Centre for International Governance Innovation

Digital Policy Hub

Digital Policy Hub – Working Paper

Democratic Accountability in Canada's Proposed Lawful Access Regime

Jamie Duncan

Fall 2024 cohort

About the Hub

The Digital Policy Hub at CIGI is a collaborative space for emerging scholars and innovative thinkers from the social, natural and applied sciences. It provides opportunities for undergraduate and graduate students and post-doctoral and visiting fellows to share and develop research on the rapid evolution and governance of transformative technologies. The Hub is founded on transdisciplinary approaches that seek to increase understanding of the socio-economic and technological impacts of digitalization and improve the quality and relevance of related research. Core research areas include data, economy and society; artificial intelligence; outer space; digitalization, security and democracy; and the environment and natural resources.

The Digital Policy Hub working papers are the product of research related to the Hub's identified themes prepared by participants during their fellowship.

About CIGI

The Centre for International Governance Innovation (CIGI) is an independent, non-partisan think tank whose peer-reviewed research and trusted analysis influence policy makers to innovate. Our global network of multidisciplinary researchers and strategic partnerships provide policy solutions for the digital era with one goal: to improve people's lives everywhere. Headquartered in Waterloo, Canada, CIGI has received support from the Government of Canada, the Government of Ontario and founder Jim Balsillie.

Partners

Thank you to Mitacs for its partnership and support of Digital Policy Hub fellows through the Accelerate program. We would also like to acknowledge the many universities, governments and private sector partners for their involvement allowing CIGI to offer this holistic research environment.

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org

Key Points

- The Strong Borders Act (Bill C-2) proposes significant changes to Canada's lawful access regime, expanding law enforcement and intelligence powers to obtain digital information from third-party service providers.
- While many critics suggest courts will find the bill unconstitutional, the legislation raises broader concerns about democratic accountability by creating shortfalls in transparency and gaps in oversight.
- The proposed lawful access regime undermines transparency by formalizing information back channels and omitting statutory reporting and disclosure requirements that appear in comparable laws.
- Bill C-2 also creates gaps in oversight. While a strong role is preserved for judicial and ministerial control, the bill is silent on the role of independent oversight bodies. Without a clear role for independent oversight, expanded surveillance risks eroding democratic norms in Canadian policing and intelligence.
- Extending mechanisms for transparency, oversight and review that already govern other aspects of national security information policy to Bill C-2 could mitigate these deficits in democratic accountability.

Introduction

On June 3, 2025, the Canadian government tabled Bill C-2[1] as one of its first actions following the election of Mark Carney's Liberal government. The omnibus bill is wide-ranging in scope with many points of controversy. This working paper focuses on contentious provisions expanding law enforcement and intelligence agencies' surveillance powers through lawful access to digital information.

Some suggest these new powers, which include warrantless access to basic information from service providers about their clients and an overhauled digital warrant regime,[2] are simply harmonizing Canadian law with existing domestic practices and those of international allies (Woolf 2025a; Canadian Association of Chiefs of Police 2025). But advocacy organizations and opposition law makers frame the proposed changes as capitulation to the demands of an increasingly authoritarian United States and an erosion of civil liberties and democratic norms in Canada (Appel 2025; Geist 2025b). Many advocates called for the wholesale withdrawal of Bill C-2 on the grounds that it would violate Canadian Charter of Rights and Freedoms (Charter) protections against unreasonable search and seizure (OpenMedia 2025).

1 Bill C-2, *An Act respecting certain measures relating to the security of the border between Canada and the United States and respecting other related security measures*, 1st Sess, 45th Parl, 2025 (first reading 3 June 2025), online: <www.parl.ca/DocumentViewer/en/45-1/bill/C-2/first-reading>.

2 *Ibid*, cls 156, 158–159, 194.

Responding to this pushback and a lack of support in Parliament, the Liberal government tabled Bill C-12[3] on October 8, 2025, effectively repackaging select provisions tightening border security and restricting access to asylum in Canada to try passing parts of their agenda more quickly (Tunney 2025). Despite the delay, the political will for an expanded lawful access regime is not dead. This working paper critically evaluates Bill C-2's proposals for lawful access in anticipation of a renewed debate. It argues that any expansions of surveillance powers for law enforcement and intelligence agencies must be accompanied by clear and enforceable institutional safeguards for democratic accountability.

