LIBRARY OF PARLIAMENT
BIBLIOTHÈQUE DU PARLEMENT

PRELIMINARY VERSION

UNEDITED

This legislative summary is available as an unedited preliminary version in PDF format only.

If the bill receives Royal Assent, this version will be replaced by a final version available in both HTML and PDF formats.

Legislative Summary

BILL C-22: AN ACT RESPECTING LAWFUL ACCESS

45-1-C22-E

7 October 2026

Revised by Sabrina Charland and Anne-Marie Therrien-Tremblay

Library and Research Services

PRELIMINARY VERSION
UNEDITED

AUTHORSHIP

7 October 2026	Sabrina Charland and Anne-Marie Therrien-Tremblay
17 March 2026	Joey Arseneault-Watters, Sabrina Charland, Alexsandra Ferland and Anne-Marie Therrien-Tremblay

ABOUT THIS PUBLICATION

Library of Parliament legislative summaries summarize bills currently before Parliament and provide background information about them in an objective and impartial manner. They are prepared by Library and Research Services, which carries out research for and provides information and analysis to parliamentarians, Senate and House of Commons committees and parliamentary associations. Legislative summaries are revised as needed to reflect amendments made to bills as they move through the legislative process.

For clarity of exposition, the legislative proposals set out in the bill described in this legislative summary are stated as if they had already been adopted or were in force. It is important to note, however, that bills may be amended during their consideration by the Senate and House of Commons and have no force or effect unless and until they are passed by both houses of Parliament, receive Royal Assent and come into force.

Any substantive changes to this Library of Parliament legislative summary that have been made since the preceding issue are indicated in **bold print**.

© Library of Parliament, Ottawa, Canada, 2026

Legislative Summary of Bill C-22
(Preliminary version)

45-1-C22-E

Ce document est également publié en français.

PRELIMINARY VERSION
UNEDITED

CONTENTS

1 BACKGROUND 1

2 DESCRIPTION AND ANALYSIS 3

2.1 Part 1: Timely Access to Data and Information (Clauses 2 to 40 of Bill C-22) 3
2.1.1 Examination of Computer Data Seized Under Warrant 3
2.1.2 Subscriber Information 4
2.1.3 Confirmation of Service Demand 5
2.1.4 Subscriber Information Production Order 6
2.1.5 International Production Request 7
2.1.6 Exigent Circumstances 8
2.1.7 *Mutual Legal Assistance in Criminal Matters Act* 9
2.1.8 *Controlled Drugs and Substances Act* and *Cannabis Act* 10
2.1.9 Coming into Force 10

2.2 Part 2: Supporting Authorized Access to Information Act (Clauses 41 to 47 of Bill C-22) 10
2.2.1 Obligations of Core Providers – Regulations 11
2.2.2 Obligations – Ministerial Orders 12
2.2.3 Obligation to Assist and Confidentiality 13
2.2.4 Administration and Enforcement 14
2.2.5 Administrative Monetary Penalties and Offences 15
2.2.6 Regulations 16
2.2.7 Annual Report 17

2.3 Part 3: Parliamentary Review (Section 48 of Bill C-22) 17
2.3.1 Parliamentary Review 17

PRELIMINARY VERSION
UNEDITED

LEGISLATIVE SUMMARY OF BILL C-22: AN ACT RESPECTING LAWFUL ACCESS

1 BACKGROUND

On 12 March 2026, the Honourable Gary Anandasangaree, Minister of Public Safety and Emergency Preparedness (Minister of Public Safety), introduced Bill C-22, An Act respecting lawful access (short title: Lawful Access Act, 2026).[1]

The House of Commons Standing Committee on Public Safety and National Security proposed 29 amendments to the bill during its study, which ended on 17 June 2026.[2] The House of Commons then passed the bill on division at report stage and at third reading on 18 June 2026, without any additional amendments.

Changes resulting from the amendments that were adopted are identified in bold print in this document.

According to the Government of Canada, lawful access refers to the ability of law enforcement, security and intelligence agencies "to lawfully obtain certain information or intercept communications."[3] Lawful access is governed by privacy laws and the *Canadian Charter of Rights and Freedoms* (the Charter), including the right to protection against unreasonable search and seizure. The Government of Canada identifies two aspects of lawful access:

- the legal authorities of law enforcement agencies and the Canadian Security Intelligence Service (CSIS) to obtain information and data, as set out in the *Criminal Code* and the *Canadian Security Intelligence Service Act* (CSIS Act);[4] and
- the technical abilities of electronic service providers (ESPs) to provide law enforcement agencies and CSIS with the information they are legally authorized to obtain under these authorities.[5]

Part 1 of Bill C-22 addresses the first aspect of lawful access mentioned above. Specifically, the provisions of this part facilitate access by law enforcement agencies and CSIS to information about a subscriber to a telecommunications service.

