Bearing Institute
BearingInstitute.ca
Safe passage for good policy.

Surveillance Without Suspicion: The Structural Dangers of Bill C-22, the Lawful Access Act

A Policy Analysis of Canada's Proposed Digital Surveillance Framework

Bearing Institute
May 2026 | Matthew Trenholm, MSc | Bearing Institute

Executive Summary

Bill C-22, the Lawful Access Act, was introduced on March 12, 2026, and referred to the Standing Committee on Public Safety and National Security on April 20, 2026. Bearing Institute does not oppose lawful access reform. Canada needs modern investigative tools for a digital world, and the bill contains some legitimate provisions. The question is whether Parliament understands what else it is passing. Buried in Part 2 of Bill C-22 is a mandatory metadata retention regime that would require electronic service providers to store location data, communication patterns, and device identifiers for every Canadian, with no suspicion required, no crime alleged, and no individual trigger needed. On retention, this would place Canada ahead of most of its Five Eyes allies, two of which impose no mandatory retention at all, while the broadest of the others still reaches a narrower set of providers than this bill. That data would include a record of everyone who visited a reproductive health clinic, an addiction treatment centre, a gender-affirming care provider, or a mental health facility, reconstructed not from the content of their communications but from their location history alone. Under Part 1 of the same bill, that data could be reached by foreign law enforcement. The bill creates its own route for enforcing foreign production demands against data held in Canada, and U.S. law already compels Canadian data held by American providers, including for agencies in jurisdictions that have pursued extraterritorial reach over residents who seek abortion care out of state. This brief identifies six structural problems in Bill C-22 that require amendment before it can become law consistent with the Charter. It recommends six specific amendments, ready to be tabled, that would preserve the bill's legitimate investigative goals while removing the provisions that pose the greatest risk to Canadians' privacy, safety, and constitutional rights.

Part 1: The Metadata Problem and a Record of Every Canadian's Most Sensitive Moments

Begin with a concrete question Parliament has not been asked to answer: what is in this data?

Section 5(2)(d) of the Supporting Authorized Access to Information Act (SAAIA), enacted by Part 2 of Bill C-22, authorizes regulations requiring "core providers" to retain categories of

metadata, including transmission data covering the date, time, duration, type, and device location of every communication, for up to one year. The government has been clear that this does not include the content of messages. It has been considerably less forthcoming about what it does include.

Location data retained under this power can reconstruct a person's physical movements through cell tower signals and device identifiers. That reconstruction is not approximate. Modern location metadata can often be sufficiently precise to infer visits to specific buildings or facilities. Retained for twelve months, it is a comprehensive diary of everywhere a person went and when, not a snapshot but a continuous record.

As Canadian privacy lawyer David T.S. Fraser stated in testimony before the Standing Committee on Public Safety and National Security on May 7, 2026: "Collected metadata will be sought by Canadian and non-Canadian authorities based on mere suspicion. That's a record of everyone who sought reproductive health care in Canada, which might be of interest to law enforcement from a Five Eyes partner."

This is not a hypothetical. It is a description of what the metadata contains, what the bill authorizes, and what foreign partners can request. Consider what that data reveals about ordinary Canadians who have committed no offence:

If a Canadian's location metadata shows…	The data could reveal…	Who might seek it
Regular visits to a reproductive health clinic	Abortion, contraception, or fertility care	U.S. state law enforcement where interstate travel for abortion is criminalized
Visits to a gender-affirming care provider	Gender identity and medical treatment decisions	Foreign jurisdictions that criminalize gender-affirming care; domestic actors
Regular attendance at an addiction treatment centre	Substance use disorder and treatment	Employers, insurers, immigration authorities
Visits to a mental health clinic or psychiatric facility	Mental health diagnoses and treatment	Insurers, licensing bodies, custody proceedings
Repeated location at an HIV clinic or sexual health centre	HIV status and sexual health decisions	Foreign jurisdictions, immigration, employers
Attendance at a place of worship	Religious affiliation and practice	Foreign governments targeting religious minorities; domestic actors in sensitive proceedings
Presence at a protest or political rally	Political association and activism	Foreign governments, intelligence services, employers

Source: Bearing Institute analysis of Bill C-22, s. 5(2)(d) SAAIA and Part 1 information-sharing provisions, cross-referenced with David T.S. Fraser (McInnes Cooper) SECU testimony, May 7, 2026.

The government has insisted that Part 2 of Bill C-22 does not create new authorities to access this data, that existing judicial authorization requirements still apply. That argument is substantially misleading for two reasons.

First, the access threshold in Part 1 of the same bill has been lowered. The subscriber information production order created by Bill C-22 requires only "reasonable grounds to suspect," the lowest investigative standard in Canadian criminal law. A person's location history, retained for a year under Part 2 and accessed through a production order under Part 1, would be obtained at that reduced threshold. The two parts of the bill interact in ways the government has not adequately explained.

Second, section 20 of the SAAIA creates a provision the government has barely acknowledged: persons designated by the Minister can enter any premises without a warrant and without notice, can examine, copy, and remove any information found in that place, and can order anyone present to provide any data they ask for. If those premises are an electronic service provider's offices, that includes access to information about their customers. The government's own Charter Statement does not address this provision.

Bearing Institute Alert *The government's Charter Statement for Bill C-22 is silent on mandatory metadata retention, the most constitutionally vulnerable provision in the bill, and silent on the warrantless ministerial entry power in section 20 of the SAAIA. Parliament is being asked to pass provisions the government has not defended under the Charter it claims to respect.*

The Five Eyes Dimension: When Canada's Data Becomes America's Evidence

Part 1 of Bill C-22 includes provisions enabling information sharing with foreign law enforcement partners. Canada is a member of the Five Eyes intelligence alliance, which includes the United States. The practical consequence of combining mandatory metadata retention with cross-border sharing powers is that data collected on every Canadian could be requested by American law enforcement agencies.

