NATIONAL POLICE FEDERATION | FÉDÉRATION DE LA POLICE NATIONALE ™

TO: Senate Standing Committee on National Security, Defence and Veterans Affairs
FROM: Rob Farrer, President
DATE: November 09, 2026
RE: **STUDY OF BILL C-22, AN ACT RESPECTING LAWFUL ACCESS**

The National Police Federation (NPF), representing nearly 20,000 Members of the Royal Canadian Mounted Police (RCMP), welcomes the opportunity to provide its views on Bill C-22, *An Act respecting Lawful Access*.

The NPF strongly supports Bill C-22 as passed by the House of Commons and urges the Senate to advance it without delay. In considering any further amendments, the Senate should assess their practical effect on investigations and reject changes that would weaken, delay, narrow, or frustrate the lawful investigation of serious offences or the effective use of evidence in subsequent prosecutions.

The NPF has consistently advocated for the modernization of Canada's lawful access framework. Our Members investigate some of the most serious and complex crimes facing Canadians, including online child sexual exploitation, organized crime, sextortion, human trafficking, terrorism, and intimate partner violence. Increasingly, the evidence needed to advance these investigations is held by telecommunications companies, online platforms and other electronic service providers.

Bill C-22 begins to address the growing gap between the lawful authorities available to investigators and their practical ability to use those authorities in a digital environment. It modernizes investigative processes and establishes a framework so that relevant service provider can respond meaningfully when legally required to do so.

To be clear, the Bill does not give police or other agencies unrestricted access to Canadians' private online information. It modernizes how existing court-authorized powers work in a digital world, so that when a judge grants an order, the system is capable of producing what the court has ordered.

1. Recommendation: Assess the Practical Impact of Further Senate Amendments

The NPF urges the Senate to support timely passage of Bill C-22 in the form adopted by the House of Commons. The House has already made substantial changes to address concerns about privacy, encryption, cybersecurity and accountability. Further restrictions risk undermining the operational purpose of the legislation.

The NPF respects the Senate's responsibility to scrutinize legislation. That scrutiny should assess both the concern an amendment seeks to address and its practical consequences for investigators, victims, and subsequent prosecutions. Any further amendment should respond to a demonstrated deficiency in the House-passed text, rather than duplicate existing safeguards or impose restrictions without evidence of their necessity.

In assessing proposed amendments, the Committee should consider whether it would:

- Delay the identification or preservation of relevant evidence;
- Prevent or impede compliance with a lawful judicial order;
- Narrow the investigation available to investigators beyond what is necessary to protect privacy;
- Reduce the reliability, integrity, or admissibility of evidence;
- Impair cooperation with domestic or international partners; and/or,
- Otherwise make it more difficult to investigate and prosecute serious offences effectively.

This assessment should also guide considerations of provider submissions. Claims that the amended framework is technically unworkable, commercially prohibitive or incompatible with secure services should be supported by provision specific evidence. Providers should explain why the Bill's existing encryption protections, cybersecurity safeguards and feasibility considerations do not adequately address their concerns. International comparisons should identify actual differences in obligations, not simply assert that Canada's proposal is unprecedented.

The NPF encourages the Senate to emphasize timely implementation, consultation with frontline investigators and technical experts, adequate resources, and monitoring of investigative outcomes. Committee observations can advance these priorities without reopening the legislative balance achieved by the House.

The central objective must remain clear: preserve meaningful privacy protections, while ensuring that lawful investigative authorities work in practice.

2. Privacy, Cybersecurity and the House of Commons Amendments

The NPF recognizes that effective lawful access must operate alongside meaningful protections for privacy, cybersecurity, and the rights guaranteed by the Canadian Charter of Rights and Freedoms. These protections matter to our Members, both as investigators responsible for exercising lawful authorities and as Canadians who rely on secure communications services.

