2025

The Quiet Resurrection of Lawful Access

An Analysis of Bill C-2

ZHAO, JULIA

CIPPIC—the Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic—is a legal clinic based at the University of Ottawa's Faculty of Law. Its mandate is to advocate for the public interest on matters arising at the intersection of law and technology.

This document is intended for informational purposes only and should not be interpreted as legal advice. For inquiries or further information, please contact cippic@uottawa.ca.

Table of Contents

Introduction

In May 2025, the federal government introduced Bill C-2, *The Strong Borders Act*, to expand lawful access powers in Canada. Bill C-2 proposed warrantless access to basic subscriber information, authorized secret ministerial directives to service providers, and imposed technical requirements to support government surveillance.[1] As a result, civil society groups, legal experts, and opposition MPs criticized the bill for overstepping privacy protections. In October 2025, the government responded by withdrawing Bill C-2 and introducing a new bill, the *Strengthening Canada's Immigration System and Borders Act* ("Bill C-12"), that excluded the controversial lawful access provisions of Bill C-2.[2]

Public Safety Minister Gary Anandasangaree insisted that introducing Bill C-12 did not represent a retreat. He framed the change as a matter of sequencing, saying the government intended to advance border and immigration measures first and revisit lawful access powers later.[3] The timing and content of Bill C-12, however, suggest that the government more likely removed the contested provisions in response to public opposition.[4] Civil liberties groups welcomed the shift but cautioned that it indicated only a delay in expanding surveillance powers, not a resolution.

Concerns about Bill C-2 extended beyond the content of its proposals. The legislative process raised questions about transparency and oversight. The government introduced the bill without public consultation or supporting evidence, and presented it as part of a larger border security bill. Canadians noticed, and the government ultimately withdrew the provisions.

Bill C-2 warrants attention not only for its substance, but also for the manner in which it was advanced by the government. This short report examines three issues related to Bill C-2: the evolution of lawful access legislation in Canada, the key provisions of Bill C-2, and what this episode reveals about the current state of privacy protection, democratic accountability, and civil liberties.

---

[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.
[2] 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.
[3] Canada, Public Safety, "Government of Canada introduces new streamlined legislation to strengthen border security and keep Canadians safe" (8 October 2025), online (news releases): <https://www.canada.ca/en/public-safety-canada/news/2025/10/government-of-canada-introduces-new-streamlined-legislation-to-strengthen-border-security-and-keep-canadians-safe.html>.
[4] Sean Boynton, "Liberals table new border bill separating plan for warrantless data demands - National | Globalnews.ca", online: *Global News* <https://globalnews.ca/news/11470122/border-security-bill-privacy-revamp/>.

History of Lawful Access Provisions

Canadian governments have been seeking to expand lawful access powers for decades. Bill C-2 followed earlier proposals to expand police search and seizure powers in digital contexts such as Bill C-52 (*Investigating and Preventing Criminal Electronic Communications Act*) and Bill C-30 (*Protecting Children from Internet Predators Act*). These bills would have required service providers to build interception capabilities and disclose subscriber information upon request. Although framed as tools to fight cybercrime or protect children, both bills faced criticism for allowing access to personal data based on low thresholds like "reasonable grounds to suspect." In the end, Bill C-52 did not proceed after the dissolution of Parliament, while Bill C-30 was withdrawn following public backlash and concerns raised by privacy commissioners.

Bill C-13, introduced in 2013 as the *Protecting Canadians from Online Crime Act*, succeeded where its predecessors failed. The bill introduced several surveillance-related provisions, including preservation demands, production orders for transmission and tracking data based on "reasonable suspicion," and legal immunity for service providers.[5] These measures formed part of a broader bill on online harms, prompted by cases like the Amanda Todd tragedy,[6] and included technical amendments to the *Criminal Code*. With minimal oversight, the bill left open the possibility for expanded surveillance in future legislation.

Around the same time, the Supreme Court's decision in *R. v. Spencer* significantly altered the legal landscape for privacy. The Court held that linking an IP address to an individual constitutes a search under s. 8 of the Charter and that neither section 487.014 of the *Criminal Code* nor *PIPEDA* provided lawful authority for such disclosure.[7] After *Spencer*, police required a warrant to compel subscriber information.