This is not an abstract risk. As of 2026, several U.S. states have enacted laws or pursued measures asserting extraterritorial jurisdiction over residents who seek abortion care out of state, including laws targeting adults who assist minors in travelling for that purpose. While broad travel bans remain legally precarious, the legislative trend is toward expanding state reach beyond their own borders. Several of these states have enacted laws that assert extraterritorial jurisdiction. A Canadian woman's cell tower location data, showing visits to a reproductive health clinic in Toronto, retained for twelve months under Bill C-22, could create the possibility of responsive disclosure under existing or future international cooperation mechanisms, including foreign law enforcement requests made through the bill's information-sharing framework.

The Centre for Free Expression at Toronto Metropolitan University has described this dimension of the bill as creating "an untenable threat to privacy" that goes beyond what any comparable Western jurisdiction has legislated. The Electronic Frontier Foundation has confirmed that the bill's data-sharing and retention provisions, taken together, expand information flows to foreign governments in ways that have no equivalent in U.S., UK, or Australian law.

Parliament has not been asked to consider this consequence. No committee witness has been asked to estimate how many Canadians' medical location data could be responsive to U.S. law enforcement requests under this framework. No impact assessment has addressed it. The government's position, that the bill fills gaps left by Supreme Court decisions in Spencer and Bykovets, does not speak to the cross-border dimension at all.

Bearing Institute Alert *Bill C-22 does not just create a surveillance database of Canadians' most sensitive movements. Through its information-sharing provisions, it creates a database that foreign law enforcement can request access to. The government has not addressed this consequence in any public statement, any committee appearance, or any Charter analysis.*

There is a dimension of the metadata retention and information-sharing provisions that has not been raised before this committee, and that the government has not addressed. Bill C-22 requires Canadian providers to retain location metadata for anyone connected to a Canadian network, including foreign nationals visiting Canada. A U.S. citizen who travels to Canada to obtain reproductive healthcare that is legal here but criminalized in her home state would generate location metadata showing her presence at a Canadian reproductive health clinic. That data would be retained for up to one year under Part 2 of this bill. Under Part 1, the retained data could become potentially responsive to foreign law enforcement requests made through existing or future international cooperation mechanisms, including requests from U.S. agencies operating under a reasonable grounds to suspect threshold. Several U.S. states have enacted laws asserting extraterritorial jurisdiction over residents who travel to obtain abortion care, and in some cases over anyone who assists that travel. Bill C-22 would make Canada's telecommunications infrastructure a potential instrument of that enforcement, retaining evidence of legal medical activity in Canada, accessible on a low evidentiary threshold to the foreign agencies most interested in it. The government has not addressed this consequence anywhere in its public statements, its committee appearances, or its Charter Statement. Parliament should require it to do so before this bill proceeds.

Part 2: The Salt Typhoon Precedent — When Backdoors Become Entry Points

The case against building government surveillance infrastructure into private communications networks is no longer theoretical. It has already happened, at scale, to Canada's closest ally, and it happened because of exactly the kind of legislation Bill C-22 proposes to enact.

In late 2024, Chinese state hackers affiliated with a group known as Salt Typhoon compromised the systems of at least nine major U.S. telecommunications companies, including AT&T, Verizon, and T-Mobile. U.S. officials and cybersecurity reporting indicated that the attackers exploited systems associated with lawful intercept infrastructure required under the Communications Assistance for Law Enforcement Act (CALEA). Rather than bypassing surveillance architecture, the intrusion appears to have leveraged the very systems designed to facilitate lawful government access.

The hackers stayed inside those networks for as long as three years before detection. They accessed metadata of calls and text messages from over a million users. They obtained an

almost complete list of phone numbers currently under U.S. government surveillance, exposing counterintelligence operations and identifying Chinese agents the U.S. had under surveillance. They accessed the personal phones of both Donald Trump's and Kamala Harris's campaign staff. Senator Mark Warner, Chair of the U.S. Senate Intelligence Committee, called it "the worst telecom hack in our nation's history."

The Electronic Frontier Foundation summarized the lesson in one sentence: "There is no backdoor that only lets in good guys and keeps out bad guys." The surveillance architecture built for law enforcement became the entry point for foreign state intelligence. The backdoor that was supposed to catch criminals handed China a master key to American communications.

Canada's own security agencies understand this. CSIS and the Canadian Centre for Cyber Security, together with allied nations' cybersecurity agencies, have issued guidance specifically advising the adoption of encryption and disabling of unencrypted protocols. They have recommended against the construction of the precise kind of architecture Bill C-22 would mandate. The bill's own sponsors are asking Parliament to build infrastructure that Canada's intelligence community has warned against building.

The Salt Typhoon parallel is directly applicable to Bill C-22 for three reasons. First, CALEA, the U.S. law whose surveillance infrastructure Salt Typhoon exploited, is substantially narrower than Bill C-22. CALEA covers traditional telecommunications; it does not apply to messaging apps or cloud services, and does not mandate pre-emptive metadata retention. Bill C-22 is broader than the law whose failure produced the worst telecom breach in American history. Second, an unnamed Canadian telecom company was breached by Salt Typhoon in February 2025, before Bill C-22 exists and before any mandatory surveillance infrastructure has been built. Third, the mandatory metadata retention provision would create a concentrated database of sensitive information about every Canadian, exactly the kind of high-value target that Salt Typhoon demonstrated hostile state actors will seek out and exploit.

CALEA (United States, 1994)	Bill C-22 (Canada, proposed 2026)	Assessment
Applies to traditional telecoms	Applies to all "electronic service providers": messaging apps, cloud services, social media, AI tools, potentially any smart device	Bill C-22 is dramatically broader
No mandatory metadata retention	Mandatory metadata retention for up to one year, potentially for all Canadians	Bill C-22 goes further than CALEA on its most dangerous dimension
No ministerial orders; judicial authorization required	Secret ministerial orders, approved by Intelligence Commissioner (not a court)	Bill C-22 provides weaker judicial oversight
Backdoor exploited by Salt Typhoon in 2024; 9 telecoms breached; worst hack in U.S. history	Bill C-22 mandates equivalent or broader infrastructure in Canada	Canada is legislating the architecture that failed catastrophically in the U.S.