Part 2 of the bill addresses the second aspect of lawful access mentioned above. The provisions of this part enact An Act respecting the obligations of electronic service providers in relation to authorized access to information (short title: Supporting Authorized Access to Information Act (SAAIA)). Under the SAAIA, ESPs could be required to develop and maintain the technical capabilities necessary to facilitate access to information in their possession by a person legally authorized to access it in

the context of criminal investigations or intelligence matters. According to the Government of Canada,

> Canada is the only country amongst its Five Eyes partners [an alliance of the intelligence services of Australia, Canada, New Zealand, the United Kingdom, and the United States (U.S.)], the G7, and across the European Union without legislation requiring ESPs to develop and maintain lawful access capabilities.[6]

Canada signed the Council of Europe's *Convention on Cybercrime* (Budapest Convention) in 2001 and ratified it in 2015.[7] In 2023, Canada signed the *Second Additional Protocol to the Convention on Cybercrime* on enhanced cooperation and disclosure of electronic evidence.[8] This protocol provides a legal framework in criminal matters to enable the disclosure of electronic evidence by ESPs to a foreign country and to strengthen direct cooperation between countries and foreign ESPs. At this time, Canada has not ratified the protocol. Canada is therefore not legally bound by the procedures set out in the Protocol.

In 2018, the U.S. enacted the *Clarifying Lawful Overseas Use of Data Act* (CLOUD Act).[9] This law requires an ESP operating in the United States to disclose user data directly to a foreign country for the purposes of a criminal investigation.[10] The enforcement of the law is contingent upon the conclusion of reciprocal bilateral agreements between the U.S. and foreign countries. Since 2022, the U.S. and Canada have been negotiating a bilateral agreement regarding this law.[11] To date, the U.S. has reached an agreement with Australia and the United Kingdom.[12]

Bill C-22 essentially incorporates parts 14 and 15 of Bill C-2, An Act respecting certain measures relating to the security of the border between Canada and the United States and respecting other related security measures (short title: Strong Borders Act), which was introduced on 3 June 2025 by the Minister of Public Safety.[13] However, certain provisions of Bill C-22 differ from those in parts 14 and 15 of Bill C-2. Notably, Part 1 provides for a narrower scope of application for requests for information without judicial authorization. Furthermore, Part 2 proposes different provisions for ministerial orders concerning ESPs by requiring the approval of the Intelligence Commissioner and removing the consultation requirement with the Minister of Industry; it also specifies inspection powers, obligation to assist, privacy, and cybersecurity considerations.[14] Furthermore, unlike Bill C-2, Bill C-22 provides in Part 3 for a parliamentary review of the bill three years after its coming into force.

With the exception of parts 4, 14 and 15, most of the measures contained in Bill C-2 were subsequently incorporated into Bill C-12, An Act respecting certain measures relating to the security of Canada's borders and the integrity of the Canadian immigration system and respecting other related security measures, which has since been passed by Parliament and was assented to in March 2026.

PRELIMINARY VERSION
UNEDITED

In recent years, Parliament has passed legislation regarding lawful access. In particular, the *Protecting Canadians from Online Crime Act*,[15] passed in 2014, allows law enforcement agencies to order or obtain a court order for the preservation of electronic evidence and establishes new court orders to obtain data relating to the transmission of communications or data used to locate an object or a person. Although the *National Security Act, 2017*,[16] enacted in 2019, did not directly address access, it, among other things, reformed the information-sharing regime and the rules governing the collection and use of national security datasets.

2 DESCRIPTION AND ANALYSIS

Bill C-22 consists of 48 clauses divided into three parts. Part 1 makes changes to several laws, Part 2 introduces the SAAIA, and Part 3 provides for a parliamentary review of Part 1 and Part 2. This legislative summary discusses the bill's main provisions without examining each clause.