Bill C-2 appears to respond to the constraints imposed by the *Spencer* decision. The bill aimed to formalize access to subscriber data by authorizing demand powers, lowering the threshold for disclosure,

---

[5] Bill C-13, *An Act to amend the Criminal Code, the Canada Evidence Act, the Competition Act and the Mutual Legal Assistance in Criminal Matters Act*, 2nd Sess, 41st Parl, 2014 (assented to 9 December 2014), SC 2014, c 31.
[6] Julia Nicol & Dominique Valiquet, "Legislative Summary for Bill C-13", online: <https://lop.parl.ca/sites/PublicWebsite/default/en_CA/ResearchPublications/LegislativeSummaries/412C13E>.
[7] *R v Spencer*, 2014 SCC 43.

and imposing technical obligations on service providers. It quickly drew legal and political opposition for overreach, lack of transparency, and potential constitutional violations. Lacking support, the government replaced Bill C-2 with Bill C-12, which retained the border-related measures, but removed the surveillance provisions. This outcome suggests that any future effort to expand lawful access powers will need to justify warrantless access as both necessary for investigations and consistent with constitutional standards.

C-2

1. Procedural Controversy

The controversy surrounding Bill C-2 was not only about the powers it proposed, but also about how the federal government advanced the bill, raising concerns about transparency, consultation, and evidence-based justification.

First, the bill was developed without public consultation. Despite its implications for privacy, the government did not engage legal experts, civil society groups, privacy commissioners, or other stakeholders. Parliament also appeared unprepared to evaluate the implementation of the bill's expanded powers across areas like policing, border enforcement, and digital surveillance.[8] Given the bill's potential to reshape the relationship between the state and citizens, the absence of engagement was both unusual and unsettling.

Second, the government embedded the surveillance powers inside an omnibus bill framed as a border security initiative. Titled the *Strong Borders Act*, the government marketed Bill C-2 as a response to organized crime, fentanyl trafficking, and cross-border enforcement challenges. In reality, it included provisions that had little to do with borders and everything to do with expanding surveillance: warrantless access to subscriber data, secret ministerial directives to compel service providers, and technical mandates requiring companies to support government access.

Third, the bill lacked a credible evidentiary foundation to support the expansion of lawful access powers. The government presented no data to show that current investigative powers were inadequate; it offered no examples of failed prosecutions, no statistics on delays or refusals, and no comparative analysis of international standards. Even the Charter Statement defending the bill characterized the proposed powers as minor extensions of existing law, despite clear conflicts with recent Supreme Court decisions.[9] These justifications rest on political messaging rather than legal or empirical support.

---

[8] Canada, House of Commons, *Debates*, 45-1, No. 9 (5 June 2025), online: <https://www.ourcommons.ca/DocumentViewer/en/45-1/house/sitting-9/hansard#13083890>.

[9] Department of Justice Government of Canada, "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" (19 June 2025), online: <https://www.justice.gc.ca/eng/csj-sjc/pl/charter-charte/c2_2.html>.

2. Proposed Substantive Powers

The most consequential elements of Bill C-2 were in Parts 14 and 15, which proposed sweeping new powers to access digital information. These provisions departed sharply from the bill's stated focus on border and public safety, introducing structural changes to Canada's privacy framework that extended far beyond infrastructure or customs reform.

a) Timely Access to Data and Information

Part 14, *Timely Access to Data and Information*, amended the *Criminal Code* to create new forms of information demands and production orders. A key provision would have allowed peace officers or public officers to demand basic customer information from telecommunications or internet service providers without prior judicial authorization (s. 487.0121(1)), which would have constituted a warrantless search. The threshold was only "reasonable grounds to suspect" (s. 487.0121(2)), a lower standard than probable cause.

Officers could also have imposed gag orders on recipients, but service providers had only five days to challenge them under s. 487.0121(7). This was an unrealistically short window, as the order might not have reached the appropriate legal department before the deadline passed.