CALEA (United States, 1994)	Bill C-22 (Canada, proposed 2026)	Assessment
No cross-border sharing provision	Part 1 includes foreign law enforcement sharing framework	Bill C-22 adds cross-border dimension absent from CALEA

Sources: CALEA (47 U.S.C. § 1001 et seq.); Bill C-22 first reading text (parl.ca); Salt Typhoon Wikipedia (wikipedia.org); EFF (eff.org); Canadian Chamber of Commerce (theglobeandmail.com)

Part 3: Five Structural Problems That Require Amendment

3.1 Mass Metadata Retention: Population-Wide Surveillance Without a Constitutional Basis

Section 5(2)(d) of the SAAIA authorizes regulations requiring core providers to retain location data, device identifiers, communication timing, and transmission data for every Canadian for up to one year, regardless of whether any individual is suspected of anything. The constitutional problem is direct: the Supreme Court's decisions in R. v. Spencer (2014) and R. v. Bykovets (2024) established that information linking online activity and location to a person's identity attracts Charter section 8 protection. The U.S. Supreme Court reached a similar conclusion in Carpenter v. United States (2018), holding that historical cell-site location information provides "an intimate window into a person's life," capable of revealing "familial, political, professional, religious, and sexual associations." The constitutional concern surrounding location metadata is therefore not uniquely Canadian. It reflects an emerging cross-jurisdictional recognition that digital location records function as deeply revealing biographical surveillance data. A blanket obligation to retain that information for tens of millions of people without any individualized trigger is inconsistent with those decisions.

The international constitutional record is unambiguous. The Court of Justice of the European Union struck down the EU Data Retention Directive in Digital Rights Ireland (2014), holding that general and indiscriminate retention of telecommunications metadata was a disproportionate interference with fundamental rights. In Tele2 Sverige, the CJEU extended that reasoning to national retention laws. Germany has no mandatory metadata retention and is instead debating a "quick freeze" model in which law enforcement can require preservation of data relating to a specific suspect. The government's Charter Statement does not address any of this.

Critics including Professor Michael Geist, Canada Research Chair in Internet and E-Commerce Law at the University of Ottawa, have noted that the bill's metadata retention requirements were introduced without prior public consultation or notice, a significant departure from the approach taken in the bill's predecessor, Bill C-2, which contained no equivalent provision. Parliamentary Secretary Ruby Sahota has described the bill publicly as 'a first step,' signalling that the government views the current surveillance framework as a foundation to be expanded rather than a fixed limit. This is confirmed by the legislative record: there was no metadata retention provision in Bill C-2. The provision has been inserted without the prior public consultation or notice that a measure of this constitutional significance requires, and without the government having produced any analysis of its Charter compliance.

A further concern that has received inadequate attention is the bill's definition of "electronic service provider." As drafted, that definition is broad enough to capture not only telecoms and messaging platforms but doctors' offices, law firms, pharmacies, hotels, and accounting practices, any entity that provides a service electronically to persons in Canada. Privacy lawyer David Fraser told this committee that under the bill as written, police could demand records from doctors' offices and hotels. Parliament does not yet know which of these entities will bear mandatory retention obligations, because the regulatory definition of "core provider," the class subject to the bill's most significant requirements, has not been published. Parliament is being asked to vote on obligations whose scope has not been defined. That is not a minor drafting gap. It is a fundamental accountability failure: the government is asking Parliament to authorize a surveillance regime and promising to tell it later who the regime applies to.

Where Bill C-22 Sits Among the Five Eyes

The government's central justification for Bill C-22, repeated in the Library of Parliament's legislative summary, is that Canada is the only country among its Five Eyes partners, the G7, and the European Union without legislation requiring service providers to develop and maintain lawful-access capabilities. On the narrow question of capability, that is accurate. The fuller picture is set out below.

Jurisdiction (law)	Lawful-access capability mandate	Mandatory metadata retention	Provider scope
United States (CALEA, 1994)	Yes, interception capability	No mandatory retention	Traditional telecom carriers
United Kingdom (Investigatory Powers Act, 2016)	Yes, technical capability notices	Targeted only: up to 12 months, by retention notice, each approved by an independent Judicial Commissioner	Telecommunications operators (broad)
Australia (TIA Act, Data Retention amendments, 2015)	Yes, interception capability	Yes, blanket: 2 years, a prescribed data set, by statute	Carriers, carriage service providers, ISPs
New Zealand (TICSA, 2013)	Yes, interception capability and network security	No mandatory retention	Public telecommunications network operators
Canada (Bill C-22, proposed 2026)	**Yes, SAAIA capability obligations and ministerial orders**	**Yes, up to 1 year, imposed by regulation on "core providers" (class not yet published)**	**"Electronic service providers": telecom, messaging, cloud, social media, potentially broader**

Source: Communications Assistance for Law Enforcement Act, 47 U.S.C. ss. 1001 et seq.; Investigatory Powers Act 2016 (UK), Part 4, s. 87 (legislation.gov.uk); Telecommunications (Interception and Access) Act 1979 (Australia), Part 5-1A, as amended by the Data Retention Act 2015 (Department of Home Affairs; OAIC); Telecommunications (Interception Capability and Security) Act 2013 (New Zealand), Parts 2 and 3 (NZ Police; GCSB); Bill C-22 and the SAAIA, and Library of Parliament, Legislative Summary of Bill C-22 (45-1-C22-E, March 17, 2026). Compiled by Bearing Institute from primary statutory and government sources, June 2026.

Two things the comparison makes clear. First, the capability gap is real. The United States, the United Kingdom, Australia, and New Zealand all require providers to maintain interception capability, and Canada, until now, did not. To that extent Bill C-22 closes a genuine gap, and the government is right to say so.

Second, and this is what the government's framing obscures, Bill C-22 does not stop at capability. It adds a mandatory metadata retention regime, and on that dimension Canada would not be catching up to its allies. It would be joining the more aggressive half of them. The United States and New Zealand impose no mandatory retention at all. The United Kingdom requires it only by targeted notice, for a maximum of twelve months, and only after an independent Judicial Commissioner approves each notice. Only Australia imposes blanket statutory retention, at two years. Canada's proposal is blanket retention by regulation, and it applies to the broadest class of providers in the comparison: not telecom carriers alone, as in every peer regime, but "electronic service providers," a category broad enough to reach messaging platforms, cloud services, and potentially well beyond. The claim that Bill C-22 simply brings Canada into line with its allies is true of the capability mandate and misleading about the retention regime bundled with it.