With democratic norms under growing threat in many parts of the world (Nord et al. 2025; Economist Intelligence 2025; Gorokhovskaia and Grothe 2025), it is not only imperative that law enforcement and intelligence agencies are properly equipped to defend democratic institutions, but also that these agencies remain accountable to them. Many experts have weighed in on the constitutionality of the proposed lawful access regime. This working paper adds to the discussion by focusing on institutional protections for democratic accountability, namely, transparency requirements and the scope of independent oversight and review.

The analysis finds claims that lawful access will usher in an Orwellian police state, espoused by some,[4] are more rhetoric than reality. But this skepticism is reasonable given the historical propensity of Canadian policing and national security organizations to push the limits of their legal authority (Office of the Privacy Commissioner [OPC] 2021; National Security and Intelligence Review Agency [NSIRA] 2024a). Ultimately, the working paper concludes that the Strong Borders Act creates shortfalls in transparency and gaps in oversight that could be addressed by extending existing frameworks for transparency, oversight and review that already apply in other areas of national security information policy.

Background: Lawful Access in Canada

The lawful access regime is largely outlined in parts 14 and 15 of the Strong Borders Act. Part 14 details new powers of search and seizure for digital information. It creates parallel powers for law enforcement and intelligence agencies to issue warrantless "information demands" to public service providers for basic information such as whether, where and for how long someone has been a client.[5] The bill specifies such demands can be issued to any "person who provides services to the public."[6] It also creates a new kind of "production order" in which a judge can grant access to subscriber information such as someone's name and address as well as "transmission data" such as

3 Bill C-12, *An Act respecting certain measures relating to the security of Canada's borders and the integrity of the Canadian immigration system and respecting other related security measures*, 1st Sess, 45th Parl, 2025 (first reading 11 December 2025), online: <www.parl.ca/legisinfo/en/bill/45-1/c-12>.

4 See https://openparliament.ca/debates/2025/6/11/jenny-kwan-1/.

5 Bill C-2, *supra* note 1, cls 158, 185.

6 *Ibid*, cl 158.

an internet protocol (IP) address.[7] The bill clarifies how authorities can issue information demands and request subscriber information from foreign jurisdictions.[8] It updates the search warrant regime with specific provisions related to accessing digital systems and data, including the content of communications, additional transmission data or documents.[9]

Part 15 creates the Supporting Authorized Access to Information Act (SAAIA), which complements the proposed framework for lawful access by mandating that electronic service providers facilitate access in accordance with part 14. The term "electronic service provider" applies to telecommunications companies, cloud providers, social media platforms or even small-scale app developers.[10] The government may designate "core providers" and set out regulations requiring them to establish technical capabilities enabling lawful access by installing software or devices for collecting transmission data or intercepting communications.[11]

These proposals build on a long and contentious history. Repeated attempts to secure lawful access over the past two decades have been challenged by privacy and civil liberties advocates and constrained by parliamentarians, the courts and federal watchdogs (Parsons 2015). Efforts under then Prime Minister Stephen Harper to legislate lawful access were abandoned amid criticism of "Big Brother"-style surveillance (Geist 2025a). Parliament eventually passed the Protecting Canadians from Online Crime Act in 2014,[12] but the Supreme Court of Canada curtailed its reach in *R. v. Spencer*,[13] ruling that subscriber information is subject to a reasonable expectation of privacy. In 2024, the courts extended this protection to IP addresses.[14]

Notwithstanding these limits to lawful access, the Canadian Security Intelligence Service (CSIS) and the Royal Canadian Mounted Police (RCMP) have repeatedly tested the limits of their powers to collect and use digital information. In 2016, a federal court ruled CSIS had exceeded its lawful authority by retaining data sets not related to a security threat or the target of an active warrant.[15] This led to the creation of the CSIS Dataset Regime through the National Security Act (2017),[16] which defined data sets and permitted uses, established the Office of the Intelligence Commissioner (ICO) and outlined a framework requiring both ministerial authorization and review by the ICO to collect, use or retain data sets. In 2020, news broke that the RCMP and several other Canadian police services had used a controversial facial recognition platform sold by Clearview AI, matching submitted photos to a database of images scraped from the internet (Carney 2020). The Privacy Commissioner subsequently ruled that Clearview's data collection practices were unlawful and that the RCMP's use of "a database compiled illegally by a commercial enterprise is a violation of the Privacy Act" (OPC 2021). But despite these

7 *Ibid*, cl 159.

8 *Ibid*, cls 158, 160, 185.

9 *Ibid*, cls 155–56, 166–71, 173–74, 187–88.

