September 4, 2025

Bill C-2 and the Return of Warrantless Access: Same Fight, New Wrapper

By: Dav More & Tulika Bali

Matter Commented On: 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)

Bill C-2, the federal government's so-called "*Strong Borders Act,"* introduced in June 2025, proposes sweeping changes across border enforcement, immigration, and criminal law. Also tucked deep in the Bill are expansive new powers for law enforcement to access subscriber data, often without a warrant. These lawful access provisions, which have been controversial in the past, are now being quietly reintroduced through omnibus national security legislation. The constitutional concerns are immediate and serious, especially under section 8 of the *Charter*. Critics argue that the Bill undermines more than a decade of privacy jurisprudence and reopens doors that *R v Spencer*, 2014 SCC 43 (CanLII) had firmly closed (see here).

In what follows, we begin by examining Bill C-2's lawful access powers and warrantless subscriber data demands, focusing on the lowered suspicion standard and its clash with *Spencer* and *Bykovets*. We then analyze the Bill's creation of a technical assistance and enforcement infrastructure, which risks compelled backdoors reminiscent of the failed Bill C-30. Next, we turn to the Bill's provisions on cross-border data sharing and CLOUD Act compliance, situating Canada's approach within emerging transnational surveillance frameworks. Finally, we consider the Bill's constitutional tensions under sections 7 and 8 of the *Charter*, before concluding with a critical assessment of its implications for privacy rights at home and abroad.

Lawful Access Powers and Warrantless Data Demands

Parts 14 and 15 of Bill C-2 create a regime allowing police and CSIS officers to demand customer information from any company providing public services, banks, telecoms, and social media, on a mere suspicion standard. Under proposed section 487.0121 of the *Criminal Code*, RSC 1985, c C-46, officers may ask whether someone is a customer, what services they use, and where they used them, without judicial pre-authorization. For the first time in Canadian law, warrantless access to subscriber data, including IP addresses, would be explicitly authorized by statute.

Bill C-2's demand powers turn on reasonable suspicion, rather than the traditional 'reasonable grounds to believe' threshold that justifies warrants and production orders. In Canadian law, reasonable suspicion is a distinct, lower standard, "something more than a mere suspicion and

something less than a belief based upon reasonable and probable grounds" (*R v Kang-Brown*, 2008 SCC 18 (CanLII) at para 75). By contrast, access to private information ordinarily proceeds on the higher reasonable belief standard (see *Hunter v Southam Inc*, 1984 CanLII 33 (SCC), [1984] 2 SCR 145 at 159–60). Courts have tended to reserve the suspicion standard for preliminary investigative techniques (e.g., sniffer-dog deployments in *R v Chehil*, 2013 SCC 49 (CanLII)), not for authorizing state access to highly revealing digital identifiers. Using suspicion to compel subscriber data therefore extends the standard beyond its usual domain, signaling an unusual and controversial lowering of the threshold for state access to constitutionally sensitive information.

The Supreme Court in *R v Bykovets*, 2024 SCC 6 (CanLII) affirmed that even IP addresses attract a reasonable expectation of privacy and cannot be obtained without a warrant (at paras 2, 28). The court confirmed that subscriber data is "the key to unlocking" a person's identity and online activity (*Bykovets*, at para 28). Bill C-2 ignores this trajectory entirely.

Adding to the concern, the Bill introduces a new production order under proposed section 487.0142 of the *Criminal Code,* which would allow judges to compel companies to disclose "all subscriber information" based merely on a suspicion standard. The scope of "subscriber information" is defined broadly, encompassing usernames, device identifiers, IP addresses, account login timestamps, payment records, service usage history, and potentially other data points that reveal patterns of behaviour (Bill C-2, Part 14). This sweeping definition effectively collapses the traditional distinction between metadata, often viewed as less sensitive, and content, which is more rigorously protected under section 8 of the *Charter*.

The Supreme Court has historically treated metadata and content differently for privacy purposes, with metadata sometimes considered less intrusive. However, in the digital age, that distinction has become increasingly artificial. As *Bykovets* recognized, metadata can reconstruct a user's digital life, exposing sensitive information such as political affiliation, religious beliefs, personal habits, locations visited, and social networks (*Bykovets*, at paras 2, 28). By granting the state broad access to such data on a low evidentiary threshold, Bill C-2 risks lowering the constitutional safeguards that currently stand between Canadians and pervasive state surveillance.

The Charter Statement from the Department of Justice insists these demands are minimally intrusive, but legal scholars have sharply disagreed. The Canadian Privacy Law Blog called the Statement's reasoning "either sloppy or intended to be deceptive", noting that police could use these powers to ask a bank for a list of all companies a person deals with, or a health clinic to identify which specialists a patient sees, all without a warrant.

Technical Assistance and Enforcement Infrastructure

Part 15 of the Bill enacts the Supporting Authorized Access to Information Act. This would impose technical assistance obligations on electronic service providers (ESPs), requiring them to build and maintain systems to comply with access orders. The Minister of Public Safety could compel specific companies to enable access mechanisms or data extraction functions. Cabinet would designate "core providers," subject to compliance audits and penalties of up to $250,000 per day for non-compliance. While the Bill includes a clause against "systemic vulnerabilities," (cl 5(3), Part 15) it is unclear how robust that protection will be in practice. Similar language has been

interpreted narrowly elsewhere, and the risk of compelled backdoors or weakened encryption remains real.