Bearing Institute Alert *On the capability mandate the government emphasizes, Canada is indeed the last of the Five Eyes to legislate. On the mandatory retention regime the government does not foreground, two of the four other Five Eyes countries impose no retention at all, a third requires independent judicial approval for each targeted notice, and only one imposes blanket retention, at a provider scope narrower than Bill C-22's. On retention and scope, the bill does not catch Canada up. It moves Canada ahead of most of its allies.*

A further dimension concerns cross-border access. The United Kingdom and Australia have each concluded a bilateral data access agreement with the United States under the U.S. CLOUD Act, the UK agreement in force since October 2022 and the Australian since January 2024, allowing each country's authorities to serve orders directly on providers in the other and bypass the slower mutual legal assistance process. Canada has been negotiating an equivalent agreement with the United States since March 2022, but as of early 2026 none has been concluded and no timeline has been set. The U.S. CLOUD Act already reaches data held by U.S.-based providers regardless of where it is stored, so U.S. process can reach Canadian data held by U.S. companies today. Should a Canada-US agreement be concluded on the trajectory the other Five Eyes agreements set, the metadata Bill C-22 requires Canadian providers to retain would become directly accessible to U.S. law enforcement, on U.S. legal process, outside the mutual legal assistance oversight that currently applies.

Parliament need not wait for any new agreement to see how the retained data could move abroad, because the bill builds a route itself: new section 22.07 of the Mutual Legal Assistance in Criminal Matters Act would let the Minister of Justice authorize the enforcement in Canada of a foreign authority's decision compelling production of transmission data or subscriber information held by a person in Canada. Enforcement requires a Canadian judge to be satisfied of the conditions in s. 487.0142(2) or s. 487.016(2) of the Criminal Code, the same reasonable grounds to suspect standard criticized in Part 3.4, so the lowest threshold in Canadian criminal

law would govern not only domestic access to this data but the enforcement of foreign demands for it. That route is in the bill now, independent of whether any data-sharing agreement is ever concluded. Parliament is being asked to mandate the database before the rules for cross-border access to it are settled.

3.2 The Section 20 Problem: Warrantless Entry the Government Won't Talk About

Section 20 of the SAAIA creates a power that has received almost no attention in parliamentary debate or media coverage: persons designated by the Minister of Public Safety may enter any electronic service provider's premises without a warrant, without notice, at any reasonable time, and may examine, copy, and remove any information or document found there. Employees of the provider must give all reasonable assistance. If those premises contain customer records, the warrantless entry extends to customer data.

The government's position is that this is a compliance inspection power, designed to verify that providers are meeting their obligations under the SAAIA, not to access customer communications. That distinction is not drawn in the text of section 20. The provision contains no limit on the category of information that may be examined or copied. Privacy lawyer David Fraser, in committee testimony, described section 20 as creating "no guardrails." The government's Charter Statement acknowledges that the entry and inspection powers "may engage section 8 of the Charter" but does not analyze that engagement in relation to section 20 specifically.

The government has also asserted that section 20 is not a new authority to access data. That claim is difficult to reconcile with what the provision actually says. Entering premises without warrant, examining and copying any information found, and ordering employees to provide any requested data is, on its face, access to data without judicial authorization.

3.3 Secret Ministerial Orders: Cabinet-Defined Surveillance Infrastructure

Section 7 of the SAAIA gives the Minister of Public Safety the power to issue orders directing any electronic service provider to build or maintain a specific technical capability. These orders are issued in secret, with mandatory non-disclosure obligations on the receiving company. The capability that can be ordered is not defined in the bill beyond what the minister determines is necessary for lawful interception.

The scope of this provision extends, in principle, to any device or service provided to Canadians. Privacy lawyer David Fraser noted in SECU testimony that "the Minister could issue a secret order to turn your Amazon Alexa into a listening device." The Centre for Free Expression at Toronto Metropolitan University noted that the bill could "force Canadian companies to build backdoors into their products before they export them abroad."

The Intelligence Commissioner oversight mechanism added to Bill C-22 (which was absent from its predecessor Bill C-2) is an improvement. But approval by the Intelligence Commissioner is not judicial authorization. The Commissioner conducts national security review functions; the Commissioner does not apply the criminal law standard of reasonableness that Charter section 8 requires. NSIRA has itself told the committee that it does not have adequate access to conduct effective oversight of orders issued under this provision.

The UK government used an equivalent ministerial order mechanism to secretly require Apple to remove encryption from iCloud globally, an order Apple refused to comply with, resulting in Apple withdrawing the Advanced Data Protection feature from the UK market. Bill C-22 contains no guardrail that would prevent the same outcome in Canada. Signal has already stated it would withdraw from the Canadian market rather than comply with a capability order compromising its encryption.

3.4 The Lowered Evidentiary Threshold: Inverting Supreme Court Reasoning

Part 1 of Bill C-22 creates a subscriber information production order allowing a judge to order disclosure of a person's name, address, account details, and device identifiers at the threshold of "reasonable grounds to suspect," the lowest investigative standard in Canadian criminal law. This directly contradicts the existing standard.

Since Spencer (2014), subscriber information has required a general production order under s. 487.014 of the Criminal Code, requiring "reasonable grounds to believe," the same standard as a search warrant. In Bykovets (2024), the Supreme Court reaffirmed that location and identity-linking data carries significant constitutional sensitivity. Bill C-22 responds to those decisions by creating a dedicated order for exactly the type of information the Court flagged as constitutionally sensitive, at a lower threshold than the Court has required.

The government's defence of the lower threshold, that it is "higher than mere suspicion," reveals the weakness of the position. "Mere suspicion" is not a threshold for search in Canadian law. It is the standard courts point to when a search is unconstitutional. Defending a standard as "not the most clearly unconstitutional option" is not a justification for choosing it over the higher standard that has governed this category of information since 2014.

