New Search Powers in Bill C-2 (the Strong Borders Act)

Are They Constitutional?

Robert Diab, Faculty of Law, Thompson Rivers University | www.robertdiab.ca

rdiab@tru.ca

Bill C-2 Backgrounder: New Search Powers in the Strong Borders Act and Their Charter Compliance

Forthcoming in Criminal Law Quarterly, Vol 73(3) 2025

23 Pages • Posted: 24 Jul 2025 • Last revised: 1 Sep 2025

Robert Diab

Thompson Rivers University - Faculty of Law

Date Written: July 23, 2025

Abstract

Bill C-2, tabled in June of 2025, will bring about the most significant expansion of investigative search powers in Canada in over a decade, along with a long sought after lawful access regime for compelling assistance from electronic service providers. This article provides a concise overview of these powers, places them in context by noting how they expand or amend existing authority, and comments on their constitutional validity. Powers in bill C-2 are canvassed here in three groups: those relating cross-border traffic, domestic investigations, and technical assistance with access to data.

Google:

Diab backgrounder ssrn

Bill C-2

Expanding Search Powers and Charter Compliance

- Tabled in June 2025,
- Most **significant expansion of investigative search powers in Canada in over a decade**.
- It introduces a long-sought **lawful access regime** for compelling assistance from electronic service providers.
- engage a host of *Charter* rights; my focus section 8.

Section 8

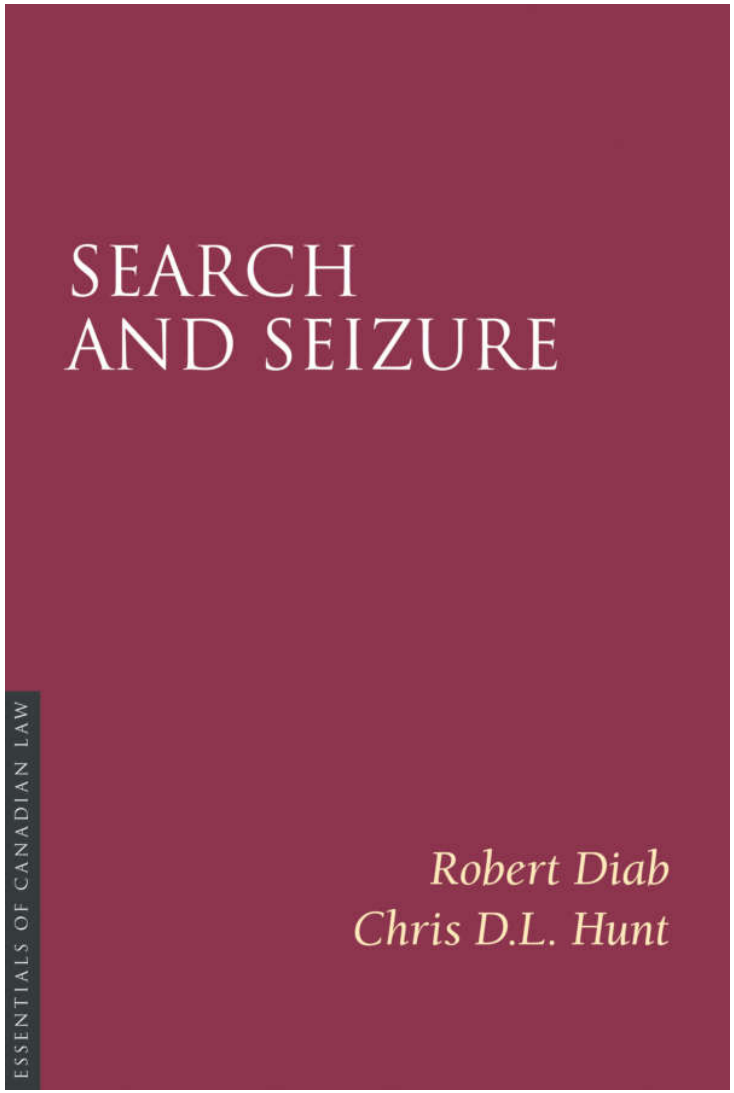
Basic coordinates

- **“Every one has the right to be secure against unreasonable search or seizure”**
- A search is considered reasonable if it is **authorized by a reasonable law and carried out reasonably**.
- What is a search/seizure (for the purposes of s 8)?
  - Something done by a state agent, acting for an investigative purpose, that interferes with REP a person has over a place or thing.

