UNSPOKEN IMPLICATIONS

A Preliminary Analysis of Bill C-2 and Canada's Potential Data-Sharing Obligations Towards the United States and Other Countries

June 16, 2025
Report No. 187

By Kate Robertson

THECITIZENLAB
munk school
OF GLOBAL AFFAIRS & PUBLIC POLICY
UNIVERSITY OF TORONTO

Copyright

Suggested Citation

Kate Robertson. "Unspoken Implications: A Preliminary Analysis of Bill C-2 and Canada's Potential Data-Sharing Obligations Towards the United States and Other Countries," Citizen Lab Report No. 187, University of Toronto, June 16, 2025.

About the Citizen Lab, Munk School of Global Affairs & Public Policy, University of Toronto

The Citizen Lab is a world-renowned research unit led by Professor Ronald J. Deibert at the University of Toronto's Munk School of Global Affairs & Public Policy. We investigate novel threats to democracy, human rights, and global security in the digital ecosystem. Over the past 25 years, the Citizen Lab's evidence-based research has played a critical role in demonstrating how digital technologies are used to undermine human rights. The Citizen Lab has published more than 180 evidence-based, peer-reviewed research reports, available online.

Contents

Excerpt

Our preliminary analysis of Bill C-2 situates the legislation within the context of existing research by the Citizen Lab about two potential data-sharing treaties that are most relevant to the new proposed powers being introduced in Bill C-2: the Second Additional Protocol to the Budapest Convention (2AP) and the CLOUD Act. Both of which carry significant constitutional and human rights risks.

Introduction

On June 3, 2025, the federal government tabled 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. The bill is omnibus legislation that, if passed, would introduce a wide array of new federal agency and law enforcement powers, and would significantly reform substantive and due process laws in Canada for migrants and asylum seekers. It is widely known that Bill C-2 is being tabled at a time where the Canadian government has entered into negotiations with the United States on matters concerning trade and security.

For several years, Citizen Lab researchers have been studying cross-border surveillance practices and frameworks around the world, including most recently, potential cross-border data-sharing frameworks between foreign law enforcement authorities. Human rights dangers are particularly acute when it comes to the potential sharing of private, sensitive information with foreign governments and law enforcement authorities. Canadian authorities know first-hand the tragic consequences that inappropriate data sharing with foreign authorities can inflict on even innocent persons. The detention, rendition, and torture of Maher Arar after Canadian authorities shared inappropriate and inaccurate information with U.S. authorities provides a "chilling example of the dangers of unconditional information sharing." The Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar properly recognized that information sharing with foreign authorities "is a highly sensitive and potentially risky exercise."[1] Moreover, in the absence of robust human rights safeguards, foreign states are also able to leverage legal procedures in rights-respecting countries in order to engage in acts of transnational repression.

Despite the wider context of negotiations between Canada and the U.S., the federal government's public statements surrounding Bill C-2–including the Minister of Public Safety's official summary–have said surprisingly little about the impact of Bill C-2 on potential data-sharing obligations in Canada towards the United States. This explanatory gap is notable given the proposed new powers appear to carry

[1] Report of the Events Relating to Maher Arar: Analysis and Recommendations (Ottawa: Commission of Inquiry Into the Actions of Canadian Officials in Relation to Maher Arar, 2006) at page 74 (pdf). See also, Internal inquiry into the actions of Canadian officials in relation to Abdullah Almalki, Ahmad Abou-Elmaati and Muayyed Nureddin, The Honourable Frank Iacobucci, q.c. Commissioner (Ottawa, Ontario: Privy Council, 2008)

far-reaching implications for data-sharing that have not been acknowledged to the broader public by the federal government, to date, in introducing the legislation.

While Bill C-2 does not explicitly state that it is paving the way for new and expanded data-sharing with the United States or other countries, the legislation contains references to the potential for "agreement[s] or arrangement[s]" with a foreign state, and references elsewhere the potential that persons in Canada may become compelled by the laws of a foreign state to disclose information.[2] Other data and surveillance powers in Bill C-2 read like they could have been drafted by U.S. officials.

Furthermore, in response to questions at a technical briefing on Bill C-2 by Justice Canada on June 9, 2025, Justice Canada officials acknowledged to the persons present at the briefing that the intent of certain provisions within Bill C-2 is to enable Canada to implement and ratify a new data-sharing treaty, publicly known as the "Second Additional Protocol" to the Budapest Convention ("2AP"). The briefing acknowledged that other cross-border "cooperation" tools were foreseeable.