The clearest way to see what the bill does is to place its new tools inside the existing hierarchy of Criminal Code production orders and warrants. Over three decades, Parliament has assigned higher or lower thresholds to investigative tools according to how revealing the information each one reaches is. The table below sets out where each existing tool sits, and where Bill C-22 places its new powers.

Investigative tool	Provision	Information it reaches	Threshold required
Part VI interception (wiretap)	Criminal Code s. 186	Content of private communications	Reasonable grounds to believe, plus investigative necessity
General production order	Criminal Code s. 487.014	Documents and data generally, including subscriber information since R. v. Spencer (2014)	Reasonable grounds to believe
Tracking warrant, an individual's movements	Criminal Code s. 492.1(2)	Movement of an individual via a device usually worn or carried	Reasonable grounds to believe
Specified-communication tracing order	Criminal Code s. 487.015	Transmission data identifying a device or person in a transmission	Reasonable grounds to suspect

Investigative tool	Provision	Information it reaches	Threshold required
Transmission data production order	Criminal Code s. 487.016	Transmission data (routing, addressing, signalling; not content)	Reasonable grounds to suspect
Tracking data production order	Criminal Code s. 487.017	Historical tracking data	Reasonable grounds to suspect
Financial data production order	Criminal Code s. 487.018	Financial account data	Reasonable grounds to suspect
Tracking warrant, things and transactions	Criminal Code s. 492.1(1)	Location of a thing, a vehicle, or a transaction	Reasonable grounds to suspect
Transmission data recorder warrant	Criminal Code s. 492.2	Real-time transmission data	Reasonable grounds to suspect
Subscriber information production order (NEW)	**Bill C-22, cl. 6, new Criminal Code s. 487.0142**	**Full subscriber information: name, address, account and service details, pseudonyms, assigned identifiers, device and equipment information**	**Reasonable grounds to suspect (offence)**
Confirmation of service demand, law enforcement (NEW)	**Bill C-22, cl. 5, new Criminal Code s. 487.0121**	**Yes or no confirmation that a telecom provider serves a named subscriber, account, or identifier**	**Reasonable grounds to suspect (offence); no prior judicial order**
Confirmation of service demand, CSIS (NEW)	**Bill C-22, cl. 31, new CSIS Act s. 20.22**	**The same yes or no confirmation, on demand by CSIS**	**CSIS mandate trigger: reasonable grounds to suspect a threat to the security of Canada (CSIS Act s. 12) or foreign-intelligence collection (s. 16); no offence required; no prior judicial order**
International production request (NEW)	**Bill C-22, cl. 7, new Criminal Code s. 487.0181**	**Subscriber information or transmission data held by a foreign provider (a "request," not an order)**	**Reasonable grounds to suspect (offence)**

Source: Criminal Code, R.S.C. 1985, c. C-46, ss. 186, 487.014 to 487.018, 492.1, 492.2 (Justice Laws Website); Bill C-22 new Criminal Code ss. 487.0121, 487.0142, 487.0181 and new CSIS Act s. 20.22; Canadian Security Intelligence Service Act, R.S.C. 1985, c. C-23, ss. 12, 16; Library of Parliament, Legislative Summary of Bill C-22 (45-1-C22-E, March 17, 2026); Canadian Bar Association, Submission on Bill C-22 (confirming s. 487.0181); R. v. Spencer, 2014 SCC 43; R. v. Bykovets, 2024 SCC 6; Department of Justice, Charter Statement for Bill C-22. Hierarchy compiled by Bearing Institute from primary statutory sources, June 2026. "Reasonable grounds to believe" is the search-warrant standard; "reasonable grounds to suspect" is the lowest investigative standard in Canadian criminal law (R. v. Chehil, 2013 SCC 49).

The hierarchy exposes an internal inconsistency. The Code already treats some location data as deserving the higher standard: a warrant to track an individual's movements through a device they carry or wear requires reasonable grounds to believe under section 492.1(2). Bill C-22 would let police obtain the identity and location-linking subscriber data that the Court flagged in Spencer and Bykovets at a threshold one full tier below that. The bill takes the single category of metadata the Supreme Court has most clearly identified as constitutionally sensitive and routes it through the lowest gate the Criminal Code contains.

This is not only a rights concern. It is a prosecutorial risk. In R. v. West (2020 ONCA 473), the Ontario Court of Appeal excluded evidence obtained through a production order for IP-address subscriber information, the very category Bill C-22's new order reaches, because the officer's information to obtain had asserted only grounds to suspect where grounds to believe were required. The Crown's case collapsed and acquittals were entered. The distinction between the two standards is not semantic. It can be the difference between evidence a court admits and evidence it excludes, which means a threshold set too low does not only expose Canadians, it exposes the prosecutions the provision is meant to support.

Bearing Institute Alert *Bill C-22 creates a new production order for the exact category of data, subscriber and identity-linking information, that the Supreme Court singled out for protection in Spencer and Bykovets, and assigns it the lowest evidentiary threshold in Canadian criminal law. Every other tool in the Criminal Code that reaches comparably revealing information sits at a higher standard.*

Two further features of the subscriber information order compound the threshold problem, and both concern the same provision. The first is its breadth. New section 487.0142 does not let the judge tailor the order to the particular subscriber details an investigation needs. It compels production of all the subscriber information related to the identifier or data specified in the application, and subscriber information is defined expansively in the bill: a person's name, pseudonyms, address, telephone number and email address, every account identifier assigned to them, the types of services they receive, the period over which they received them, and the identifiers of the devices and equipment they used. The judge specifies what the police are matching against. The judge does not get to limit what comes back. The Privacy Commissioner has flagged exactly this, recommending that the provision be amended so the order produces only the subscriber information specified in it rather than all of it. As drafted, an order seeking to confirm a single detail sweeps in the subscriber's entire service and device profile.