10 *Ibid*, cl 194, s 2(1).

11 *Ibid*, cl 194, s 5.

12 *Protecting Canadians from Online Crime Act*, SC 2014, c 31.

13 *R v Spencer*, 2014 SCC 43, [2014] 2 SCR 212.

14 *R v Bykovets*, 2024 SCC 6 (CanLII).

15 *X (Re)*, 2016 FC 1105 [ODAC Decision].

16 *National Security Act*, 2017 (SC 2019, c 13).

measures, subsequent reporting from the OPC (2024) and NSIRA (2024a) has suggested the RCMP and CSIS continue to collect and use digital data in ways that may exceed their lawful authority.

Democratic Accountability in the Digital Era

National security and law enforcement institutions present a paradox for democratic accountability (Leuprecht and McNorton 2021). Those tasked with defending democracies often operate in ways that defy common expectations of democratic institutions. Secrecy, deception and otherwise unlawful activity are part of the job (Brodeur 2010). The spread of digital technologies has sharpened this paradox. The massive proliferation of private sector digital surveillance — what some call "surveillance capitalism" (Zuboff 2019) — has produced vast reservoirs of information. Even if their formal powers remain constrained, Canadian law enforcement and intelligence agencies leverage open-source digital information and private data brokers to expand their investigative reach (OPC 2024; NSIRA 2024a). As criminal activity and threats to national security have extended online, it is logical that police and security agencies would seek to enhance their capacity to identify and interrupt these activities.

Yet the rise of surveillance capitalism alongside evidence of past abuses in Canada and among international allies feeds into narratives of pervasive state surveillance, which contribute to public mistrust (Lyon 2014; McMullen 2022, 2023). This mistrust limits public tolerance for the kinds of expanded powers proposed in Bill C-2. Strong frameworks for democratic accountability are crucial to fostering greater legitimacy in Canadian policing and intelligence. While democratic accountability is complex and multi-faceted, this working paper analyses democratic accountability in Bill C-2 along two dimensions: transparency and oversight.

Transparency means government actions — including those in the secretive realm of national security — are as open and understandable as possible to enable informed public scrutiny and deliberation. The legitimate requirement of operational secrecy must be balanced with the need to prevent abuse and promote democratic debate. Reforms must be assessed for how they affect this balance.

Oversight means that the actions of law enforcement and national security organizations are subject to meaningful independent scrutiny. Courts, elected officials and independent review bodies provide the checks necessary to ensure surveillance powers are exercised lawfully and proportionately. Expansions of surveillance powers must be examined for their impacts on external oversight, with attention to whether they create gaps in accountability.

Together, these considerations provide a way of evaluating lawful access not as a narrow question of constitutionality, but as a broader test of Bill C-2's implications for democratic accountability at the institutional level.

Transparency

Critics suggest the Strong Borders Act is a "Trojan Horse" law (Larsen 2025). The bill would significantly expand government access to personal information about Canadian residents for investigative purposes that have little to do with border security. The "undemocratic practice" of packing wide-ranging legislative proposals into expansive omnibus bills, expediting political agendas by fracturing debate, has become common in Canada (Dodek 2017). Critics of Bill C-2 argue that burying lawful access in an omnibus bill is a bad-faith attempt to blunt civil liberties opposition and exploit American pressure for tighter border security (Geist 2025a). Kate Robertson (2025) describes how the law quietly sets the foundation for Canada's participation in expansive and undeclared international law enforcement data-sharing agreements. Considering these factors, it appears Bill C-2 has been presented to the public in a manner that precludes the possibility of meaningful democratic debate about the extent of the changes it would make.

On top of transparency concerns regarding how the proposed changes were tabled, the bill itself creates important transparency deficits by failing to account for how information accessed by officials is documented and reported. Under the current lawful access rules, major telecommunications providers voluntarily publish annual transparency reports disclosing the number of law enforcement requests for information they received that year (OPC 2016). The broad scope of service providers covered in Bill C-2 means that a much wider range of organizations will be subject to information demands and production orders, many of whom will lack the resources and incentives to publicly disclose them. Charter critiques of lawful access have argued the broad definition of service providers means that doctors, lawyers or psychologists could be required to disclose information about their clients, challenging their confidentiality obligations (Woolf 2025b; Geist 2025c). But Michael Geist points out this broad definition will also undermine existing norms of voluntary reporting: "Every law firm isn't going to provide a transparency report on how many requests they've faced" (Lake 2025). Even if every small business that received these requests did disclose them, this information would remain fragmented and difficult to assess in the aggregate.