A ‘Reasonable Law’ Under Section 8

Balancing Law Enforcement and Privacy Interests

- ‘**Law is reasonable**’: does it strike **right balance** between law enforcement and privacy interests?
- The Supreme Court of Canada considers **four factors** in this assessment:
  - Whether the power relates to a criminal or regulatory offence.
  - The state or laws enforcement interest at issue.
  - The impact on personal privacy.
  - The oversight and accountability safeguards.


SEARCH
AND SEIZURE
ESSENTIALS OF CANADIAN LAW
Robert Diab
Chris D.L. Hunt

Part 1

Powers Related to Cross-Border Traffic

Bill C-2

Border Enforcement and Information Sharing

Amending various statutes

- Initial portions of C-2 changes relating to:
  - Customs and immigration enforcement.
  - Coastal patrol.
  - Canada Post.
  - Financial crimes.
  - Sex offender registry.

Information sharing amendments

IRPA, Oceans Act, PCMLTFA

- *IRPA* powers to **share info** about visa/citizenship status with prov/fed agencies for law enforcement (addresses, reasons for refusal)
- *Oceans Act*: expands the **coast guard**'s mandate to include "security patrols" and the "collection, analysis and disclosure of information or intelligence".
- *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*: obliges FINTRAC to **disclose information** to the Commissioner of Canada Elections based on "reasonable suspicion" of relevance to an election offense investigation
- Authority to disclose is not a power to search/seize

Customs Act Amendments

Expanded CBSA Inspection Powers

- Compels **warehouse operators and transporters** to provide “free access” to goods stored and to “open any package or container” without grounds.
- While “goods” can include data on devices, new provisions **apply to “goods destined for export... loaded... or stored**,” thus not devices a person carries upon departure.
- Probably reasonable: lower EP at border + high state interest (*R v Simmons*, SCC 1988)

Canada Post Corporation Act Amendments

Expanded Search and Seizure of Mail

- Bill amends the *CPCA* to allow for the search and seizure of mail under any Act of Parliament, including *Criminal Code* powers.
- Expands the corporation's power to **open letter mail on "reasonable suspicion" of "non-mailable matter"**. (Before this: only non-letter mail.)
- Raises questions about whether expanding warrantless search on "reasonable suspicion" to letter mail, (higher EP) strikes reasonable balance.

Sex Offender Information Registion Act Amendments

Lowered Thresholds and New Collection Powers

- C-2 **lowers the threshold** for police to **share information** with foreign and domestic agencies **from "necessary" to "reasonable grounds to believe it would assist"** in investigating or preventing sex offences.
- Info collection powers clarified to include recording "any tattoos or distinguishing marks".
- CBSA agents permitted to **disclose more specific travel details** and consult the SOIRA database.
- New info collection powers **not likely to offend section 8** (given SCC's holdings in *Rodgers* on DNA collection from offenders not engaging high EP).

Criminal Detection Powers under the PCMLTFA

Banks as Agents of Investigation

- C-2 amends the PCMLTFA to **allow banks** and other institutions to "**collect** an individual's **personal information** without the individual's knowledge or consent" **if police disclose** it to them.
- Banks **can then use info "for the purpose of detecting** or deterring a contravention of the laws of Canada" related to **money laundering, terrorist activity financing, or sanctions evasion**.
- **Potential section 8 violation**: bank as agent of the police? Taking investigative steps that intrude on privacy — without oversight or a reasonable standard = unreasonable search.

Part 2

Domestic Investigative Powers

Bill C-2

Criminal Code and CSIS Act

New Tools for Law Enforcement in Canada

- New ‘information demand’ and production order powers.
- Amendments to computer search warrants, exigent search provisions, foreign entity requests, and mutual legal assistance.
- New declaratory and indemnification provisions.