The Bill limited grounds for challenge to situations where compliance would have been unreasonable or where privileged information would have been disclosed (s. 487.0121(10)). Under s. 487.0121(1), the demand covered a range of subscriber details, but the most concerning part was clause (e), which obliged disclosure of other service providers the customer might have used. For example, if an ISP had a Hotmail address on file, it could have been required to disclose that the customer was also a Microsoft user. Where accounts were tied to single-sign-on systems like Microsoft or Google logins, this could have exposed a broader network of linked services. The government framed this as a triage tool that was intended to help police identify jurisdiction from an IP address, but its scope extended much further.

Alongside this, the Bill introduced a new production order for subscriber information (s. 487.0142(1)), which did require judicial authorization. However, the threshold remained "reasonable suspicion" that any federal offence had been or would be committed (s. 487.0142(2)). The order compelled disclosure of "all subscriber information" in the provider's possession. That term was defined in s. 487.011 as including name, pseudonym, address, telephone number, email address, account identifiers, service types and periods, among others. Unlike traditional production orders, which specified the data sought, this order

captured a wide range of information by default. It was also not limited to serious crimes, as even minor offences under statutes such as the *National Parks Act* could have triggered it.[10]

The Bill also strengthened the framework for voluntary disclosure. Police retained the ability to request information informally, and the amendments granted immunity to service providers who chose to comply (s. 487.0195(2)-(3)), even if their contractual terms limited cooperation to situations "required by law." These provisions weakened privacy assurances made to customers and increased institutional pressure to comply with police requests. The Bill also authorized officers to rely on "publicly available" information (s. 487.0195(4)), but because the term was not defined, it could have been interpreted broadly to include leaked or hacked datasets.

The Bill further codified exigent circumstances. Where there was an imminent risk to life or danger of evidence destruction, and it was impracticable to obtain a warrant, officers could have issued demands with immediate legal effect (s. 487.11(a)-(b)). Another change introduced a new kind of warrant for tracking or transmission data. Judges could have authorized collection not only for the specified device or account, but also for any "similar" device or item discovered later (s. 492.2(1.1)). While this allowed investigators to expand surveillance without returning to court, it raised concerns about vagueness and overbreadth.

Finally, the bill proposed a new mechanism for cross-border requests. A judge could have authorized an officer to issue a request, not a binding order, to a foreign telecom provider for subscriber or transmission data (s. 487.0181(1)-(4)). The threshold was again only reasonable suspicion. Compliance remained voluntary and depended on the foreign provider's own legal obligations.

b) Supporting Authorized Access to Information Act

Part 15, *Supporting Authorized Access to Information Act*, created a new statutory regime to mandate service access that went beyond the *Criminal Code* and *CSIS Act*. Its purpose was to ensure that electronic service providers (ESPs) could build and maintain the capacity to give police and intelligence agencies access to information (s. 3).

The definitions were deliberately broad: an ESP could have been almost anyone offering digital services in Canada (s. 2). "Access" included interception of communications, and "information" covered any

[10] PrivacyLawyer, "#LawfulAccess is back: An overview of Part 14 of Bill C-2: Strong Borders Act" (8 June 2025), online (Youtube): <https://youtu.be/wOgo4TuoJec?si=GGSFpE8Ooco-jrin>.

intelligence or data authorized under the *Criminal Code* or *CSIS Act*. This gave the statute sweeping reach over internet platforms, cloud providers, and telecoms.

The most significant privacy issue arose from the obligations imposed on "core providers." Cabinet could have designated classes of core providers (s. 5(1)) and then required them to install and maintain technical capabilities to extract, organize, and deliver subscriber information (s. 5(2)). While there was an exemption where compliance would have required introducing a "systemic vulnerability" (s. 5(3)), the term was undefined and left to Cabinet to flesh out in regulation. This opened the door for the government to narrow the protection and potentially mandate designs that weakened encryption.

Beyond core providers, the Minister of Public Safety could have issued secret orders to any ESP, even if they were not "core." Orders were exempt from publication (s. 7(5)), as ESPs were barred from disclosing their existence (s. 15), and the Minister decided whether compensation was paid (s. 7(3)). These secrecy provisions meant that users had no way of knowing when their provider was compelled to facilitate surveillance.