Codifying the ability to issue information demands may generate a paper trail that could, in theory, be disclosed in court or used to monitor the overall use of these powers. But the introduction of formal information demands is accompanied by the legalization of existing informal practices. The bill includes provisions explicitly permitting voluntary disclosures — flows of data from third parties to security agencies requiring no standard documentation — and the use of data that is already publicly available.[17] The latter appears to constitute permission to purchase data from private brokers, a practice commonly employed in the United States to circumvent the need for warranted access to information (Robertson 2025; Larkin and Abuzneid 2024). The use of a broad definition of "publicly available information" may also leave the door open to using hacked, stolen or leaked data that has entered the public domain.[18]

This means police and intelligence personnel may collate voluntary disclosures and public information, within the constraints of privacy laws, to infer details that might otherwise require a warrant without disclosing this to any outside authority.

17 Bill C-2, *supra* note 1, cls 164, 185, s 20.24(1).

18 *Ibid*, cl 164.

Additionally, if service providers know they can be compelled to provide certain information, they may deem undocumented voluntary disclosures preferable to formal information demands or production orders. They may find that voluntary disclosure reduces the administrative burden of compliance, lowers reputational and legal liability because there is no formal record of the disclosure, and helps maintain positive relationships with national security and law enforcement agencies. Formalizing these back channels entrenches secrecy and limits any potential transparency gains associated with formally documented information demands.

In addition to undermining existing transparency norms and formally sanctioning the use of under-documented back channels, Bill C-2 notably does not contain any provisions requiring agencies using lawful access powers to report on their use. This sets the proposed lawful access regime apart from other national security information policy under legislation such as the Security of Canada Information Disclosure Act,[19] the data set regime under the CSIS Act,[20] and the Avoiding Complicity in Mistreatment by Foreign Entities (ACA) Act,[21] which all require some form of record-keeping and regular reporting to oversight bodies. Certain information collection and disclosure activities would fall within the scope of existing reporting requirements, particularly between CSIS and NSIRA,[22] and to a lesser extent between the RCMP, the Canada Border Services Agency (CBSA) and the planned Public Complaints and Review Commission (PCRC).[23] But for the most part, information demands, voluntary disclosures and privately sourced information fall outside existing requirements, and there is no specific obligation to track or report how often powers of lawful access are used and in what context.

Finally, Robert Diab (2025a) argues that "sweeping confidentiality provisions" under the SAAIA create opportunities for abuse. The act compels electronic service providers (ESPs) to develop technical capabilities granting law enforcement and intelligence agencies access to data ranging from subscriber information to intercepted communications in line with existing warrant and production-order requirements.[24] There is a clear obligation to assist in implementing requests under the SAAIA, accompanied by a comprehensive regime of audits, inspections and penalties to ensure compliance.[25] While an ESP may challenge a demand it believes is unlawful in court,[26] they have no obligation or even necessarily the ability to oversee the lawful use of these capabilities and are prohibited from disclosing their existence to the public. This design poses "a likely impediment to holding police or CSIS agents accountable," since unlawful or overbroad searches that do not culminate in criminal charges or sanctions against ESPs are unlikely to ever surface (ibid., 21).

19 *Security of Canada Information Disclosure Act*, SC 2015, c 20, s 2.

20 *CSIS Act*, RSC 1985, c C-23, ss 11.01–11.25.

21 *Avoiding Complicity in Mistreatment by Foreign Entities Act*, SC 2019, c 13, s 49.1 [*ACMFE Act*].

22 *ACMFE Act*, *supra* note 21, ss 6, 8; *National Security Intelligence Review Agency Act*, SC 2019, c 13, s 22, ss 6(4), 11.25, 12.1(3.5), 17(2), 19(3), 20.1(26) [*NSIRA Act*].

23 The PCRC will investigate complaints and conduct reviews of the RCMP and the CBSA that are not national security related. See *Public Complaints and Review Commission Act*, SC 2024, c 25.

24 *Ibid*, cl 194, s 5.

25 *Ibid*, cl 194, ss 5, 14, 18–45.

26 *Ibid*, cl 194, s 16.