The House of Commons amended Bill C-22 to strengthen safeguards governing encryption, cybersecurity, judicial oversight, transparency and metadata retention. The NPF supports the House passed framework as a workable balance between investigative effectiveness and the protection of Canadians' rights, including:

- **Encryption:** Providers cannot be compelled to decrypt user-encrypted information unless they supplied the encryption and possesses the information necessary to decrypt it.
- **Cybersecurity:** Obligations cannot require providers to introduce systemic vulnerabilities or prevent them from correcting such vulnerabilities.
  Investigative Access: Subscriber-information production orders must specify the information authorized by the court. Specified ministerial orders require Intelligence Commissioner approval, alongside enhanced NSIRA notification, reporting and review.
- **Metadata Retention:** The maximum regulated retention period was reduced from 12 months to six months, with an additional requirement to establish that the specified metadata is essential to effective and timely investigations.

The NPF supported the original 12-month maximum, recognizing that victims may delay reporting offences and complex investigations can take considerable time to identify relevant digital evidence. Reducing that maximum to six months already represents a significant limitation on the proposed framework. Although the NPF supports passage of the House passed Bill, that support should not be interpreted as agreement that six months will meet every investigative need.

The House has already responded substantially to privacy and industry concerns. The Senate should preserve that balance and avoid further restrictions that would leave investigators with lawful authorizations but no practical means of obtaining the evidence they cover.

3. The Operational Problem the Bill Addresses

The scale of the challenge is stark. The rate of police-reported online child sexual exploitation has risen 347% since 2014, with 16,905 incidents reported in 2024 alone.[1] Police-reported extortion is three times higher than a decade ago.[2] In nearly every serious file our Members work today, digital evidence is not peripheral, it is at the heart of every investigation.

Yet Canada remains the only Five Eyes nation without a legal framework requiring electronic service providers to maintain the technical capability to comply with judicial authorizations. The result is a paradox familiar to RCMP investigators: a judge issues a production order or wiretap authorization, and the service provider simply cannot, or will not, comply because it has no system to do so. Investigations stall, evidence is lost, victims remain at risk, and offenders go unidentified.

Since the Supreme Court of Canada's decisions in *R. v. Spencer* (2014) and *R. v. Bykovets* (2024), even the most basic step of identifying who is behind an IP address linked to criminal activity requires a court order. Our Members support that constitutional framework. What they need is legislation that ensures the process works efficiently, that providers can deliver on court orders, and that investigators are not forced to watch evidence disappear while navigating procedural gaps that date from 1995.

Bill C-22 responds directly to these realities by creating clear, Charter-compliant tools tailored to low-level identifying data, clarifying when emergencies allow for immediate action, and ensuring that core providers have the capability to comply with judicial authorizations. These measures will not prevent crime on their own, but they will remove systemic barriers that currently prevent police from getting to the starting line in many digital investigations.

4. How the Bill Will Benefit Investigations

4.1 Confirmation of Service: Eliminating the Identification Bottleneck

One of the most persistent frustrations in digital investigations is the inability to determine which provider holds relevant subscriber information. Today, when an officer identifies an IP address or phone number tied to criminal activity, there is no efficient mechanism to confirm which company services that identifier. Investigators often send speculative requests to multiple providers, each of which may take weeks to respond, if they respond at all.

---

[1]Statistics Canada; Police-reported incidents of online child sexual exploitation in Canada, 2024
https://www150.statcan.gc.ca/n1/daily-quotidien/260310/dq260310a-eng.htm
[2]Statistics Canada; Police-reported crime statistics in Canada, 2025
https://www150.statcan.gc.ca/n1/daily-quotidien/260722/dq260722a-eng.pdf

Bill C-22 would allow a peace officer or public officer to issue a demand requiring a telecommunications service provider to confirm whether it provides or has provided service to a specified subscriber, client, account, or identifier. The officer must have reasonable grounds to suspect both that s federal offence has been or will be committed and that the confirmation will assist its investigation. The demand must specify a response deadline that allows at least 24 hours, subject to the statutory review process.