Computer Searches (Criminal Code)

Enhanced Warrant Powers for Digital Data

- New provisions allow for **warrants** to search “computer data” on a “computer system” already “in the possession of” police on reasonable grounds.
- Judges can now impose limits on data examination here to a “stipulated class of data,” done by **dedicated officer**.
- person conducting data extraction **not to share out-of-scope info** with other investigating officers.
- formalizes safeguards that judges could previously implement, potentially enhancing privacy protection for data within police-held computers.

Code: ‘Information Demand’ Power

Low Threshold for Private Information Requests

- new ‘information demand’ power allows police to make a written demand to service providers whether they provided services to a target/account/sub ID and if they hold “transmission data”—and if so where and when.
- can be as little as 24h to respond.
- “reasonable grounds to suspect” that a federal offence has been or will be committed, and the information “will assist in the investigation”.
- confidentiality conditions and a short five-day window for judicial review.

Information demand

487.0121 (1) A peace officer or public officer may make a demand in Form 5.0011 to a person who provides services to the public requiring the person to provide, in the form, manner and time specified in the demand, the following information:

(a) whether the person provides or has provided services to any subscriber or client, or to any account or identifier, specified in the form;

(b) if the person provides or has provided services to that subscriber, client, account or identifier,

(i) whether the person possesses or controls any information, including transmission data, in relation to that subscriber, client, account or identifier,

(ii) in the case of services provided in Canada, the province and municipality in which they are or were provided, and

(iii) in the case of services provided outside Canada, the country and municipality in which they are or were provided;

(c) if the person provides services to that subscriber, client, account or identifier, the date on which the person began providing the services;

(d) if the person provided services to that subscriber, client, account or identifier but no longer does so, the period during which the person provided the services;

(e) the name or identifier, if known, of any other person who provides services to the public and who provides or has provided services to that subscriber, client, account or identifier and any other information, if known, referred to in any of paragraphs (b) to (d) in relation to that other person and that subscriber, client, account or identifier; and

(f) if the person is unable to provide any information referred to in paragraphs (a) to (e), a statement to that effect.

Conditions for making demand

(2) The peace officer or public officer may make the demand only if they have reasonable grounds to suspect that

(a) an offence has been or will be committed under this Act or any other Act of Parliament; and

(b) the information that is demanded will assist in the investigation of the offence.

CSIS Act: Information Demand Power

Expanded Authority for Intelligence Agencies

- similar ‘information demand’ added to the *Canadian Security Intelligence Service Act*.
- CSIS agents can make an ‘information demand’ without grounds.
- CSIS can only make the demand “[f]or the purpose of performing its duties and functions under section 12 or 16,” which relate to threats to national security or foreign intelligence investigations.
- may not targeting Canadian citizens/permanent residents.

Code: Production Order for Subscriber Information

Broadening Access to User Data

- new production order specifically for “all subscriber information” attaching to an account for services, obtainable on “reasonable suspicion”.
- The bill adds an expansive definition of "subscriber information" to *Code*, including types of services, devices used, and billing information.
- *R v Spencer* affirmed high privacy interest in subscriber info: “reasonable suspicion” standard too low?
- A shortened five-day time limit for recipients to seek judicial review of production orders raises concerns about effective safeguards.

(2) Section 487.011 of the Act is amended by adding the following in alphabetical order:

subscriber information means, in relation to any client of a person who provides services to the public or any subscriber to the services of such a person,

(a) information that the subscriber or client provided to the person in order to receive the services, including their name, pseudonym, address, telephone number and email address;

(b) identifiers assigned to the subscriber or client by the person, including account numbers; and

(c) information relating to the services provided to the subscriber or client, including

(i) the types of services provided,

(ii) the period during which the services were provided, and

(iii) information that identifies the devices, equipment or things used by the subscriber or client in relation to the services. (*renseignements relatifs à l'abonné*)

Request of a Foreign Entity

Extraterritorial Reach for Digital Evidence

- C-2 adds a new section allowing a peace or public officer to **ask a judge** to authorize them to make a “**request to a foreign entity** that provides telecommunication services" to produce documents with transmission data or subscriber information.”
- officer must establish “reasonable suspicion” that a federal offence has been or will be committed and the evidence will assist the investigation.
- addresses concerns about police jurisdiction to demand information from foreign entities, framing it as a “request” to finesse issues of comity and respect for foreign sovereignty.