Oversight

Bill C-2's shortfalls in transparency bleed into inadequacies in its provisions for independent oversight. Charter critiques have emphasized that despite being limited to basic details, information demands could "paint a detailed picture of your activities simply by confirming the various companies you interacted with" without judicial oversight (Woolf 2025b). But critics have paid less attention to how the bill preserves, and even modestly extends, judicial discretion. Judges would have new explicit powers to limit examination warrants to specific digital data or specified classes of information.[27] There are also provisions allowing judges to limit direct police access to digital systems by requiring a third party to mediate access to warranted information.[28] Judicial authorization would be required to obtain a production order for subscriber information and for peace officers to request such information from foreign jurisdictions, albeit against the relatively low standard of having "reasonable grounds to suspect" an offence has or will be committed.[29] Companies that receive information demands or production orders can request a judicial review within five days,[30] although some claim this is insufficient and creates a loophole where an order may be issued but not immediately served (Lake 2025).

Whereas provisions in part 14 lean on judicial authority for oversight, the SAAIA (part 15) defers more responsibility for oversight to executive discretion. Cabinet is empowered to set sweeping regulations requiring ESPs to develop surveillance capabilities, install hardware and comply with ministerial orders.[31] The minister and their delegates can grant exemptions, issue compliance orders and send inspectors into private premises while also adjudicating alleged violations.[32] Judicial review is available, but only after the ESP provides the minister with at least 15 days' notice, effectively positioning the executive as the primary arbiter of how law enforcement and intelligence agencies may use powers legislated under the SAAIA.[33]

While the implications of lawful access for judicial and ministerial authority are largely contained in the text of the law, independent oversight bodies such as NSIRA and the ICO are not mentioned at all. Maintaining the status quo would mean that information-sharing activities with some connection to national security remain subject to NSIRA investigation and review.[34] The Privacy Commissioner retains the right to investigate complaints and initiate audits regarding breaches of privacy law.[35] Some CSIS information collection practices under the proposed regime may constitute data sets, thus falling under purview of the ICO. Beyond inadvertent overlaps with existing reporting mandates, there is no statutory requirement for independent oversight or review of lawful access.

27 *Ibid*, cl 156, s 487(2.5).

28 *Ibid*, cl 156, s 487(2.6).

29 *Ibid*, cl 159, s 487.0142, cl 160, s 487.0181.

30 *Ibid*, cl 158, s 487.0121(7).

31 *Ibid*, cl 194, ss 5(2), 17, 46.

32 *Ibid*, cl 194, ss 5–36.

33 *Ibid*, cl 194, s 16.

34 *NSIRA Act*, *supra* note 22, s 8.

35 See www.priv.gc.ca/en/about-the-opc/what-we-do/.

These gaps in independent oversight are particularly troubling considering Bill C-2's provisions for international information sharing. The Strong Borders Act positions Canada to ratify the Second Additional Protocol (2AP) to the Budapest Convention and to negotiate a bilateral agreement under the US Clarifying Lawful Overseas Use of Data (CLOUD) Act (Robertson 2025). Both instruments are designed to streamline and significantly scale up cross-border access to digital evidence compared to the current regime of mutual legal assistance treaties (MLATs). Bill C-2 itself requires both ministerial and judicial authorization for cross-border disclosures.[36] Yet Cynthia Khoo and Kate Robertson (2025) warn that through a CLOUD Act agreement, US officials may be authorized to demand data directly from Canadian providers. Kate Robertson and Verónica Arroyo (2024) further emphasize that the 2AP could enable transnational repression by allowing foreign states — including the United States — to target and monitor dissidents in Canada for activities that may be protected under Canadian law.

Even if Canada designs information-sharing frameworks to align with the Charter on paper, in practice maintaining robust safeguards over cross-border information exchanges has proven challenging in other contexts. NSIRA's most recently available review of the implementation of the ACA — a law designed to ensure Canadian authorities are not complicit in information sharing tied to torture or other forms of mistreatment — found that departments systematically underassess risks and fail to escalate serious cases for review (NSIRA 2024b), showing how the letter of the law and the law in action can diverge in complex cross-jurisdictional settings. Adding to this, Canadian authorities are unable to ensure downstream uses of data uphold Canadian laws and democratic norms (Wong, Duncan and Lake 2025). This is true of the MLAT process, where once information leaves Canada, the Canadian government has limited power to dictate how it is used. But the 2AP and CLOUD Act frameworks are designed for high-volume, expedited transfers of information, thereby amplifying these challenges. In the absence of a robust framework for independent oversight of lawful access and cross-border information sharing, the potential for systematic abuses and unaccountable harms is high.