There was a general obligation to assist: on request from a peace officer, CSIS employee, or the Minister, all ESPs had to provide reasonable assistance to test or enable access equipment (s. 14). Combined with the confidentiality rules, this gave the government broad coercive reach while shielding the process from public scrutiny.

Enforcement was backed by inspections (s. 19), mandatory internal audits (ss. 21-22), compliance orders (ss. 23-26), and significant penalties. Administrative monetary penalties could have reached up to $250,000 per violation, and criminal fines could have been up to $500,000 for corporations and $100,000 for individuals (ss. 27-45).

Implications

1. Personal Privacy and Surveillance

Bill C-2 would have changed how the government interacted with Canadians online. It authorized police and federal agencies to demand subscriber data from service providers without a warrant. This included names, addresses, email accounts, IP histories, device identifiers, and other information that connected a person to their digital activity.[11]

This data is biographically rich, and can map a person's identity and behaviour. An IP address can reveal one's location, the websites they visit, who they talk to, and the services they use. In *Bykovets*, the Court confirmed that an IP address attracts a reasonable expectation of privacy under s. 8 of the *Charter*, describing it as "the key to unlocking a user's Internet activity and, ultimately, their identity."[12] Under Bill C-2, the government could have accessed this data based only on "reasonable suspicion," without any requirement for judicial approval or notice to the person being investigated.

The impact would have been widespread. The Bill applied not just to telecom companies, but to any business or organization that provided services to the public. This included internet providers, email services, hospitals, schools, cloud storage companies, online retailers, banks, and legal service platforms. Police could have asked whether a named person had used a service, what devices were involved, and when and where that activity took place.

Imagine going to a therapist through a virtual mental health app. Under Bill C-2, that company could have been compelled to confirm that you were a user, and potentially shared details that identified you, without your knowledge, without a warrant, and without a judge reviewing the request. That information could later have been disclosed to other departments or foreign governments.

2. Costs for Businesses and Consumers

The law also created new compliance burdens for businesses. If a provider received a demand for information, they had only 24 hours to respond and five days to challenge the order. The bill empowered the Minister of Public Safety to secretly require certain "core" service providers to redesign their systems to enable real-time surveillance or data access. These obligations could have remained confidential, with

[11] Holly Lake, "A Big Brother Bill" (21 July 2025), online: *National Magazine* <https://nationalmagazine.ca/en-ca/articles/law/in-depth/2025/a-big-brother-bill>.
[12] *R v Bykovets*, 2024 SCC 6.

no public reporting or oversight.

For small or mid-sized companies, the cost of redesigning infrastructure, hiring compliance staff, or retaining legal counsel would have been significant.[13] These businesses might have passed those costs along to users through higher fees, reduced services, or changes to privacy policies. For example, an independent internet provider might have introduced new charges to cover compliance, or a medical app might have started collecting less data to reduce liability, even if that weakened the service. Customers would have been affected without even knowing why.

The pressure to comply quickly, in secret, and without guidance would have created confusion and legal risk. Some industries, especially healthcare, finance, and legal services, already follow strict privacy rules. Bill C-2 placed them in an impossible position: comply with government orders and risk violating professional or legal confidentiality, or resist and face financial penalties as high as $500,000.

3. Hidden Surveillance and Chilling Effects

For individuals, the secrecy surrounding these powers was troubling, as Bill C-2 contained no requirement to notify people that their data had been accessed. Gag orders could have prevented service providers from saying anything for up to a year. Most people would've never known they had been surveilled, leading to a chilling effect: If people are unsure if their internet searches, support group memberships, or communications could trigger surveillance, they may think twice before seeking help or expressing themselves. The fear of being watched could have discouraged people from searching for sensitive information, accessing legal advice, or even contacting a therapist.