These provisions are reminiscent of Bill C-30, *Protecting Children from Internet Predators Act* (1st Sess, 41st Parl), a controversial 'lawful access' Bill that was stalled and never enacted. The Bill was introduced in 2012 and sought to give police expanded access to online subscriber information without judicial oversight. It was met with widespread backlash from civil liberties groups, privacy commissioners, legal academics, and the public at large, who warned that such unchecked powers posed serious risks to Canadians' privacy rights. The controversy reached a boiling point when then Public Safety Minister Vic Toews infamously stated in the House of Commons that critics of the Bill could "either stand with us or with the child pornographers" (House of Commons Debates, 13 Feb 2012 at 1110). The Bill was ultimately withdrawn in 2013. Bill C-2 appears to have learned from the political fallout of Bill C-30, not by narrowing the scope of access powers, but by burying them in omnibus legislation framed around border security. The framing has changed, but the surveillance logic remains largely intact. What was once rejected by the public under the spotlight of scrutiny is now being reintroduced through quieter, more technical channels.

Cross-Border Data Sharing and CLOUD Act Compliance

Bill C-2 also paves the way for cross-border data exchange. It modifies the *Mutual Legal Assistance in the Criminal Matters Act,* RSC 1985, c 30 (4th Supp), to allow Canadian judges to compel foreign service providers to disclose data. It also allows Canadian authorities to apply for judicial authorizations to ask foreign companies directly for information, a legal mechanism that mirrors the requirements of the US CLOUD Act and the Second Additional Protocol to the Budapest Convention (2AP).

As Citizen Lab notes, Bill C-2 appears deliberately designed to enable Canada to comply with these frameworks considering the federal government's intentions to this Bill in its ratification of 2AP (Section 4: Putting the Cart Before the Horse). However, both raise serious concerns about human rights, oversight, and data protection. Once Canadian data leaves the country, *Charter* protections no longer apply which may leave Canadians and much of the world "vulnerable to arbitrary and abusive data collection practices by domestic law enforcement agencies" as a result of 2AP ratification which Bill C-2's passing would contribute to (Citizen Lab at Section 2: The Potential Impact of the 2AP). Without robust safeguards, Canadians' data could be accessed by foreign states with weaker privacy laws.

Constitutional Tensions: *Charter* Sections 7 and 8

Section 8 of the *Charter* requires that searches be authorized by law, that the law itself is reasonable, and that the search is carried out in a reasonable manner (*Hunter v Southam Inc* at 159). It also requires prior judicial authorization for searches that intrude upon a reasonable expectation of privacy, except in exigent circumstances (*Hunter v Southam Inc* at 160).

By authorizing access to personal data on a mere suspicion standard, and sometimes without any judicial authorization at all, Bill C-2 likely fails to meet the privacy threshold established by the

Supreme Court. In *Spencer*, the Court recognized that even "basic" identifiers, such as subscriber information, may lead to the identification of individuals engaged in highly private or intimate activities, often presumed to be anonymous, rendering such disclosures a search under section 8 of the *Charter* (*Spencer*, at para 66). More recently, in *Bykovets*, the Court reiterated that even anonymized data like IP addresses attract a reasonable expectation of privacy because of their potential to be de-anonymized and linked to biographical core information (*Bykovets*, at paras 4–8, 47–48). These rulings collectively underscore that access to digital identifiers without judicial oversight raises serious constitutional concerns under section 8.

The Charter Statement tries to justify the approach taken in Bill C-2 by asserting that the information at issue is not particularly sensitive. The Bill authorizes designated officials to obtain only basic information about the nature of the services provided, which is limited in scope and does not include the contents or details of communications. Any further access to data would continue to require a search warrant or production order under existing legislation. However, this claim is directly contradicted by binding Supreme Court jurisprudence including *Bykovets* and *Spencer*. Courts have been clear that privacy analysis is contextual, and in the digital age, identifiers are no longer harmless which has caused concerns in this Bill passing.

Conclusion

Bill C-2 revives the lawful access agenda under the guise of border protection. It introduces broad new surveillance powers with minimal oversight, limited transparency, and serious constitutional concerns. The *Charter* jurisprudence is clear: access to personal data requires judicial authorization. Parliament cannot sidestep that principle through definitional games or omnibus legislation.

The implications, however, extend beyond Canada's borders. Bill C-2's cross-border data sharing mechanisms would plug Canada directly into the architecture of the CLOUD Act and the 2AP, which enable foreign governments, including those with weak privacy protections to request data from Canadian companies with limited oversight. This exposes Canadians, and global users of Canadian platforms, to potentially arbitrary or abusive surveillance regimes abroad.

Citizen Lab warns that Bill C-2's approach to foreign cooperation reflects a trend of outsourcing surveillance powers to transnational systems without domestic accountability. If passed, the Bill would not only lower privacy protections at home, it would help export that erosion abroad. The privacy implications of Bill C-2 extend beyond domestic constitutional concerns to raise international issues as well.

Many of Bill C-2's provisions seem ripe for constitutional litigation whether challenged under sections 7 or 8 of the *Charter*. Canadians should be alarmed by any legislation that expands surveillance while reducing safeguards, especially when it is buried in a border bill. This is not just a question of policy. It is a question of rights.

This post may be cited as: Dav More & Tulika Bali, "Bill C-2 and the Return of Warrantless Access: Same Fight, New Wrapper" (4 September 2025), online: ABlawg, http://ablawg.ca/wp-content/uploads/2025/09/ Blog_DM&TB_BillC-2.pdf

To subscribe to ABlawg by email or RSS feed, please go to http://ablawg.ca

Follow us on Twitter @ABlawg