Strengthening Democratic Accountability in the Strong Borders Act

Despite Bill C-2's deficits regarding transparency and oversight, the idea that the bill will create a regime of "Big Brother"-style mass surveillance is hyperbole. A strong role for judicial and ministerial oversight of state surveillance is preserved under the proposed regime, which aligns with updates made in other democratic jurisdictions (Diab 2025b). However, advocates and opposition law makers are right to be skeptical given the historical tendency of policing and national security agencies to test the limits of their authority. The lawful access regime proposed under the Strong Borders Act expands surveillance authority but does little to reinforce the institutions tasked with

36 Bill C-2, *supra* note 1, cl 183.

holding police and intelligence agencies accountable. This analysis highlights three main findings, each paired with a recommendation.

Key Finding 1

Burying lawful access in an omnibus bill inhibits open democratic debate, promoting mistrust and undermining the legitimacy of Canadian police and intelligence agencies.

- **Recommendation 1: Table parts 14 and 15 of the Strong Borders Act as standalone legislation.** A cloak-and-dagger approach to expanding surveillance powers undermines the legitimacy of Canadian policing and national security institutions. An open debate regarding the operational imperatives of lawful access to information will help ensure that law enforcement and intelligence agencies are defending democracy rather than undermining it.

Key Finding 2

The lack of reporting requirements makes the proposed lawful access regime less transparent and less accountable compared to other Canadian information law and policy.

- **Recommendation 2: Create a statutory requirement to publicly report administrative statistics on lawful access, including cross-border exchanges, voluntary disclosures and private data brokers.** Specific reporting requirements outlined in the regulations should include the number of information demands and production orders issued, how often law enforcement accessed information through voluntary disclosures or data brokers, and the number of foreign information requests sent and received under the regime. Such arrangements would align the lawful access regime with reporting requirements under legislation such as the Access to Information Act, the Security of Canada Information Disclosure Act and the ACA Act. These statistics should be broken down by jurisdiction as well as by the size and sector of service providers involved. A high-level report from each agency should be made available to the public on an annual basis, with more detailed reports sent to NSIRA and the PCRC.

Key Finding 3

The role for independent oversight over the implementation of lawful access is unclear and underdetermined.

- **Recommendation 3: Extend NSIRA and PCRC statutory mandates to include an annual joint review of the implementation of lawful access.** While NSIRA already reports annually on the implementation of the ACA, the kinds of information sharing proposed in Bill C-2 cut across the mandates of both organizations. NSIRA and the PCRC should independently review the implementation of lawful access within the scope of their respective mandates each year. To avoid the duplication of efforts due to overlaps in their mandates and to ensure consistent messaging, their reviews should be coordinated with findings synthesized into a joint annual report. This expanded remit should be reflected in the budgets of review and oversight agencies.

About the Author

Jamie Duncan is a former Digital Policy Hub doctoral fellow, a Ph.D. candidate at the University of Toronto's Centre for Criminology and Sociolegal Studies and an affiliate of the Schwartz Reisman Institute for Technology and Society. Jamie is an interdisciplinary social scientist studying information policy, technology governance and security. His work has appeared in academic journals such as *The British Journal of Criminology* and *Internet Policy Review*, as well as popular outlets such as *The Globe and Mail*. Jamie's doctoral research investigates the role of technology adoption in deepening international cooperation on border security among the Five Eyes partners (Australia, Canada, New Zealand, the United Kingdom and the United States).

Acronyms and Abbreviations

ACA	Avoiding Complicity in Mistreatment by Foreign Entities
CBSA	Canada Border Services Agency
CLOUD Act	Clarifying Lawful Overseas Use of Data Act
CSIS	Canadian Security Intelligence Service
ESPs	electronic service providers
ICO	Office of the Intelligence Commissioner
IP	internet protocol
MLATs	mutual legal assistance treaties
NSIRA	National Security and Intelligence Review Agency
OPC	Office of the Privacy Commission
PCRC	Public Complaints and Review Commission
RCMP	Royal Canadian Mounted Police
SAAIA	Supporting Authorized Access to Information Act
2AP	Second Additional Protocol

Works Cited

Appel, Jeremy. 2025. “Carney’s Capitulation.” *The Orchard* (blog), June 4. www.readtheorchard.org/p/carney-bends-the-knee-to-trump-on.

Brodeur, Jean-Paul. 2010. *The Policing Web*. Oxford, UK: Oxford University Press.

