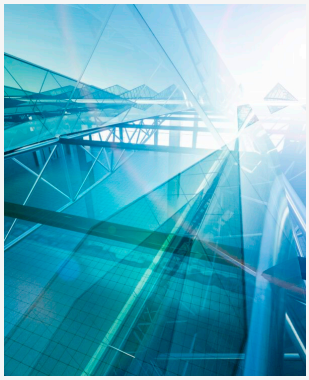
OSLER

Beyond borders: government grants itself powerful access to data, reduced oversight

JUNE 19, 2025 6 MIN READ



Related Expertise

- Artificial Intelligence
- Disputes
- Privacy and Data Management
- Regulatory
- Retail and Consumer Products
- Risk Management and Crisis Response
- Technology

Authors: Michael Fekete, John Salloum, Christopher Naudie, Lipi Mishra

Canada's proposed Bill C-2 (or the *Strong Borders Act*) will overhaul key aspects of Canada's lawful access regime; namely, the circumstances in which law enforcement and governmental agencies can both compel the production of information and other data and impose related gag orders. These changes will have far-reaching implications for both businesses operating in Canada and civil liberties.

The lawful access provisions within Bill C-2, introduced June 3, 2025, create "information demands" and orders that can be issued to *any* provider of services to the public (including telecommunication companies, banks, hotels, rental car companies, streaming services and other online platforms) and — despite the title of the Act — the exercise of these powers is not limited to matters of border security or illegal drugs.

Key changes include the following:

- Warrantless information demands for customer information. Law enforcement and a wide range of governmental agencies (e.g., Competition Bureau, Health Canada, Office of the Superintendent of Financial Institutions, etc.) will be authorized to issue an information demand (without a warrant or judicial order) that requires a provider of services to the public to confirm whether it or another business provides or has provided services to a specified subscriber, client, account, or identifier, including when those services were provided, the location of the services, and whether the provider possesses related information.
- Production orders for subscriber information:. Law enforcement and governmental agencies will be authorized to seek production orders from the court covering a broad range of subscriber information, including pseudonyms, contact information, IP addresses and device information, if it has "*reasonable grounds to suspect*" that any federal offence has been or will be committed. If exigent circumstances exist, production of subscriber information, transmission data, or tracking data can be compelled without any judicial order.
- Cross-border data sharing: The Bill will help enable cross-border data sharing, both by

permitting law enforcement in Canada to seek a judicially sanctioned request to a foreign provider of telecom services to provide subscriber information, or transmission data under a "*reasonable grounds to suspect*" standard. As well, it will amend the *Mutual Legal Assistance in Criminal Matters Act* to facilitate enforcement in Canada of foreign requests for subscriber information or transmission data.

- Access to information processed by electronic service providers: The Bill includes a new statute — the *Supporting Authorized Access to Information Act*— that will authorize the Minister of Public Safety and Emergency Preparedness to make regulations or issue orders compelling electronic service providers to, among other things, develop or install devices, and test and maintain equipment that will enable law enforcement access to, and the ability to extract information from, the provider's service.

Why the changes are significant

Charter of Rights and Freedoms

Bill C-2 represents the federal government's latest attempt to enhance the ability of law enforcement to gain warrantless access to subscriber information. Prior bills proved to be controversial, in part because of concerns about civil liberties, possible violations of the *Charter of Rights and Freedoms*, and the impingement on the quasi-constitutional privacy rights of Canadians.

The Supreme Court of Canada has previously ruled that there is a reasonable expectation of privacy in Internet subscriber information, including in a user's IP address, thereby triggering protections from warrantless demands for information under Section 8 of the Charter. While Bill C-2 does not contemplate warrantless access to *all* categories of subscriber information, it does authorize warrantless demands to information that will enable law enforcement to seek production orders covering broader categories of subscriber information based on a new standard that only requires "reasonable grounds to *suspect*" that any federal offence has been or will be committed.

It is expected that this element of the Bill will be tested in court. A Charter challenge is likely to highlight how a warrantless demand for information about a subscriber can be made in the context of an investigation of any offence (rather than only more serious criminal offences or national security matter) and can be issued to the provider of *any* service to the public (rather than only providers of telecommunications or Internet services). As well, a Charter challenge is likely to focus on how the threshold of warrantless access is set at the lowest level (reasonable grounds to suspect), rather than at a level more protective of individual rights (reasonable grounds to believe).

Backdoor access to information

Providers of telecommunications, cloud and other electronic services typically deploy access controls, cryptography and similar safeguards to protect a user's information from unauthorized access. The *Supporting Authorized Access to Information Act* may be viewed as upending these protections and, more broadly, treating service providers as an extension of law enforcement or governmental agencies. This perspective may arise if, for example, service providers are required by the Minister to enable backdoor access to, or the interception of, information processed within messaging or cloud services.

While Bill C-2 does contemplate an exception for "systemic vulnerabilities," the definition of the term has been left to the regulations.

New challenges for businesses

If enacted, Bill C-2 may impact the operations of any business that provides services to the public, rather than only providers of telecom or online services. Moreover, we expect law enforcement and governmental agencies will issue information demands for subscriber information as a common investigative technique when the identity of a suspect or potential witness is unknown. This likely will lead to a significant increase in the number of production orders, given the enhanced ability to identify previously anonymous individuals. The low legal threshold for production orders covering subscriber information (reasonable grounds to suspect) is similarly anticipated to result in an increased number of orders being issued.

In addition to responding to a surge in volume of lawful access demands for information, businesses will need to operationalize by responding to some demands *in as little as 24 hours* and by seeking to challenge production orders in court within only five days of receipt.

While it will not be possible to fully assess the impact of the *Supporting Authorized Access to Information Act* until regulations are issued, it is clear Bill C-2 can be used to compel electronic service providers to take potentially intrusive and costly steps to enable access to and extraction of information from their platforms.

Next steps

The new federal government has placed a priority on advancing the Bill, but it is expected the lawful access provisions in Bill C-2 will be the subject of meaningful debate within Parliament, as well as detailed review at committee. While it is premature to speculate on whether the government will be open to amendments, there is no question that stakeholders will be carefully considering the implications of the Bill and what changes may be warranted.

Please also see the Osler Update on Bill C-2's proposed money laundering-related changes.