



Canadian Association of Chiefs of Police
Association canadienne des chefs de police

Submission to the
House of Commons' Standing Committee on
Public Safety and National Security

Bill C-22: An Act respecting lawful access

Submitted by:

Commissioner Thomas Carrique

(President)

Representing:

Canadian Association of Chiefs of Police

May 26, 2026

Distinguished committee members. Thank you for the opportunity to comment on Bill C-22. Today, virtually every serious criminal investigation has a digital component.

Organized crime groups, child predators, fraudsters, violent offenders, and extremists rely on encrypted communications, digital platforms, anonymization tools, and foreign-based services to coordinate criminal activity, evade detection, frustrated prosecution; and, ultimately, victimize innocent Canadians.

Criminals are leveraging digital infrastructure and encryption, while the police are hindered by outdated legislation that does not prioritize public safety.

Bill C-22 is not about expanding unchecked police powers. It's about ensuring that judicially authorized investigations can function effectively in a complex and ever-changing digital environment.

To the benefit of bad actors, too often, lawful access debates focus exclusively on the privacy interests of suspects and the financial interests of big tech, while overlooking the rights of victims to safety, justice, and timely intervention.

The police are not asking for; nor does, Bill C-22 authorize broad surveillance.

It does not permit warrantless interception of communications. It does not eliminate judicial oversight; and it does not provide unrestricted access to browsing history or social media content.

The legislation preserves *Charter* protections and maintains judicial authorization requirements for advanced investigative techniques. Bill C-22 also addresses practical investigative gaps.

For example, it creates a confirmation-of-service process — a simple “yes” or “no” — so, investigators can determine which telecommunications provider actually hold relevant records before spending valuable time seeking judicial authorization for records that do not exist.

It creates a production order process for basic subscriber information based on reasonable suspicion, allowing investigators to advance early-stage investigations.

It also addresses delays involving foreign-held evidence, where investigators currently rely on mutual legal assistance processes that can take many months while evidence disappears.

In fact, Bill C-22 provides clearer statutory rules in areas where courts, providers, and investigators currently face inconsistent interpretations and legal uncertainty.

Bill C-22 prevents the harboring of criminals by setting out the requirement for electronic service providers to develop and maintain systems capable of providing police with communication and information we are legally authorized to obtain, and require, to advance criminal investigations.

It is important to note – C-22 is not a surveillance tool; it is a lawful access framework.

Metadata will be retained for a maximum of one year, including information such as date, time, duration, or origin of transmission, it is critical to note that there will be no obligation to retain content such as emails, web browsing history, or social media activities.

Furthermore, retention does not equal access - judicial authorisation will still be required.

Metadata is the bare minimum of information that could assist investigators in complex investigations such as homicide; international child sexual exploitation; extortion; or cross border auto thefts, human trafficking, and the smuggling of drugs and firearms. drug trafficking.

These types of crimes can far exceed a one-year investigation period and can all involve the need for lawful access.

Absent reasonable suspicion of criminal activity, police will not, and can not, judicially seek and lawfully obtain telecommunication metadata about a private citizen of Canada going about their daily lives.

Additionally, there are other safeguards built into the Act. Regulations made by the Governor in Council must consider privacy and cyber security impacts, feasibility, costs to providers and impacts to customers, and the Intelligence Commissioner must approve orders prior to their issuance to an electronic service provider.

Bill C-22 also prevents any requirement that will cause an electronic service provider to introduce a systemic vulnerability - defined in the Act as a "*substantial risk that secure information could be accessed by a person who does not have any right or authority to do so*".

Frankly, from a law enforcement perspective, the concerns by some major telecommunications companies, and special interest privacy advocates, about encryption and cybersecurity are overstated.

The legislation as written does not compel companies to weaken encryption or create vulnerabilities; but rather, under a legislative framework, it ensures electronic services providers are not serving as a safe haven for criminal and terrorist-related activity compromising public safety locally, nationally, and internationally.

In closing, the CACP believes Bill C-22 strikes a reasonable and necessary balance between privacy; accountability; victims' rights; and public safety and urges Parliament to advance this critically needed legislation.

Thank you.