Canadian Association of Chiefs of Police. “Statement: Canada’s Police Chiefs Welcome the *Strong Borders Act*.” June 4. www.cacp.ca/_Library/Position_Statements/CACP_Statement_-_Bill_C-2_Strong_Borders_Act.pdf.

Carney, Bryan. 2020. “Clearview, Maker of RCMP’s Facial Recognition Software, Exits Canada.” The Tyee, July 7. https://thetyee.ca/News/2020/07/07/Clearview-AI-Exits-Canada/.

Clarke, Amanda. 2019. *Opening the Government of Canada: The Federal Bureaucracy in the Digital Age*. Vancouver, BC: UBC Press.

Diab, Robert. 2025a. “Bill C-2 Backgrounder: New Search Powers in the Strong Borders Act and Their Charter Compliance.” *Criminal Law Quarterly* 73 (3). http://dx.doi.org/10.2139/ssrn.5363319.

– – –. 2025b. “Canada’s Lawful Access Bill: Heavy on Secrecy, Light on Accountability.” Opinion, Centre for International Governance Innovation, July 15. www.cigionline.org/articles/canadas-lawful-access-bill-heavy-on-secrecy-light-on-accountability/.

Dodek, Adam M. 2017. “Omnibus Bills: Constitutional Constraints and Legislative Liberations.” *Ottawa Law Review* 48 (1). https://rdo-olr.org/omnibus-bills-constitutional-constraints-and-legislative-liberations/.

Economist Intelligence. 2025. “EIU’s 2024 Democracy Index: trend of global democratic decline and strengthening authoritarianism continues through 2024.” February 27. www.eiu.com/n/democracy-index-2024/.

Geist, Michael. 2025a. “Privacy at Risk: Government Buries Lawful Access Provisions in New Border Bill.” *Michael Geist* (blog), June 4. www.michaelgeist.ca/2025/06/privacy-at-risk-government-buries-lawful-access-provisions-in-new-border-bill/.

– – –. 2025b. “Lawful Access on Steroids: Why Bill C-2’s Big Brother Tactics Combine Expansive Warrantless Disclosure with Unprecedented Secrecy.” *Michael Geist* (blog), June 20. www.michaelgeist.ca/2025/06/lawful-access-on-steroids/.

– – –. 2025c. “Why Bill C-2 Faces a Likely Constitutional Challenge By Placing Solicitor-Client Privilege at Risk.” *Michael Geist* (blog), June 25. www.michaelgeist.ca/2025/06/why-bill-c-2-faces-a-likely-constitutional-challenge-by-placing-solicitor-client-privilege-at-risk/.

Gorokhovskaia, Yana and Cathryn Grothe. 2025. *Freedom in the World 2025: The Uphill Battle to Safeguard Rights*. Washington, DC: Freedom House. https://freedomhouse.org/report/freedom-world/2025/uphill-battle-to-safeguard-rights.

Khoo, Cynthia and Kate Robertson. 2025. “Canada-U.S. Cross-Border Surveillance Negotiations Raise Constitutional and Human Rights Whirlwind under U.S. CLOUD Act.” The Citizen Lab, February 24. https://citizenlab.ca/2025/02/canada-us-cross-border-surveillance-cloud-act/.

Lake, Holly. 2025. “A big brother bill.” *National Magazine*, July 21. https://nationalmagazine.ca/en-ca/articles/law/in-depth/2025/a-big-brother-bill.

Larkin, Samantha B. and Shakour Abuzneid. 2024. "Ending Privacy's Gremlin: Stopping the Data-Broker Loophole to the Fourth Amendment's Search Warrant Requirement." *Journal of Information Security* 15 (4): 589–611. https://doi.org/10.4236/jis.2024.154033.

Larsen, Mike. 2025. "Liberal government's troubling approach to privacy revealed in new legislation." FIPA, June 10. https://fipa.bc.ca/research-resources/2025-bill-c-2-and-c-4/.

Leuprecht, Christian and Hayley McNorton. 2021. *Intelligence as Democratic Statecraft: Accountability and Governance of Civil-Intelligence Relations Across the Five Eyes Security Community — the United States, United Kingdom, Canada, Australia, and New Zealand*. Oxford, UK: University Press.

Lyon, David. 2014. "Surveillance, Snowden, and Big Data: Capacities, consequences, critique." *Big Data & Society* 1 (2). https://doi.org/10.1177/2053951714541861.