The second feature is sharper, because it runs against the logic the rest of the bill follows. The confirmation of service demand, the narrow yes-or-no power that Part 4 of this brief credits as proportionate, must not be made if it would disclose medical information or information subject to solicitor-client privilege or the professional secrecy of advocates and notaries. The CSIS confirmation demand carries the identical carveout. The subscriber information production order carries none. Yet the production order is the broader instrument: the demand reaches only telecommunications providers, while the order can be served on any person who provides services to the public, which, as Part 3.1 notes, includes doctors' offices and law firms. The result is inverted. The bill shields medical and privileged information from its least intrusive tool and strips that shield from the more intrusive one, the very tool capable of reaching the

providers who hold such information. A production order to a medical clinic or a law office for subscriber data would carry no statutory protection for the categories of information the demand is forbidden to touch.

The CSIS dimension requires precision. Bill C-22 does not create a CSIS version of the subscriber information production order. What it gives CSIS, through new section 20.22 of the CSIS Act, is the confirmation of service demand: the power to require a telecommunications service provider to confirm whether it serves a named subscriber, account, or identifier. That demand is not triggered by suspicion of an offence. CSIS may issue it in performing its duties relating to activities that may on reasonable grounds be suspected of constituting threats to the security of Canada under section 12 of the CSIS Act, or for foreign-intelligence collection under section 16, and it carries no requirement of prior judicial authorization. A judge becomes involved only as a backstop, under section 20.24, if a provider declines to comply.

The concern in the intelligence context is therefore one of oversight rather than threshold. Unlike a criminal accused, a person of interest to CSIS will ordinarily never learn the demand was made and will have no opportunity to challenge it in open court. Bearing Institute does not propose lowering the threshold critique onto the confirmation of service demand, which, as Part 4 notes, is a proportionate tool. The point is that this CSIS power should fall squarely within the NSIRA oversight discussed in Part 3.6.

3.5 Access Without an Order: The Publicly Available Information and Foreign-Law Disclosure Gaps

Several of the bill's powers require a judge. Several of its routes to data require nothing at all. New section 487.0195 of the Criminal Code provides that no production order, warrant, or confirmation of service demand is necessary for a peace officer or public officer to receive, obtain, and act on any information that is available to the public. On its face this is unremarkable, since police have always been able to read what is genuinely public. The difficulty is that "available to the public" is not defined, and in 2026 the category is not stable. Data exposed through a breach, a hack, or an unlawful leak is, in a literal sense, available to the public, and the provision would let police obtain and act on it with no authorization and no judicial check. The Privacy Commissioner has cautioned that a person does not forfeit a reasonable expectation of privacy in their information simply because it has been disclosed without their knowledge or consent, for example through a data breach. As drafted, the bill invites investigative use of unlawfully exposed personal data, including the very metadata Part 2 would compel providers to retain, should that data ever be breached.

A second no-order route runs through subsection 487.0195(3). It provides that no order or demand is necessary for police to receive and act on information that a person provides voluntarily or is required to provide by law, including the law of a foreign state. The voluntary-disclosure piece is reasonable, since police have always been able to act on tips. The foreign-law piece is not. It would let a Canadian provider compelled by a foreign government to hand over data do so, and let Canadian police then receive and act on that data, with no Canadian order and no Canadian judicial standard ever applied. Combined with the cross-border exposure described in Part 3.1, this creates a channel in which a foreign legal demand, rather

than a Canadian judge, determines when Canadians' data reaches the authorities. The provision should not treat compulsion under a foreign law as equivalent to lawful authority in Canada.

Bearing Institute Alert *Bill C-22 requires judicial authorization for some of its powers and none for others. The undefined "publicly available" exception would let police act on hacked or leaked data, and the foreign-law disclosure provision would let a foreign legal demand, not a Canadian judge, decide when Canadians' data reaches the authorities.*

3.6 The Oversight Gap: NSIRA Cannot Do Its Job

Canada's national security oversight architecture assumes that the National Security and Intelligence Review Agency (NSIRA) can conduct effective independent review of intelligence activities. NSIRA itself has told the Standing Committee on Public Safety and National Security that, as currently drafted, the SAAIA does not give NSIRA adequate access to information to fulfill its oversight mandate in relation to ministerial orders. The bill provides NSIRA only with an unredacted copy of the Minister's annual public report, a document produced 90 days after year-end and made available to NSIRA within the first 15 sitting days thereafter.

NSIRA notes that this is anomalous. The CSIS Act and the Communications Security Establishment Act, both of which govern activities conducted pursuant to ministerial authorizations, require periodic information provision to NSIRA as a matter of course. Bill C-22 creates a new category of ministerial order with significant surveillance implications and provides less oversight access than the existing national security framework. NSIRA has proposed targeted amendments to address this gap. The government has not indicated whether it will accept them.

Part 4: What Bill C-22 Gets Right

Bearing Institute's analysis is not a rejection of lawful access reform. Several provisions in Bill C-22 represent legitimate and proportionate responses to real investigative gaps.

The confirmation of service demand is a proportionate tool. Allowing police to ask a telecom provider whether a named person is a customer, a yes or no answer with no detailed subscriber data and no location information, is a narrow power that addresses a specific gap created by Spencer without significant Charter exposure. It is the right tool for the specific problem it solves.

The Intelligence Commissioner oversight mechanism is a genuine improvement over Bill C-2, which had no equivalent check. Requiring ministerial orders to be approved before taking effect introduces a quasi-judicial review function that was entirely absent from the earlier version. It is not sufficient, but its absence would make the bill worse.

The parliamentary review requirement, a mandatory review three years after the provisions come into force, is welcome. If the bill passes with its structural problems intact, a binding parliamentary review creates at least one future accountability moment.

Meta, in its formal submission to SECU, stated that Part 1 of Bill C-22, with narrowly tailored amendments, "would provide law enforcement with an effective legal framework for obtaining necessary data in a timely manner." That assessment, from a company that is simultaneously opposing Part 2, reflects the genuine bifurcation in the bill: Part 1, fixed, is defensible. Part 2, as written, is not.