4. Disproportionate Harm to Vulnerable Groups

This effect could've been especially serious for vulnerable groups. Refugees, asylum seekers, and racialized communities already experience higher levels of surveillance.[14] Bill C-2 allowed for broad data sharing between government agencies and foreign partners.[15] That included the potential for immigration-related data to reach authorities in other countries, even those with poor human rights records.

---

[13] "Bill C-2: Strong Borders Act Introduces Lawful Access and Data Disclosure Regime" (25 June 2025), online: <https://www.fasken.com/en/knowledge/2025/06/bill-c2-strong-borders-act-introduces-lawful-access-and-data-disclosure-regime>.

[14] "Statement on Bill C-2 | Canadian Council for Refugees" (5 June 2025), online: <https://ccrweb.ca/en/statement-bill-c-2>.

[15] Tamir Israel, "CCLA and coalition of coalitions call for withdrawal of Bill C-2" (11 July 2025), online: *CCLA* <https://ccla.org/privacy/ccla-joins-calls-for-withdrawal-of-bill-c-2/>.

The Canadian Council for Refugees warned that this kind of sharing could expose people to danger, including persecution or retaliation. These concerns were not abstract. In the *Maher Arar* case, Canadian officials shared inaccurate information with U.S. authorities, resulting in Mr. Arar being detained, rendered, and tortured in Syria.[16] Bill C-2 could've had similar outcomes by enabling wider, faster, and less accountable information sharing.

5. Cross-border Surveillance and Data Protection

The Bill was also designed to support Canada's participation in the Second Additional Protocol to the Budapest Convention.[17] This treaty allowed for foreign governments to request subscriber data directly from Canadian service providers. In most cases, those requests would not require court oversight in Canada. The Privacy Commissioner of Canada has criticized Canada's current legal regime as lacking "comprehensive, appropriate, and robust safeguards"[18] for digital-era sharing. The Bill also laid the groundwork for future data-sharing deals under the *U.S. CLOUD Act*. Unlike Canadian law, the United States does not recognize a privacy right for data shared with service providers.[19] After Canadian information enters U.S. systems, intelligence agencies may retrieve and circulate it among departments. Canadian residents have limited means to influence its subsequent use.

Summary of Concerns

Bill C-2 eroded the basic structures of democratic accountability. It did not include mandatory notice provisions for individuals, regular reporting to Parliament, or transparency obligations for service providers. Many organizations, especially those outside the tech sector, might not even realize they were subject to the law, and others might comply without understanding the legal risks to their users. People affected by surveillance would have few ways to find out, and fewer ways to push back. Bill C-2 would have created a system of broad, secretive, and largely unchecked surveillance. It would've affected ordinary internet users, patients, customers, students, and workers, not just criminal suspects. It would've shifted the costs and risks of surveillance onto businesses, institutions, and individuals, and it would've done so without meaningful public oversight.

---

[16] Lysanne Louter, "The Maher Arar Case" (6 March 2017), online: *Amnesty International Canada* <https://amnesty.ca/legal-brief/case-maher-arar/>.
[17] Kate Robertson, "Unspoken Implications: A Preliminary Analysis of Bill C-2 and Canada's Potential Data-Sharing Obligations Towards the United States and Other Countries" (16 June 2025), online: <https://citizenlab.ca/2025/06/a-preliminary-analysis-of-bill-c-2/>.
[18] *Ibid*.
[19] *Ibid*.

Conclusion

Bill C-2 proposed significant surveillance powers without adequate oversight or justification, prompting public criticism and raising constitutional concerns. In response, the government introduced Bill C-12, which removed those specific provisions but maintained the broader objective of expanding border-related issues. Government officials characterized the shift as a matter of sequencing, to advance border and immigration priorities first while taking additional time to review the surveillance elements, rather than a withdrawal or a commitment to public consultation.

Bill C-12 advances the same objectives as Bill C-2 through more limited and targeted measures. The challenge now is not how to sequence these powers, but whether they can be justified at all. If the government intends to pursue stronger state authority, it must first show why those powers are needed and how they will be kept in check. That means more than drafting limits on paper; it means meaningful public consultation, clear legal thresholds, independent oversight with the power to intervene, and structural protections that cannot be softened by regulation or buried in omnibus bills.