The federal government's quiet acknowledgement that new provisions in Bill C-2 are being introduced to implement the 2AP treaty raises broader questions about the full extent of Bill C-2's impacts as it concerns data-sharing with U.S. law enforcement authorities. Bill C-2 is 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 Canada and the United States under a piece of U.S. legislation called the Clarifying Lawful Overseas Use of Data Act ("CLOUD Act").

As a result, this preliminary analysis of Bill C-2 situates the legislation within the context of existing research by the Citizen Lab about two potential data-sharing treaties that are most relevant to the new proposed powers being introduced in Bill C-2. Part 2 introduces Citizen Lab research analyzing the constitutional and human rights implications of the 2AP. The research was previously submitted as part of the Department of Justice's 2024 consultation on its consideration of whether Canada should ratify the treaty. Part 3 connects Bill C-2's proposed powers to Citizen Lab's recent analysis of the constitutional and human rights implications of a potential CLOUD Act agreement with the United States. Both Parts 1 and 2 underscore the significant democratic, public interest, and human rights implications if Canada were to assume these new data-sharing obligations towards foreign law enforcement authorities. As a result, Parts 4-5 conclude by raising broader issues regarding the public's and Parliament's current inability to meaningfully assess the complex and consequential new powers in Bill C-2, given the federal government's current lack of transparency about its intent as regards to potential new data-sharing obligations towards the United States or other countries.

[2] 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, clause 160. See also clause 164 (proposing s 487.0195(3) of the Criminal Code, RSC 1985, c C-46).

2. The Potential Impact of the 2AP to the Budapest Convention: Expediting Human Rights Abuses

Given the government's acknowledgement that new powers in Bill C-2 are intended to enable Canada to ratify the 2AP, Part 2 of this preliminary analysis of Bill C-2 introduces in-depth analysis of 2AP, as one of the major cross-border data-sharing frameworks under consideration, between Canada and foreign law enforcement authorities in the United States and elsewhere. The Citizen Lab's analysis of the constitutional and international human rights implications of the 2AP provides broader context regarding the potential implications of Bill C-2, as it relates to the 2AP. The analysis was authored by Kate Robertson and Verónica Arroyo.[3]

The 2AP is a new law enforcement data-sharing treaty that is designed to bypass existing mutual legal assistance frameworks between countries, and to expand the speed and volume of data-sharing between law enforcement authorities in different countries. The United States is a signatory of the treaty and would potentially be making requests for Canadian data under the framework.[4] If Canada were to ratify the treaty, it would very likely prompt "a significant increase in the volume of requests for communication-related information by foreign and Canadian investigative entities, with a corresponding impact on the right to privacy."[5] Moreover, if the 2AP is adopted as a global standard, it would contribute to the elimination and diminishment of protections that are critical to mutual legal assistance treaties and norms. As a result, "much of the world's population may be left vulnerable to arbitrary and abusive data collection practices by domestic law enforcement agencies." Internationally, it has been the subject of significant criticism by human rights organizations around the world.
During a consultation in early 2024 on the question of whether Canada should ratify the 2AP, the Privacy Commissioner of Canada raised concerns with the Department of Justice about "significant privacy implications" of the treaty. The Privacy Commissioner analysis further makes clear that without much needed law reform, Canada does not have "comprehensive, appropriate, and robust safeguards", given

[3] Kate Robertson and Verónica Arroyo, "A Constitutional and Human Rights Law Analysis of the Second Additional Protocol to the Budapest Convention," Citizen Lab Submission to the Consultation on the Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence (CETS No. 224), March 2024. Verónica Arroyo was a research assistant at the Citizen Lab at the time the analysis was prepared. As a result, the findings and analysis do not necessarily reflect those of her current employer.
[4] Canada would also assume new obligations towards other countries that have been linked to abuse of transnational cooperation mechanisms, such as Turkey and Serbia. In 2022, Serbia (a country that has already ratified the 2AP) extradited a Bahraini dissident to Bahrain following an INTERPOL Red Notice, even though the extradition directly contravened an injunction that had been issued by the European Court of Human Rights: Ruth Michaelson, "'Illegal' extradition of Bahraini dissident from Serbia calls Interpol's role into question", The Guardian (16 February 2022). Moreover, if Canada were to ratify the treaty, it would also have no say over which additional countries join the treaty.
[5] Information and Privacy Commissioner of Ontario, "Consultation on the Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence", April 12, 2024, at p 3 (pdf).