The Breadth of Opposition *Meta, Signal, Apple, NordVPN, the Canadian Chamber of Commerce, five law professors, the Centre for Free Expression, NSIRA, and the Electronic Frontier Foundation are not a coalition of organizations that typically agree on anything. Their shared opposition to Part 2 of Bill C-22 is not a coincidence. It is a signal.*

Part 5: Legislative Recommendations — Amendments You Can Table

Each of the six recommendations below is designed to preserve the legitimate investigative goals of Bill C-22 while removing the provisions that create the greatest constitutional, security, and human rights risks. The first three address Part 2, and the remaining three address Part 1, the cross-border and no-order access gaps, and the parliamentary process.

Recommendation 1: Strike the Mandatory Metadata Retention Provision (s. 5(2)(d) SAAIA)

The Action: Delete s. 5(2)(d) of the SAAIA, which authorizes regulations requiring core providers to retain metadata on all Canadians for up to one year with no individualized basis. Replace it with a targeted "quick freeze" preservation framework: law enforcement may require a specific provider to preserve data relating to a specific identified person for a defined period, subject to judicial authorization at the "reasonable grounds to believe" standard. General, population-wide retention without individualized suspicion should not be authorized.

The Goal: Mass metadata retention is inconsistent with Charter s. 8 as interpreted in Spencer and Bykovets. It has been struck down by the Court of Justice of the European Union and by multiple national constitutional courts. It creates a concentrated database of Canadians' most sensitive location data (medical visits, religious attendance, political association) that is accessible to foreign law enforcement partners. The targeted quick freeze model, used in Germany and recommended by digital rights organizations internationally, achieves the government's investigative objective without creating a national surveillance database of innocent people.

Legislative Anchor: Bill C-22, s. 41 (SAAIA, s. 5(2)(d)): delete and replace with targeted preservation framework

Recommendation 2: Remove Section 20's Warrantless Entry Power or Require Judicial Authorization

The Action: Amend section 20 of the SAAIA to require a judicially authorized warrant before any designated person may enter an electronic service provider's premises and examine, copy, or remove information. Alternatively, if an inspection power is retained, add an explicit prohibition on accessing any customer data without a warrant, and require that any document or data removed during an inspection be sealed and reviewed by an independent judicial officer before it may be used for any purpose.

The Goal: Section 20 as drafted creates a power of warrantless entry and data access that the government has not defended in its Charter Statement and has not clearly explained in committee. The government's claim that this is merely a compliance inspection power is not supported by the text of the provision, which contains no limitation on the category of information that may be examined. The warrantless entry of business premises to access electronic records engages Charter s. 8 and requires judicial authorization.

Legislative Anchor: Bill C-22, s. 41 (SAAIA, s. 20): amend to require judicial authorization

Recommendation 3: Define and Judicially Authorize Ministerial Orders; Prohibit Encryption Backdoors Explicitly

The Action: Amend s. 7 of the SAAIA to: (a) define by statute the categories of technical capabilities that can be ordered, rather than leaving scope to ministerial discretion; (b) require judicial authorization, not merely Intelligence Commissioner approval, before any ministerial order takes effect; (c) include an explicit statutory prohibition on orders that require breaking or circumventing end-to-end encryption, with the prohibition defined by reference to independent technical standards bodies rather than ministerial interpretation; and (d) require annual public reporting of the number and general nature of orders issued.

The Goal: Secret ministerial orders of undefined scope represent a departure from the rule of law. The Salt Typhoon hack demonstrated that government-mandated surveillance infrastructure creates entry points for hostile state actors. CSIS and the Canadian Centre for Cyber Security have advised against building such infrastructure. NSIRA has confirmed it cannot provide effective oversight under the current framework. Judicial authorization, not Intelligence Commissioner approval, is the standard the Canadian constitutional tradition requires.

Legislative Anchor: Bill C-22, s. 41 (SAAIA, s. 7): amend capability definition, authorization requirement, and transparency provisions

Recommendation 4: Restore the Threshold, Limit the Scope, and Protect Privileged Records in the Subscriber Information Order

The Action: Amend the subscriber information production order in Part 1 (new s. 487.0142 of the Criminal Code) in three respects. (a) Threshold: require "reasonable grounds to

believe" rather than "reasonable grounds to suspect." A tiered approach is acceptable, with basic identifying information such as name and address available at the lower threshold and detailed subscriber, device, and location-linking data requiring the higher standard that has governed this category since Spencer. (b) Scope: amend s. 487.0142(1) so the order produces only the subscriber information specified in it, rather than all of the subscriber information, as the Privacy Commissioner has recommended. (c) Privilege: add the carveout for medical information and information subject to solicitor-client privilege or professional secrecy that already applies to the confirmation of service demand and the CSIS demand, so the broader production power is no less protective than the narrow one.

The Goal: Subscriber information has attracted Charter protection since Spencer (2014), and the existing production order framework has required reasonable grounds to believe since that decision. Bykovets (2024) reaffirmed the constitutional sensitivity of location and identity-linking data, yet Bill C-22 lowers the threshold for precisely this category of information. Evidence obtained at the lower threshold is vulnerable to Charter challenge and could be excluded at trial, defeating the investigative purpose of the provision and potentially compromising prosecutions of serious crimes. The threshold is not the only defect. As drafted the order compels a subscriber's entire service and device profile rather than the detail an investigation needs, and unlike the confirmation demand it can be served on doctors, lawyers, and other custodians of sensitive records with no carveout for medical or privileged information. The three amendments address how strong the grounds must be, how much the order sweeps in, and whose protected records it can reach.

Legislative Anchor: Bill C-22, Part 1: amend new s. 487.0142 of the Criminal Code (threshold, scope, and privilege carveout)

Recommendation 5: Add Cross-Border Safeguards and Close the No-Order Access Gaps

The Action: Amend three provisions that let Canadians' data reach the authorities without a Canadian judicial standard. (a) Cross-border enforcement: amend new s. 22.07 of the Mutual Legal Assistance in Criminal Matters Act to require reasonable grounds to believe, consistent with Recommendation 4, before a foreign production decision is enforced against data held in Canada, and add a dual-criminality requirement so that no foreign decision may be enforced where it relates to conduct that is not an offence in Canada. (b) Foreign-law disclosure: amend s. 487.0195(3) of the Criminal Code so that compulsion under the law of a foreign state is not treated as lawful authority in Canada, and police may not act on data disclosed under a foreign legal demand absent the authorization that the same data would require in Canada. (c) Publicly available information: amend s. 487.0195(4) so that information "available to the public" excludes information the officer knows or ought reasonably to suspect was disclosed through a breach, a hack, or other unauthorized access.