McMullen, Greg. 2022. "Pulling Back the Curtain on Canada's Mass Surveillance Programs – Part One: A Decade of Secret Spy Hearings." British Columbia Civil Liberties Association, December 14. https://bccla.org/2022/12/pulling-back-the-curtain-on-canadas-mass-surveillance-programs-part-one-a-decade-of-secret-spy-hearings/.

– – –. 2023. "Pulling Back the Curtain on Canada's Mass Surveillance Programs – Part Two: The CSE Secret Spying Archive." British Columbia Civil Liberties Association, March 16. https://bccla.org/2023/03/pulling-back-the-curtain-on-canadas-mass-surveillance-programs-part-two-the-cse-secret-spying-archive/.

Nord, Marina, David Altman, Fabio Angiolillo, Tiago Fernandes, Ana Good God and Staffan I. Lindberg. 2025. *Democracy Report 2025: 25 Years of Autocratization — Democracy Trumped?* Gothenburg, Sweden: V-Dem Institute, Department of Political Science, University of Gothenburg. www.v-dem.net/documents/61/v-dem-dr__2025_lowres_v2.pdf.

NSIRA. 2024a. *NSIRA Review of CSIS Dataset Regime*. March 27. Ottawa, ON: NSIRA. https://nsira-ossnr.gc.ca/en/reviews/find-a-review/21-15/report/.

– – –. 2024b. *Review of departmental implementation of the Avoiding Complicity in Mistreatment by Foreign Entities Act for 2022*. Report. Ottawa, ON: NSIRA. https://publications.gc.ca/site/fra/9.954895/publication.html.

OPC. 2016. *Consultation on Canada's National Security Framework*. December 5. Ottawa, ON: OPC. www.priv.gc.ca/en/opc-actions-and-decisions/submissions-to-consultations/sub_psc_161205/.

– – –. 2021. "RCMP's use of Clearview AI's facial recognition technology violated *Privacy Act*, investigation concludes." News Release, June 10. www.priv.gc.ca/en/opc-news/news-and-announcements/2021/nr-c_210610/.

– – –. 2024. *Investigation of the RCMP's collection of open-source information under Project Wide Awake*. Special Report to Parliament. Gatineau, QC: OPC. www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/202324/sr_pa_20240215_rcmp-pwa/.

OpenMedia. 2025. "Over 300 Organizations Unite to Demand Complete Withdrawal of Bill C-2." Press release, June 18. https://openmedia.org/press/item/over-300-organizations-unite-to-demand-complete-withdrawal-of-bill-c-2.

Parsons, Christopher. 2015. "Stuck on the Agenda: Drawing Lessons from the Stagnation of 'Lawful Access' Legislation in Canada." In *Law, Privacy and Surveillance in Canada in the Post-Snowden Era*, edited by Michael Geist, 257–83. Ottawa, ON: University of Ottawa Press.

Robertson, Kate. 2025. “Unspoken Implications: A Preliminary Analysis of Bill C-2 and Canada’s Potential Data-Sharing Obligations Towards the United States and Other Countries.” The Citizen Lab, June 16. https://citizenlab.ca/2025/06/a-preliminary-analysis-of-bill-c-2/.

Robertson, Kate and Verónica Arroyo. 2024. “Expediting Human Rights Abuses: A Constitutional and Human Rights Analysis of the Second Additional Protocol to the *Budapest Convention on Cybercrime*.” March. Toronto, ON: The Citizen Lab, Munk School of Global Affairs & Public Policy, University of Toronto. https://citizenlab.ca/wp-content/uploads/2025/06/PDF-copy-June-2025-Submission.pdf.

Tunney, Catharine. 2025. “Liberals hoped their border bill would quickly pass. Now they’re aiming for next year.” CBC News, November 22. www.cbc.ca/news/politics/border-security-bill-c-12-9.6988286.

Wong, Wendy H., Jamie Duncan and David A. Lake. 2025. “Why data about people are so hard to govern.” *Regulation & Governance* 19 (1): 236–52. https://doi.org/10.1111/rego.12591.

Woolf, Marie. 2025a. “Border security bill would give law enforcement access to internet subscriber information without a warrant.” *The Globe and Mail*, June 4. www.theglobeandmail.com/canada/article-strong-borders-act-law-enforcement-internet-information-access/.

– – –. 2025b. “Border bill powers would allow warrantless police requests to doctors, abortion clinics, hotels.” *The Globe and Mail*, June 16. www.theglobeandmail.com/politics/article-border-bill-csis-snooping-powers/.

Zuboff, Shoshana. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York, NY: Public Affairs.