Declaratory and Indemnity Provisions

Uncertainty Regarding Voluntary Disclosure

- New declaratory provisions assert that police do not need authority to “receive any information... and to act” on it, if a person volunteers it without being asked.
- *R v Spencer* rejected similar declaratory provisions as sufficient authority for police to request private information, holding that asking for private information constitutes a search and requires lawful authority.
- bill also amends indemnity provisions to shield persons/companies from liability for voluntarily disclosing “information” police ask for (even if otherwise prohibited by privacy laws like PIPEDA), potentially reducing incentive for providers to insist on formal demands.
- If police request information that engages a reasonable privacy interest without lawful authority, it could still lead to the exclusion of evidence.

For greater certainty

487.0195 (1) For greater certainty, no preservation demand, preservation order, keep account open or active order or production order is necessary for a peace officer or public officer to ask a person to voluntarily preserve data that the person is not prohibited by law from preserving, to voluntarily keep an account open or active that the person is not prohibited by law from keeping open or active or to voluntarily provide a document to the officer that the person is not prohibited by law from disclosing.

No civil or criminal liability

(2) A person who preserves data, keeps an account open or active or provides a document in those circumstances does not incur any criminal or civil liability for doing so.

2014, c. 31, s. 20; 2024, c. 17, s. 362.

164 Subsection 487.0195(2) of the Act is replaced by the following:

Request for information

(1.1) For greater certainty, no information demand made under section 487.0121 is necessary for a peace officer or public officer to ask a person to voluntarily provide any information referred to in paragraphs 487.0121(1)(a) to (f) if the person is lawfully in possession of the information.

No civil or criminal liability

(2) A person who preserves data, keeps an account open or active or provides a document in the circumstances referred to in subsections (1) or who provides information in the circumstances referred to in subsections (1.1) does not incur any criminal or civil liability for doing so.

Voluntary or compelled provision of information

(3) For greater certainty, no production order or warrant, or information demand made under section 487.0121, is necessary for a peace officer or public officer to receive any information from a person who is lawfully in possession of it and to act on the information if the person provides it voluntarily or is required by law, including a law of a foreign state, to provide it.

Publicly available information

(4) For greater certainty, no production order or warrant, or information demand made under section 487.0121, is necessary for a peace officer or public officer to receive, obtain and act on any information that is available to the public.

‘Must the Police Refuse to Look?’ Resolving the Emerging Conflict in Search and Seizure Over Civilian Disclosure of Digital Evidence

(2023) 68:4 McGill Law Journal

42 Pages • Posted: 9 Nov 2023 • Last revised: 19 Apr 2024

Robert Diab

Thompson Rivers University - Faculty of Law

Date Written: November 5, 2023

Abstract

Courts in Canada are dealing more frequently with an old problem in a new guise: civilians bringing police digital evidence that engages a suspect’s privacy interest (text messages, email). Do police carry out a seizure when they receive it or a search when they proceed to review it, even briefly? Should police ‘refuse to look’ before obtaining a warrant or other authorization? If so, why? What measure of protection would calling this a search or seizure under section 8 of the Charter afford Canadians? The Supreme Court of Canada has yet to decide these issues directly, and trial, appeal courts, and commentators have offered widely diverging responses to the questions they raise. In doing so, courts and commentators alike have lost sight of the Supreme Court’s principled approach to what constitutes a search or seizure and when it will be reasonable. Applying this approach in R v Marakah, McLachlin CJ in obiter held that receiving a text exchange from a third party would require police to obtain a warrant before reading it, but she provided no rationale. This article articulates the Court’s principled approach and shows why diverging approaches among recent courts and commentators are not compelling. More crucially, given how central digital communication has become to all of us, the article sets out a rationale for insisting on a warrant before police review texts or photos, and what is at stake in failing to provide this vital safeguard.

Exigent Circumstances & Mutual Legal Assistance

Warrantless Seizures and International Cooperation

- **Exigent Circumstances**: C-2 amends the *Code* to explicitly allow for the seizure of subscriber information, transmission, or tracking data without a production order in exigent circumstances.
  - codifies power police already had at common law and is likely to be found reasonable.
- ***Mutual Legal Assistance in Criminal Matters Act*** (MLACMA): adds provisions for a more expeditious process for **enforcing foreign production orders** for subscriber information and transmission data, fulfilling international agreement mandates.
  - Minister of Justice is obliged to “make arrangements for the enforcement” if the tests for those orders in the *Code* are met.

