Lawful Access

This document is meant to assist the reader in understanding various scenarios in which lawful access provisions contained within Bill C-2 will assist police in serious criminal investigations.

Prepared by:

Canadian Association of Chiefs of Police

September 9, 2025

BILL C-2 (*STRONG BORDERS ACT*) - PART 14 and 15: LAWFUL ACCESS

Bill C-2 contains several amendments to the *Criminal Code* which will clarify police authority and increase response times for criminal investigations.

1. Clarifying Voluntary Disclosure of Subscriber Information

Bill C-2 addresses ambiguity stemming from the Supreme Court's *R. v. Bykovets 2024* decision, by codifying what subscriber information police can receive without a court order, when it is voluntarily provided. This change restores clarity for internet child exploitation (ICE) investigators requesting basic subscriber information (BSI) from service providers or international partners. It removes uncertainties caused by *Bykovets*, ensuring no delay in identifying suspects tied to child exploitation imagery.

Hypothetical Example

A Canadian father notices his 12-year-old daughter is chatting online with someone claiming to be a teen. He is suspicious that it may be an adult. The father checks the chat logs and sees explicit messages and a shared image that appears to be child sexual abuse material. He contacts local police and provides screenshots, the username, and the suspect's IP address which is all visible within the peer-to-peer chat tool. Currently, due to *Bykovets*, officers may hesitate to act on the IP address voluntarily provided by the father, unsure if it violates privacy law. They may delay action while obtaining a production order, risking continued harm. With Bill C-2, police would be able to immediately act on voluntarily provided information and locate the suspect's service provider, shortening the response time. Additionally, police would no longer fear civil liability for using the data or violating privacy law in these types of circumstances.

2. Introduction of a New Information Demand Regime Based on Reasonable Suspicion

Bill C-2 creates a new tool allowing investigators to issue demands for, among other things, whether the person provides or has provided services to a subscriber, possesses or controls information, including transmission data, in relation to that subscriber, etc. This streamlines investigative timelines and assists in narrowing down the information sought by police agencies which may then be obtained via judicial authority.

Example (Alberta)

In a criminal harassment/stalking case, the victim discovered a tracking device attached to their vehicle. The device used a global SIM card which would roam on Canadian telecommunication networks to transmit data back to its owner. Investigators issued preservation demands to major Canadian Service Providers (CSP) asking them to retain any data associated with the tracker's IMSI number. However, preservation demands only require data to be stored for 21 days and do not compel companies to confirm whether they are in possession of the relevant data. In this instance, only two out of four CSPs confirmed they had no data, leaving investigators uncertain about the remaining companies' records, making it difficult to establish grounds for further orders. Preservation demands do not require CSPs to confirm whether data exists. Investigators struggle to meet the threshold of belief that a provider has data in their possession or control, slowing investigations and creating uncertainty. Bill C-2 introduces the Information Demand, which would require CSPs to confirm whether their network carried the tracker's data. This confirmation would allow investigators to pursue production orders to obtain routing and location information tied to the device, therefore saving investigation time for the safety of the victim.

Example (Atlantic provinces)

On a missing person's file that turned into a homicide/obstructing justice file, investigators had a suspect who repeatedly changed their phone number and telecommunications service provider. Investigators had to resort to deploying multiple Transmission Data Recorder Warrants on the phones of their associates to identify their new phone number. In the context of this investigation, the new Information Demand in Bill C-2 would have greatly increased the speed at which the suspect's new phone numbers would have been identified and reduced the number of Transmission Data Recorder Warrants required, ultimately increasing the efficiency and expediency of the investigation.

Example (Quebec)

Investigators conducted a multi-year investigation into online fraudulent activities involving the trafficking of personal information and breach of trust. This investigation was complicated by the fact that everything was done online, and the real identity of the suspects was not known. Investigators sent multiple requests to a specific CSP to confirm that the information they intended to seek with a production order was available and under their control. However, for most of their requests, the service provider declined to complete the requested checks to confirm the existence of the data and/or record. Preservation demands do not require CSPs to confirm whether data exists. Currently, investigators must get a production order to obtain information they are not even certain exists (obtaining judicial authorizations to find 30 days later that no records existed at that CSP). This creates unnecessary delays, juridical authorizations and setbacks in an investigation, causing increased investigative delays at the expense of victims and citizens. Bill C-2 introduces the Information Demand tool to enable investigators to demand information from the CSPs who have the information in their possession or control.

3. Changing the Threshold for Subscribers' Information

The current judicial authorization requirements to obtain subscribers' information is reasonable grounds to believe (RGTB) that an offence has occurred and RGTB that the document or data will afford evidence of the offence. Bill C-2 creates a new production order specifically for subscriber information, based on reasonable grounds to suspect.