Practical example- sextortion of a youth (current state vs future state)

- **Current state:** An officer investigating a sextortion complaint receives a tip identifying a phone number used to threaten a teenage victim. Under the current regime, the officer must guess which carrier services that number and apply for a production order, a process that can take weeks. If the wrong provider is targeted, the process starts over. During this period, the suspect can keep contacting the victim, move to new accounts, or delete evidence.
- **Future state with C-22:** Under the Bill, the Member could issue a confirmation-of-service demand with a specified response deadline, allowing at least 24 hours. Once the appropriate provider is confirmed, investigators could direct the appropriate judicial application to that provider, reducing avoidable inquiries and repeated legal steps.

4.2 Streamlined Subscriber Information Production Orders

Bill C-22 creates a dedicated subscriber information production order under proposed section 487.0142 of the *Criminal Code*. A justice or judge must be satisfied, on information under oath, that there are reasonable grounds to suspect that a federal offence has been or will be committed and that the specified subscriber information is in the recipient's possession or control and will assist the investigation. The order provides a tailored route to defined identifying and service-related information while maintaining judicial scrutiny.

Practical example- organized auto theft ring

- **Current state:** Officers investigating an organized auto theft ring identify multiple accounts on a messaging platform being used to coordinate vehicle thefts and arrange export shipments. Currently, obtaining subscriber information for each account requires a general production order, the same instrument used to compel disclosure of far more sensitive records. Preparing and litigating these orders is time-consuming, which allows vehicles to be exported or re-VINed while police are still trying to figure out who is behind the accounts.
- **Future state with C-22:** The dedicated subscriber information order could help investigators to identify account holders and advance investigative steps sooner, thus disrupting the broader criminal network financing weapons and drugs.

These targeted tools distinguish defined subscriber information from communications content and other categories of evidence, while preserving judicial scrutiny of information sought and its connection to the investigation.

4.3 Exigent Circumstances: Acting When Every Minute Counts

Bill C-22 clarified and extends section 487.11 of the *Criminal Code*. Where the statutory conditions for the relevant warrant or order exist, but exigent circumstances make obtaining it impracticable, the provision would permit specified investigative steps without prior judicial authorization. This includes seizure of subscriber information, transmission data and tracking data covered by the provisions identified in the bill. These are exceptional authorities, not a substitute for obtaining judicial authorization where it is practicable to do so. Their exercise remains subject to applicable constitutional

requirements and judicial scrutiny. This reflects the reality that digital evidence can vanish in seconds, particularly with auto-deleting messages and live-streamed abuse.

Practical example- live-streamed child sexual abuse

- **Current state:** An officer receives a report of an active livestream depicting the sexual abuse of a child. Investigators need to identify the account, obtain relevant technical information and locate the child urgently. Existing law provides some exigent-circumstances authorities, but investigators must assess which authority applies to each investigative step and whether prior judicial authorization is required. These legal and practical complexities can complicate an already time-sensitive response.
- **Future state with C-22:** The Bill would provide a clearer statutory basis for obtaining specified subscriber information, transmission data or tracking data without prior judicial authorization where the conditions for the relevant order exist, but exigent circumstances make obtaining it impracticable. This would help investigators to take urgent steps to identify and local the child, while remaining subject to applicable legal thresholds and constitutional safeguards. It would not guarantee immediate provider disclosure, access to encrypted content or identification of the child's location.

Emergency authorities should remain exceptional and subject to the safeguards established by law. At the same time, the legislation must allow investigators to respond when delay could result in the loss of evidence, continued danger to a victim, or the disappearance of a suspect. Any proposed amendments should not introduce uncertainty or delay that would make these provisions ineffective when urgent action is required.

4.4 Cross-Border Data Requests: Reaching Evidence Where It Lives

Crime no longer respects jurisdictional boundaries, and neither does digital evidence. Our Members routinely investigate offences where critical data such as IP addresses, account information, communications metadata is held by foreign service providers. The mutual legal assistance process can take months or even years. In the meantime, evidence is purged, accounts are deleted, and offenders continue to victimize Canadians.

Bill C-22 introduces a new mechanism that would supplement, not replace, mutual legal assistance and other lawful cooperation channels. It would provide a standardized, Canadian court-authorized route for requesting specified subscriber information or transmission data held by foreign providers. It could reduce delay where a provider can lawfully respond directly, but would not override foreign law or guarantee compliance.