existing gaps in Canadian privacy laws like the Privacy Act. The Information and Privacy Commissioner of Ontario agreed, while emphasizing that "[a]bsent appropriate rule of law or proportionality standards, there is a risk that the Protocol may have the effect of infringing upon the human rights of persons whose data is obtained from Ontario-based public or private sector organizations at the hands of foreign jurisdictions that do not share our free and democratic values."[6] While those concerns were raised in respect of Ontario, the same danger would be present across Canada.

In conducting a constitutional and human rights analysis of the 2AP–submitted to the Department of Justice during its consultation on the 2AP–the authors recommend that Canada should decline to ratify the treaty. Canada should instead play a leadership role in prioritizing international efforts to address cross-border gaps in human rights compliance, and to invest in fully resourcing cross-border data-sharing protocols that require and harmonize robust human rights protections from all signatories. In summary, the analysis found:

1. The 2AP permits state signatories to seize, share, retain, and use potentially large volumes of private data from public or private entities in respect of both digital and non-digital information.
2. As a whole, the 2AP's proposed method of expediting higher volumes of cross-border sharing of evidence is by eliminating or diminishing human rights safeguards, including the obligation to obtain prior, independent judicial authorization when seizing private information and sharing it with foreign law enforcement authorities. Rather than "establishing high standards, the protocol prioritizes law enforcement access at almost every turn."
3. The 2AP would specifically authorize, if not require, searches and seizures of private data, in circumstances that fall short of international human rights obligations requiring independent authorization and review for just cause. The protocol's toleration for inadequate human rights safeguards is a direct threat to existing protections under international human rights law. While the 2AP contains some opportunity for Canada to reserve against some of the most intrusive aspects of the treaty, opportunities for reservations are too limited, and fail to offset the broader problem that the instrument itself, as a whole, represents a threat to human rights everywhere.
4. The 2AP allows signatories to make secret agreements across borders between police agencies on their own, or between governments, that would potentially result in the whole cloth elimination of privacy and human rights safeguards.
5. The optional data protection standards set out in Article 14 of the 2AP either fall short of, or are inconsistent with, modern data protection principles and treaties. These gaps expose Canada to particular dangers given, as noted above by the Privacy Commissioner of Canada and others, Canada's privacy laws have not been modernized for the digital age, and lack much needed safeguards.

[6] Information and Privacy Commissioner of Ontario, "Consultation on the Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence", April 12, 2024, at p 3-4 (pdf).

6. By normalizing and tolerating an inadequate data sharing regime, the 2AP may be further weaponized against human rights by authoritarian governments around the world, who would point to the 2AP when justifying their own invasive surveillance and data sharing programs.

The complete analysis and submission can be read here.

3. Additional Implications of Bill C-2 for Data-sharing Between Canada and the United States Under a Potential CLOUD Agreement

On February 24, 2025, the Citizen Lab published an analysis, authored by Cynthia Khoo and Kate Robertson, of the Canada-U.S. negotiations under the CLOUD Act, and summarized key constitutional and human rights considerations relevant to public and democratic debates in Canada. The full text is available here.

The analysis of a potential Canada-U.S. CLOUD agreement identified a "minefield of incompatibilities and contradictions between Canada's constitutional and human rights frameworks, and those of the [United States]." The Canadian Supreme Court has established in numerous contexts that the law under Canada's Charter is different from U.S. law when it comes to human rights—stating as recently as last year that "[o]ur approach is distinct from the United States" when it comes to privacy rights. With the expansion of digital technologies in everyday life, the U.S. approach has shown itself to become increasingly unworkable in the digital age. The linked analysis outlines this historical legal divergence:

> Since the 1970s, U.S. courts have said that individuals are disentitled from constitutional privacy protections for information that they voluntarily share with a third party—this is known as the "third-party doctrine". Information caught up in this longstanding doctrine is exposed to warrantless seizures by U.S. law enforcement.
>
> The U.S. approach has not aged well. Fifty years later, smartphones are now ubiquitous, each loaded to the hilt with third-party apps hoovering up reams of private data about the most intimate and sensitive aspects of our daily lives. Amidst a sprawling data broker market that includes selling targeted ad data to law enforcement and government agencies, U.S. lawmakers and civil society have been trying to close part of this third-party-doctrine-enabled loophole, such as through the aptly titled The Fourth Amendment Is Not For Sale Act. While a 2018 U.S. Supreme Court decision marked an important shift towards a new approach, it is still far from clear if (or how far) the U.S. courts will go down this path.
>
> In contrast, that potential seedling of a new path in the U.S. is already Canada's well-trodden, constitutionally settled road. Since the early 1990s, Canada's top courts have repeatedly rejected the United States' approach to limiting privacy rights through the third-party

> doctrine. In a landmark judgment, Canada's Supreme Court decided that it would not follow the U.S. jurisprudence that has ultimately pushed swaths of government surveillance outside the oversight of U.S. judges. The Court foresaw that if electronic surveillance were to be left unregulated, it would have the potential "to annihilate any expectation that our communications will remain private". Thus, in many cases, the same types of personal data that are considered fair game in the U.S., are constitutionally protected from warrantless search and seizure in Canada.

In addition to the risk of subordinating existing Canadian protections to U.S. law if a CLOUD agreement were to be implemented, the analysis outlines further gaps in human rights protections in the United States that point to why "it is more critical than ever that Canada protectively and unwaveringly holds its own constitutional lines."

However, Bill C-2 would significantly expand law enforcement surveillance powers, by eliminating or watering down existing protections in Canadian law. Preliminary analysis of the law raises significant constitutional issues, including the potential that it appears poised to open the floodgates to a wide array of data-mining practices, including the collection of data from commercial data brokers, and other data-fueled algorithmic surveillance systems. As other recent analysis of Bill C-2 has also pointed out, other new proposed powers in respect of subscriber data are zombie-like proposals from previous failed attempts by past governments, each time using differing rationales. For example, new provisions in Part 14 of Bill C-2 would substantially dilute the legal threshold police must meet for accessing sensitive categories of data, including subscriber data, despite Supreme Court of Canada jurisprudence stating that these types of data requests engage "significant privacy interests."

The new powers in Bill C-2 are also notable given they overlap with some of the exact areas that Canada's constitutional protection provides greater protection against unreasonable surveillance than that of the US constitution, in ways that were anticipated to be the root of incompatibilities between the two countries in reaching a potential CLOUD agreement. As noted in Citizen Lab's prior analysis, such differences are not arbitrary, but are the result of fundamental constitutional and human rights differences in Canada, as well as decades of Supreme Court of Canada jurisprudence explicitly recognizing that Canada has taken a distinct approach from the United States on these very issues.

For example, Bill C-2 would create a new power allowing law enforcement to obtain warrantless access to any information that is provided to them "voluntarily" by any person (presumptively including a wide range of technology companies and electronic service providers). However, Canadian courts declined to follow U.S. constitutional doctrine when repeatedly making clear that such third-parties do not have the constitutional authority to consent to data disclosures on behalf of another individual.

Another of the proposed powers in Bill C-2 would give law enforcement authorities a warrantless authorization to demand that any person "who provides services to the public" must disclose if they have provided services to an individual. Among other risks, the provision would open the door to

information sharing with law enforcement authorities in states like Mississippi, Idaho, or Tennessee,[7] by compelling warrantless access to information about whether a person has obtained services from an abortion clinic in Canada.

The stakes of a potential CLOUD agreement should not be underestimated. In the process of preparing its analysis of the CLOUD Act, Citizen Lab researchers learned through informal consultations that Canadian officials have also at least at one point considered expanding the potential CLOUD agreement with the United States to include U.S. national security agencies. This would foreseeably expose public and private entities in Canada to data demands directly from U.S. intelligence agencies, without the involvement of the Canadian courts. It is difficult to overstate the reverberations that such an agreement would have on the Canadian landscape. The powers in Bill C-2 applicable to the Canadian Security and Intelligence Service (CSIS), bear additional scrutiny in this regard, given the potential that these powers–alongside existing powers in Canadian law–would simultaneously pave the way for reciprocal powers by U.S. national security agencies. At this time, there is no public information available regarding what such an agreement would include.