The Goal: The bill builds the retention database and then opens several routes by which the data in it can reach law enforcement without a Canadian judge applying a Canadian standard. A foreign production decision can be enforced here on reasonable suspicion, a foreign legal demand can pull data from a Canadian provider that police then use, and unlawfully exposed data can be treated as fair game because it is, technically, public. The dual-criminality requirement is the safeguard that most directly protects the people this brief is concerned about, since it would stop Canadian infrastructure from being used to enforce foreign demands for evidence of activity, such as reproductive or gender-affirming healthcare, that is lawful in Canada. Together these amendments ensure that the Canadian constitutional standard, not a foreign one and not the accident of a data breach, governs access to Canadians' information.

Legislative Anchor: Bill C-22: amend MLAA s. 22.07 and Criminal Code s. 487.0195(3) and (4)

Recommendation 6: Require a Supplementary Charter Statement Addressing Metadata Retention, s. 20, and Cross-Border Sharing Before Third Reading

The Action: Parliament should not proceed to third reading until the government tables a supplementary Charter Statement addressing: (a) the consistency of mandatory metadata retention (s. 5(2)(d) SAAIA) with R. v. Spencer, R. v. Bykovets, and the international constitutional consensus in Digital Rights Ireland and Tele2 Sverige; (b) the constitutional basis for the warrantless entry and inspection power in s. 20 of the SAAIA; and (c) the interaction between Part 1 information-sharing provisions and foreign law enforcement requests for data about Canadians' medical, religious, and political activity.

The Goal: The government's Charter Statement is silent on the bill's most constitutionally vulnerable provisions. Under s. 4.2 of the Department of Justice Act, the Minister of Justice is required to examine legislation for Charter inconsistency. A Statement that omits the mandatory metadata retention provision and the s. 20 warrantless entry power does not fulfill that obligation. Parliament cannot make an informed decision on Charter compliance without the government's actual constitutional analysis of the provisions most likely to be challenged.

Legislative Anchor: Standing order / SECU procedural motion: condition report stage on tabling of supplementary Charter Statement

Summary: What Bearing Institute Recommends

Recommendation	Provision	Constitutional Basis	What It Preserves
1. Strike mandatory metadata retention	SAAIA s. 5(2)(d)	Charter s. 8; Spencer; Bykovets; Digital Rights Ireland	Quick-freeze targeted preservation for specific suspects

Recommendation	Provision	Constitutional Basis	What It Preserves
2. Require warrant for s. 20 entry and data access	SAAIA s. 20	Charter s. 8; rule of law	Compliance inspection with proper judicial oversight
3. Define, judicially authorize, and prohibit encryption backdoors in ministerial orders	SAAIA s. 7	Rule of law; Charter s. 8; Salt Typhoon precedent	Technical capability framework with judicial supervision
4. Restore threshold, limit scope, and add privilege carveout	New s. 487.0142 Criminal Code	Charter s. 8; Spencer; Bykovets	Subscriber information order with proper threshold, scope, and protections
5. Add cross-border safeguards and close no-order access gaps	MLAA s. 22.07; Criminal Code s. 487.0195	Charter s. 8; dual criminality; rule of law	Foreign and public-data access held to a Canadian standard
6. Require supplementary Charter Statement before third reading	Entire bill	Department of Justice Act s. 4.2; parliamentary accountability	All legitimate investigative tools in Parts 1 and 2

Conclusion

Canada needs a lawful access framework. Law enforcement agencies have legitimate digital investigative needs that the existing legal toolkit, written largely in an analogue era, does not adequately address. The Supreme Court's decisions in Spencer and Bykovets created gaps that Parliament has both the authority and the responsibility to fill. Bearing Institute does not dispute any of that.

The question is not whether lawful access legislation is needed. It is whether Bill C-22 is that legislation, or whether Parliament is, without fully understanding what it is doing, passing a mandatory mass surveillance regime disguised as a law enforcement modernization bill.

The mandatory metadata retention provision does not target criminals. It targets everyone. The data it captures does not record suspicious activity. It records medical appointments, religious attendance, political association, and intimate personal decisions, movements that reveal things people share with their doctors, not their governments. That data, retained for a year, would be accessible to foreign law enforcement partners in jurisdictions where some of those activities are criminalized.

The technical infrastructure Bill C-22 would mandate has already been built, and already been catastrophically compromised, in Canada's closest ally. The backdoors built for law enforcement became the entry point for Chinese state intelligence. Canada's own security agencies have advised against building equivalent infrastructure. Parliament is being asked to build it anyway, at a broader scale than the American law that failed.

None of this requires bad intentions on the part of the bill's sponsors. It requires only what the bill contains: a surveillance provision inserted without public consultation, a warrantless entry

power the government has not defended, and a technical capability mandate broader than anything in comparable Western jurisdictions, in a bill the government is asking Parliament to pass quickly.

The six amendments recommended in this brief would preserve Part 1's legitimate investigative tools, fix the most dangerous provisions in Part 2, and require the government to produce the Charter analysis that Parliament is owed before voting. That is not an anti-reform position. It is the minimum standard of legislative accountability that a bill of this constitutional significance demands.

Matthew Trenholm

Matthew Trenholm, MSc, is a co-founder of the Bearing Institute and a published researcher in the Journal of International Health Sciences and Management. He has worked in Canada's busiest emergency room for twenty years.

Bearing Institute is a Canadian public-policy institute focused on legislative research and ready-to-table amendments. We would welcome the opportunity to present this analysis during committee hearings or Senate consideration of Bill C-22, and are available to provide further analysis on request.

BearingInstitute.ca