Part 3

Supporting Authorized Access to Information Act

Bill C-2

Supporting Authorized Access to Information Act (SAAIA)

Compelling Electronic Service Provider Assistance

- Part 15 of C-2 introduces new statute: SAAIA, will apply to “electronic service providers” (ESPs): anyone who ‘provides services to persons in Canada’ (defined: creation/storage/transmission of info)
- purpose is to compel ESPs to **make technical modifications** to equipment to **provide police and CSIS** personnel with immediate **access to private data**.
- Act modeled after legislation in other Five-Eye nations (Britain, Australia, NZ).
- Act’s scope is broad but police/CSIS must be have authorization (e.g., warrants, requisite grounds, exigent circumstances).

Compelling Assistance and Charter Concerns

Technical Modifications, Secrecy, and Sweeping Powers

- The Minister can compel ESPs, including “core providers,” to implement technical capabilities or install/maintain/test devices to enable authorized persons to access information. (CPs ongoing)
- Factors for assessing conditions imposed against ESPs, but not CPs.
- While the Act aims to ban compelling actions that introduce a “systematic vulnerability,” Minister has the power to define this term, which critics argue could effectively allow for backdoors to encryption.

Core providers — obligations

(2) The Governor in Council may make regulations respecting the obligations of core providers, including regulations respecting

(a) the development, implementation, assessment, testing and maintenance of operational and technical capabilities, including capabilities related to extracting and organizing information that is authorized to be accessed and to providing access to such information to authorized persons;

(b) the installation, use, operation, management, assessment, testing and maintenance of any device, equipment or other thing that may enable an authorized person to access information; and

(c) notices to be given to the Minister or other persons, including with respect to any capability referred to in paragraph (a) and any device, equipment or other thing referred to in paragraph (b).

Systemic vulnerability

(3) A core provider is not required to comply with a provision of a regulation made under subsection (2), with respect to an electronic service, if compliance with that provision would require the provider to introduce a systemic vulnerability in electronic protections related to that service or prevent the provider from rectifying such a vulnerability.

Compelling Assistance and Charter Concerns

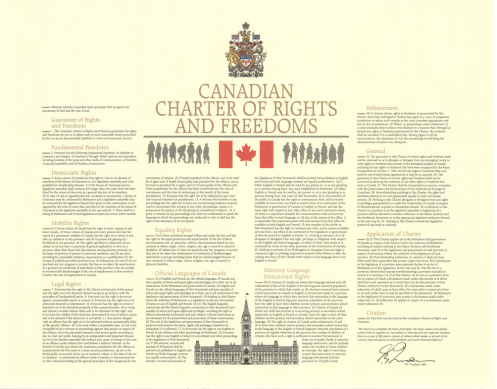
Technical Modifications, Secrecy, and Sweeping Powers

- Confidentiality provisions prohibit ESPs from disclosing orders or related information, potentially impeding accountability for inadvertent/unreasonable searches conducted by police or CSIS.
- Act grants sweeping search powers to “designated persons” for compliance inspections,
    - Including: allowing examination and copying of anything, including documents or electronic data, with minimal safeguards, raising doubts about section 8 reasonableness.

Conclusion & Key Takeaways

Balancing Security and Privacy in the Digital Age

- significant expansion of investigative powers across various domains, from border security to digital data access.
- Key areas of Charter concern include:
  - The low “reasonable suspicion” threshold for the new ‘information demand’ power and production orders for subscriber information.
  - The broad powers granted under the SAAIA, especially regarding confidentiality and inspection powers.
  - The potential for banks and other entities to act as police agents in criminal detection, conducting searches without adequate safeguards.


CANADIAN CHARTER OF RIGHTS AND FREEDOMS

First Session, Forty-fifth Parliament,
3 Charles III, 2025

HOUSE OF COMMONS OF CANADA

BILL C-2

to the security of the border between Canada and the security measures

FIRST READING, JUNE 3, 2025

MINISTER OF PUBLIC SAFETY