4. Putting the Cart Before the Horse: Transparency in Parliament Regarding Treaty-making

Given significant democratic, public interest, and human rights implications of Canada's potential agreement to a data-sharing framework with foreign authorities in the United States and/or elsewhere, it is surprising that the federal government is now quietly introducing the powers necessary to ratify the 2AP, without making this intent explicit to the broader public when it introduced Bill C-2. As noted above in Part 3 in relation to the CLOUD Act agreement, transparency is also critical surrounding the purpose of introducing several other new surveillance powers that would erode protections that are well-established in Canadian constitutional law, while concurrently granting U.S. law enforcement significant new reciprocal powers if a CLOUD agreement were to be reached.

At the briefing on June 6, 2025, government officials defended their current approach by stating that the formal ratification of the 2AP would ultimately require–at a later date–compliance with Parliamentary process. However, by proceeding in this manner, the government has bypassed critical democratic accountability controls. There is a significant democratic and public interest imperative in having explicit and fulsome transparency surrounding the intended data-sharing implications of Bill C-2 generally, and towards the United States in particular, before Parliament embarks on its study and debate of the proposed legislation. Providing the public with transparency surrounding the purpose and potential use of the proposed new powers is in keeping with democratic values, serves to protect public trust, and also ensures that Parliamentarians are able to meaningfully and carefully consider the implications of proposed powers–having regard to how they would actually be used.

[7] Naomi Cahn & Sonia Suter, "Crossing state lines to get an abortion is a new legal minefield, with courts to decide if there's a right to travel," Conversation, 6 September 2024.

It bears noting that the Government of Canada's Policy on Tabling of Treaties in Parliament itself directs that the federal government should not be quietly introducing treaty-implementing legislation through the backdoor of Parliament without making its intention explicit. The policy states that where reform of Canadian law is required in order to align with the obligations of a potential new treaty, the federal government must observe a waiting period before introducing implementing legislation to enable democratic debate:

For treaties that require implementing legislation before the Government can proceed to ratification, acceptance, approval or accession ("ratification"), the Government will:

- Observe a waiting period of at least twenty-one sitting days before the introduction of the necessary implementing legislation in Parliament;
- Will allow Members of Parliament the same opportunities to debate, present and vote on motions, as for those treaties which do not require implementing legislation;
- Will subsequently introduce the implementing legislation for these treaties; and
- Seek, only when the legislation is adopted, the authorization from the Governor in Council to express consent to be bound by the treaty.

By reversing these steps, the Canadian government would be creating a situation where powers relevant to highly controversial data-sharing obligations (under either a potential CLOUD agreement with the United States, or the 2AP) would be implemented under Canada's nose, without most people in Canada being any the wiser. If the government does not make explicit its intended use of the proposed powers, there may also be no further opportunity outside the context of the study of Bill C-2 for a parliamentary committee to receive expert testimony and study the implications of any intended data-sharing obligations towards the United States or other countries.

5. Conclusion

This introductory analysis of Citizen Lab's research concerning cross-border data sharing frameworks relevant to Bill C-2 is not intended to serve as a comprehensive analysis of the new powers in the proposed legislation. Instead, the preliminary analysis points to the need for fulsome transparency from the federal government regarding the intent and potential implications of Bill C-2 for data-sharing with law enforcement authorities from the United States and elsewhere, and for compliance with Canada's Policy on Tabling of Treaties in Parliament.

Both the 2AP and CLOUD Act data-sharing frameworks have each been shown to carry significant constitutional and human rights risks. As noted above, Bill C-2 itself contains several areas where

proposed powers appear designed to roll out a welcome mat for expanded data-sharing treaties or agreements with the United States and other foreign law enforcement authorities. But, this is not a matter that should be left to mystery, with the public having to gather clues as to the potential implications of complex surveillance powers that are as far-reaching geographically as they appear to be constitutionally. The federal government's acknowledgement in its briefing on June 6 that it intends to use certain powers in Bill C-2 to seek the ratification of 2AP only engages broader questions, and raises the need for explicit and fulsome explanations to the public regarding its intent in relation to the 2AP, what the implications of the 2AP would be for Canada, and whether it intends to enter other data-sharing obligations with foreign authorities including the United States. Only then should any enabling legislation be put forward and then carefully considered in full.