For example, where permitted by applicable foreign law and provider procedures, the court-authorized request could allow investigators to obtain specified subscriber or transmission data without first completing the full mutual legal assistance process.

Practical example- transnational fraud ring targeting seniors

- **Current state**: An officer investigating a transnational fraud ring determines that the suspects are using a US-based messaging platform to coordinate the scheme. Currently, the Member must navigate the cumbersome mutual legal assistance treaty process, which can take six months to a year. During this period, the fraudsters may move platforms, withdraw proceeds, and re-target victims.

- **Future state with C-22**: Under the Bill, the officer applies to a Canadian court for authorization to request the data directly from the foreign provider, using a clear legal framework that international partners recognize. This dramatically compresses the timeline and reduces the risk of evidence loss, while ensuring judicial oversight of cross-border data requests.

For Parliamentarians, the core point is that this is not "extra-territorial surveillance." It is a clear, court-supervised mechanism for asking foreign companies to cooperate in serious criminal cases, replacing today's patchwork of informal requests and lengthy diplomatic channels.

4.5 Ensuring Providers Can Comply with Lawful Orders

Part 2 of Bill C-22 would enact the *Supporting Authorized Access to Information Act*, establishing a framework to address a problem that warrant and production order reforms cannot solve on their own: investigators may have lawful authority to obtain information, but the relevant electronic service provider may lack the technical capability to produce it.

For our Members, the distinction between legal authority and technical capability is critical. A judicial authorization does not, by itself, ensure that a provider can isolate, retrieve and securely deliver the information covered by that authorization. Part 2 would establish requirements intended to make lawful access workable, rather than leaving investigators dependent on inconsistent technical arrangements.

The framework provides two complementary mechanisms:

- **Core-provider regulations:** The Governor in Council could prescribe classes of "core providers" and establish baseline technical obligations to facilitate authorized access.
- **Individual ministerial orders:** The Minister of Public Safety could impose specified obligations on electronic service providers through the applicable statutory process, including independent approval by the Intelligence Commissioner.

These mechanisms should not be confused with the authority to obtain evidence in an individual investigation. Capability requirements would help ensure that providers are technically equipped to respond; investigators would still require a separate lawful basis to obtain the information. Part 2 does not itself authorize police to intercept communications or access an individual's information.

The framework also recognizes that technical obligations must be feasible, proportionate and secure. It expressly requires consideration of compliance feasibility, costs, impacts on users, privacy and cybersecurity when establishing relevant regulatory requirements and ministerial orders. Ministerial orders may also provide for reasonable compensation. These provisions create mechanisms for addressing substantiated implementation concerns without abandoning the principle that relevant providers should support lawfully authorized investigations.

The House passed safeguards further limit what providers can be required to do. Obligations cannot require the introduction of a systemic vulnerability or prevent a provider from correcting one. Nor can they be construed as compelling a provider to decrypt information encrypted by a service user, or ensure that authorities can decrypt it, unless the provider supplied the encryption and possesses the information necessary to decrypt it.

The NPF supports these safeguards. Our objective is not to require providers to deliver information they cannot lawfully or technically access. It is to establish clear, enforceable and appropriately tailored

obligations so that relevant providers can give meaningful effect to lawful authorizations within the limits established by Parliament.

Implementation will be important. In developing regulations, the government should assess appropriate coverage of relevant telecommunications, messaging, cloud and virtual private network services, including foreign-based services used in Canada. Coverage and obligations should be evidence-based, technically feasible and proportionate to the services involved, while remaining consistent with the Bill's encryption and cybersecurity protections. The NPF encourages meaningful consultation with frontline investigators and technical experts to ensure that the framework addresses demonstrated investigative gaps.

The Senate should preserve this capability framework. Where providers identify concerns, the Committee should ask them to identify the precise obligation at issue, explain its technical or legal implications, and address the feasibility considerations and safeguards already included in the House passed text. Further restrictions should respond to demonstrated deficiencies, not leave investigators with lawful authorizations that remain ineffective in practice.