equipment or other thing by core providers that may enable an authorized person to access information by presenting lawful authority to a core provider; … 5(2*bis*) No obligation under this *Act* can require a core provider to	Amend s 5(2) to This amendment would encode the government's stated intention to preclude obligations that would require digital services to provide direct access to government agencies while prohibiting specific design obligations.
Rec. 4	Amend s2(1) so that SAAIA's definition of systemic vulnerabilities fully accounts for cybersecurity impacts: ***systemic vulnerability*** means a vulnerability in the electronic protections of an electronic service that creates a ~~credible~~ material risk~~, based on recognized international technical standards, that secure~~ to the confidentiality, security and availability of information ~~could be accessed by a person who does not have any right or authority to do so,~~ other than a risk that relates only to information related to persons with respect to whom a warrant, order or other authority to access information conferred under the *Criminal Code* or the *Canadian Security Intelligence Service Act* ~~— or any similar authority conferred under another Act of Parliament —~~ applies.	Aligns SAAIA with well-recognized cybersecurity concepts by requiring that credible risks to the confidentiality, security and availability of information be considered when assessing whether exceptional access mechanisms are justified. The reference to formal international standards should further be removed, as there is no consistent source of international technical standards in this context.

Rec. 5	Amend section 2(4) so that it prevents all attacks on encryption: 2(4) No order or regulation shall be made ~~obligations~~ under this Act that would have the effect of weakening encryption including by ~~are to be construed as~~ compelling any electronic service provider: (a) to decrypt, or to ensure that an authorized person is able to decrypt, any information that is encrypted by a person to whom the electronic service provider provides services, unless the encryption was provided by the electronic service provider and the provider possesses the information necessary to decrypt the information; or (b) to bypass, compromise or degrade, or to develop the capability to bypass, compromise or degrade, encryption unless the encryption was provided by the electronic service provider and the provider possesses the information necessary to decrypt the information.	Aligns SAAIA with Australia's regime (TOLA, 317ZG), international human rights obligations in the EU and UK (*Podchasov*), all of which prohibit measures that weaken, bypass or circumvent end-to-end encryption and with the US regime (see, CALEA).
Rec. 6	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 listed in section 183 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.	Ensures that the government is required to properly justify its orders. a. Aligns our regime with Australia and the UK by requiring that the government to establish that imposing a particular obligation is necessary to investigations of serious crimes or national security (AUS, TOLA, s317T (serious crimes/national security); UK, IPA, s253(1)(necessity & serious crimes/national security)). b. Requires the government to demonstrate that their investigative objectives cannot be achieved by other means (; c. Align the regime with our Five Eyes partners by requiring obligations to be proportionate (AUS, TOLA, s317(V)(a); UK, IPA, s 254(2)(b). See also: CSE Act s 34). d. Align with Australia's regime (TOLA s 317H) by preventing the regime from being used to compel companies to intercept private metadata or do other things that would typically require a court order. See also Criminal Code, s 487.01(c).
Rec. 7	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 listed in section 183 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. 8	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 6 months; b. limit the application of the regime to telecommunications carriers (phone and internet providers, including satellite);	The data retention regime is unlikely to be compatible with the *Charter* and should be removed to align Canada with our Five Eyes partners (the US and New Zealand do not have data retention regimes), as well as European Union partners in digital trade. Were it to be retained: a. Limiting this regime to preservation will avoid threats to VPNs and other secure

	c. specify what categories of data can be required to be preserved in the text of the statute; and d. ensure that these categories 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.	networks while ensuring the consistent availability of data that police and security agencies say they require; b. Limiting the regime to telecom carriers would align Canada's regime with the UK (UK, IPA 2016, s 87) and the US/NZ which have no data retention obligations. c + d are both from the Australian regime and provide more specificity and limits on what can be retained while prohibiting any obligation to retain location information that is not already being used by the service provider to provide the service in question (AUS, TIA, ss 187A(4(e) and 187AA item 6).
Rec. 9	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.	
Rec. 10	Delete paragraph 47(1)(c) of SAAIA.	So that key terms cannot be defined by regulation, but would instead require legislative amendment.
Rec. 11	Require regulations (s. 5) and orders (s. 7) to expire after one year.	Align SAAIA with Australia's regime (AUS, TOLA, s 317TA(1A)). SECU added a 2 year expiry mechanism for orders issued under s7, requiring that the justification for these be reconsidered every 2 years. But other regimes require *all* obligations to be justified every year.
Rec. 12	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.	The SAAIA lacks restrictions or limitations on what the ESP can do with retained or preserved metadata, or on what happens to the metadata once the retention period expires.
Rec. 13	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*.	The SAAIA lacks restrictions or limitations on what happens to the metadata once the retention or preservation period expires.
Rec. 14	Limit obligations imposed through SAAIA to an ESP's own services.	
Rec. 15	Add a provision to the SAAIA establishing that ESPs cannot be compelled to deceive or mislead their customers or the public.	
Rec. 16	Remove the following from sections 5(3) and 7(3) of SAAIA: "(f) any other factor that the Governor in Council considers relevant"	The sets of considerations that can justify an obligation need to be spelled out in the Act.

Recommendations for Part 1		
Rec. 17	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].	Corresponds to Part B of our detailed analysis, to fix the problem that the proposed section 487.0195(4) creates a framework that contradicts and confuses clear Canadian *Charter* jurisprudence, which has consistently recognized public information is not categorically exempt from section 8 protection.
Rec. 18	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) 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.	Corresponds to Part D of our detailed analysis, to fix the problem that the proposed section 487.0195(3) would have the effect of adding a "for greater certainty" clause which would introduce confusion to the law and unconstitutional effects and harms.
Recommendations for Foreign Law Enforcement Access to Data		
Rec. 19	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.	Corresponds to Parts C.1 and C.2 of the detailed analysis published by the CCLA and Citizen Lab (linked above), as Bill C-22 is positioned to enable Canada to enter data-sharing treaties with foreign states, either in whole or in part.
Rec. 20	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.	Necessary safeguards to update Canada's laws given Canada's recent signing of two treaties (Second Additional Protocol and UN Cybercrime Convention), which make such protections an option to be exercised under Canadian law. The option should be taken by Canada, given the significant risks outlined in Part C of our detailed analysis.