Hypothetical Example

A missing person investigation where the potential victim was involved in previous auto thefts. The auto theft ring would be a potential motive for the victim disappearing and it is suspected the missing person was killed or hurt. Phone records from the victim's cellular device show several unknown phone numbers who have contacted the missing person in the days leading up to their last known sighting. Learning the subscriber information for the persons associated with the numbers would assist police in being able to interview those persons regarding the suspected murder or the suspected auto theft ring, which may have led to motive for the foul play. Currently, at most times in early investigations such as this, there are only reasonable grounds to suspect that an offence has occurred. An application could be denied solely because of these circumstances. Information that assists the investigation (such as contact names for numbers of a victim or suspect) is a useful avenue of investigation for police. This information provides a starting point of basic information in order to interview people, eliminate obvious non-persons of interest and/or establish a pattern of use for a phone user. It is not necessarily the case that an affiant can articulate evidence would be obtained vs. reasonable grounds to suspect that it would assist in the investigation of the offence.

Hypothetical Example

A Canadian teacher reports that her 13-year-old student confided receiving repeated Instagram messages from someone asking for sexual pictures. The teacher provides police with a screenshot showing the username and a general sense of when the messages started. Currently, police need reasonable grounds to believe a crime occurred to obtain a general production order — a high threshold early in the investigation. With limited evidence, they might hit a legal wall and be unable to act quickly. With Bill C-2's new production order for subscriber information, which is based on reasonable suspicion, officers can issue a demand to Instagram's Canadian legal counsel for basic subscriber information tied to the username, earlier in the investigation. They receive the IP address, associated email, and name and can advance the investigation more urgently.

4. Response Time for Production Orders

Under the current *Criminal Code*, a person, financial institution or entity may apply in writing to revoke or vary a production order within 30 days. Bill C-2 changes the 30-day limit to 5 days. This dramatically enables faster access to critical evidence. Some jurisdictions across Canada have paid to request expedited production orders to speed up the process. As an example, as of August 6, 2025, York Regional Police Service has provided payment of $500 to various telecommunications companies on 35 occasions to expedite the procurement of phone records. This process has resulted in a total cost of $17,500. These requests were supported by judicially approved warrants and associated to threshold offences. Having prompt access to these telecommunications records is a necessity for police investigations.

Example (Ontario)

In a homicide, offenders lured the victim outside through calls from an individual posing as a 'friend'. After briefly meeting them, the victim was shot and fatally wounded. The investigation relied heavily on production orders and video evidence. Investigators obtained the victim's phone records, which identified the suspect number. Further production orders revealed related callers, guiding a timely video canvass. Surveillance footage linked suspects to a vehicle, hotel meetings, and eventually to the crime. CSPs returned some production order results in under 48 hours, which was critical to securing time-sensitive video evidence before it was overwritten. The case ended in convictions for first-degree murder. However, in other similar cases, CSPs have taken the full 30 days allowed, which would have caused crucial evidence to be lost.

Example (Ontario)

In November 2024, an armed home invasion occurred, and the lone female victim was confronted by two suspects, one of whom was armed with a firearm. The suspects demanded the victim turn off the alarm that had been triggered, which she complied with. The victim's husband attempted to contact her after receiving an alert on his phone of the alarm being triggered. When he was unable to reach her, he contacted a neighbour to go check on the residence. As the neighbour entered the front door area of the residence, he was shot by one of the suspects. The shooting victim was in the company of his 6-year-old child at the time of the shooting. This residence was also targeted for a Break & Enter in October 2024, and during this incident, the suspect vehicle rammed responding police cruisers. Two suspects fled on foot, one of which was apprehended. Two loaded firearms were recovered during this incident. Several interests were identified from each incident, but investigators were required to wait 30 days for results, significantly delaying the investigation.

Example (Ontario)

Between August - September 2024, a female victim met an unknown male party on an online dating site. The romance developed into an investment opportunity where the suspect's customer service representatives attended the victim's residence on three separate occasions to collect a total of $170,000 in cash. The overall fraud was over 2 million dollars. Although the incident is not violent in nature, immediate access to results to identify suspects would have been beneficial to prevent further victimization to this victim and/or identify other victims.

Example (Ontario)

In June 2025, masked suspects armed with hammers attended a jewellery store at a large mall and attempted to gain entry. When entry wasn't gained, they fled to a waiting vehicle. A similar incident occurred in July 2025 in which all jewellery cases were smashed. Investigators have sought production orders in both incidents and are waiting for production order results.

Example (jurisdiction not specified)

In a homicide case, a victim was shot by an acquaintance at the roadside. Investigators urgently needed cell phone records to confirm contacts and locate the suspect who was believed to be carrying both the victim's phone and a handgun. The suspect was later reported brandishing the weapon, which had not been recovered. Investigators had judicial authorization for a phone tracker, but no data could be obtained, preventing location tracking. An expedited response for call records and tower data was necessary to identify potential witnesses, confirm communications, and recover the gun, which posed an ongoing safety risk to the community. Delays threatened both public safety and the preservation of critical evidence. Production order delays limited the investigators' ability to quickly identify suspects, witnesses, and the location of a firearm believed to still be in circulation.

5. Enhanced Access to Cross-Border Digital Evidence

Bill C-2 creates a foreign production order mechanism for subscriber information and transmission data held by foreign entities, helping investigators acquire critical evidence from U.S.-based platforms (e.g., Facebook, Dropbox, Snapchat). Most online child sexual abuse material cases involve offshore tech companies. Previously, Canadian investigators faced delays navigating Mutual Legal Assistance Treaties (MLATs) or relying on voluntary cooperation. With this provision aligned to the 2nd Additional Protocol to the Budapest Convention, Internet Child Exploitation (ICE) units can now facilitate data disclosure with less friction, accelerating evidence collection and protecting child victims.

Hypothetical Example

The National Child Exploitation Crime Centre (Canada) receives a National Centre for Missing & Exploited Children CyberTip (U.S. reporting centre) about a Canadian IP address uploading child sexual abuse material to Dropbox. Local police identify the IP and seize the suspect's devices, but the most critical evidence, including the actual child sexual abuse material images, are stored in the suspect's Dropbox account, hosted in the U.S. Currently, police must request assistance via the MLAT, which can take months. By the time access is granted, evidence may be deleted or overwritten, and therefore the prosecutions may be weakened. Under Bill C-2, officers can issue a foreign production order directly to Dropbox's legal team, expediting access to evidence and reducing delays and dependency on MLATs.

Example (Quebec)

In controlled delivery cases, where contraband shipments are detected, law enforcement rely on production orders to identify consignees and suspects. However, delays in judicial review and corporate responses often allow suspects to abandon shipments before police can act. CSPs also charge high fees for expedited data (EPO), requiring senior management's approval to release funds, which delays proceedings further. Courthouses are frequently bottlenecked by requests, with judges unable to process them quickly. In Montreal, investigators face weekly delays just to meet with judges. Additionally, some judges refuse production orders involving foreign service providers, and U.S. companies frequently reject Canadian requests.

These delays cause investigational stalemates, especially when victims are involved. Bill C-2 shortens production order timelines from 30 to 5 days, clarifies Canadian authority to seek data from foreign entities, and streamlines judicial processes to reduce bottlenecks and costs in urgent contraband cases.

6. Tracking Similar Things

Bill C-2 enables a judge or justice to authorise investigators to obtain tracking data that relates to the location of a thing or similar thing.

Example (jurisdiction not specified)

In organized crime investigations, suspects routinely swap vehicles to evade surveillance. In one case, investigators received judicial authorization to track the target's vehicle, only to find on the installation day that the suspect had switched cars. The affiant had to rewrite the Information to Obtain (ITO) for the second vehicle, draft and submit a new warrant for the second vehicle, losing valuable time. Similarly, suspects often use rental vehicles, switching frequently, to frustrate law enforcement. Every time a suspect changes vehicles or devices, it forces police to reapply for new tracking authorizations, creating investigative gaps. Current Tracking Warrants apply only to specific vehicles or devices, forcing repeated applications when suspects switch. Bill C-2 allows pre-authorization to track 'similar' things (such as vehicles) in an investigation.

7. Codifying the Release of Subscriber Information Related to Transmission Data

Currently, section 492.2(1) of the *Criminal Code* allows a justice or judge to authorise investigators to obtain transmission data via a Transmission Data Recorder Warrant (TDRW). The subscribers' information (name and address) is then usually obtained by means of an Assistance Order, outlined in section 487.02 of the *Criminal Code*, which accompanies the TDRW. In the province of Quebec, it is sometimes impossible to obtain subscriber information via an Assistance Order, as some judges refuse to authorize them. Bill C-2 clarifies and standardizes the way subscriber information related to transmission data should be obtained in Canada.

***Example (Quebec)* – Homicide investigation**

The judge refused the Assistance Order to obtain the subscriber's information (name and address) stating that "the assistance necessary for the execution of the requested transmission data recorder warrant… is determined according to the purpose of the primary warrant, and not to obtain additional information which is not transmission data but which may provide assistance in interpreting the data collected. If the legislator had wanted to authorize this, it could have said so in clear terms (…)".

***Example (Quebec)* – Sexual Assault**

The judge refused the entire TDRW saying "Names and contact information do not constitute transmission data".

***Example (Quebec)* – (Offence not specified)**

The judge refused the assistance order to obtain the subscriber's information and stated "Subscriber information is not covered by section 487.02 of the Criminal Code. 487.02 of the Criminal Code is not intended to expand the acts authorized by 492.2 of the Criminal Code which is authorized on the basis of suspicion. There is a reasonable invasion of privacy as to the subscriber's name (referring to the *Spencer* decision). I am not bound by 2019 NLCA 6."

CONTRIBUTIONS BY:

Canadian Association of Chiefs of Police - Electronic Crime Committee

Canadian Association of Chiefs of Police – Law Amendments Committee

Ontario Provincial Police

Peel Regional Police Service

Royal Canadian Mounted Police

Sûreté du Québec

Toronto Police Service

Vancouver Police Department

York Regional Police Service

Ministry of the Attorney General, Ontario