2.1 PART 1: TIMELY ACCESS TO DATA AND INFORMATION (CLAUSES 2 TO 40 OF BILL C-22)

Part 1 of Bill C-22 amends several Canadian laws, including the *Criminal Code* and the CSIS Act, with respect to the collection of information and the lawful access powers of law enforcement and CSIS. While the main elements of Part 14 of Bill C-2 are also contained in Bill C-22, the scope of certain provisions in Bill C-22 is different.

According to the Government of Canada – with the goal of responding to the Supreme Court of Canada's (SCC) decisions in *R. v. Spencer* (2014) and *R. v. Bykovets* (2024), which held that obtaining basic information requires lawful authority – Part 1 of Bill C-22 provides law enforcement with two "new investigative tools."[17] Those tools are (i) the "confirmation of service demand," which Bill C-22 makes available to law enforcement through amendments to the *Criminal Code* and to CSIS through the CSIS Act, as well as (ii) the "subscriber information production order." In addition to creating these tools, Bill C-22 amends the *Criminal Code* to provide for the examination of computer data seized under warrant, establishes a mechanism to request the production of information from a foreign entity, and sets rules for the warrantless seizure of digital information under exigent circumstances.

2.1.1 Examination of Computer Data Seized Under Warrant

To examine computer data, law enforcement can apply for a search warrant under current section 487 of the *Criminal Code*, which authorizes entry on to private premises and seizure of property. In *R. v. Vu* (2013),[18] the SCC ruled that police must obtain specific judicial authorization to search a computer, even if they already

PRELIMINARY VERSION
UNEDITED

hold a valid warrant to search premises. In practice, this often involves two steps, and potentially two warrants.

Clause 3 of Bill C-22 amends section 487 of the *Criminal Code* to allow a judge to authorize, by issuing a search warrant, the examination of computer data seized under the warrant, or contained in a computer seized under the warrant (new section 487(2.3)). It also allows a judge to issue a warrant for examination of data contained in a computer that is already in the possession of law enforcement (new section 487(2.4)). In both cases, the judge must be satisfied that there are reasonable grounds to believe[19] that the computer data will provide evidence of an offence.

Bill C-22 establishes conditions for the examination of data under a warrant relating to computer data. Specifically, new section 487(2.5) provides that such examination may be subject to any conditions that a judge considers advisable to ensure the examination is reasonable. In contrast, Bill C-2 allows a judge to impose specific conditions, including, for example, that the examination be limited to a specified class of computer data, and that the extraction of such data be performed by someone who is not otherwise involved in the investigation.

2.1.2 Subscriber Information

Currently, the *Criminal Code* does not define the term "subscriber information." In *R. v. Spencer* in 2014, the SCC indicated that subscriber information includes the "name, address and telephone number of the customer using [an Internet Protocol (IP)] address."[20] In *R. v. Bykovets* in 2024, the SCC defined the term as "the name, address, and contact information – associated with an individual [IP] address."[21] In *R. v. Spencer*, the SCC established that a reasonable expectation of privacy is attached to subscriber information and that a request by law enforcement for this type of information constitutes a "search" under section 8 of the Charter, which protects against unreasonable search or seizure. The SCC arrived at the same conclusion with regard to IP addresses in *R. v. Bykovets*.

Clause 4 of Bill C-22 provides a definition of subscriber information that encompasses a broader range of information than the SCC's definition of that term. Bill C-22's definition includes the name, address, telephone number and email address of a client or subscriber to "a person who provides services to the public." As well, it comprises the subscriber's pseudonym, the "identifiers assigned" to the subscriber, such as an account number, and "information relating to the services provided to the subscriber," including the types of services provided, the duration of the subscription, and information that identify devices and equipment used by the subscriber.

Bill C-22 does not provide a definition of "a person who provides services to the public." It could be interpreted broadly as comprising anyone offering services to the

public and who may hold data relevant to police investigations. For example, it could include Internet service providers as well as third parties who provide services to clients with IP addresses, which could include social media platforms, e-commerce sites, cloud service providers, and other businesses.

2.1.3 Confirmation of Service Demand

Clause 5 of Bill C-22 amends the *Criminal Code* to provide law enforcement with the ability to demand that a telecommunications service provider confirm whether they provide or have provided telecommunication services to a specified subscriber, client, account, or identifier. Clause 31 of Bill C-22 makes amendments to the CSIS Act to enable CSIS to make such demands to telecommunications service providers.

Bill C-22 establishes conditions relating to the "confirmation of service demand." In clause 5 of Bill C-22, new section 487.0121(2) of the *Criminal Code* provides that a peace officer or public officer (peace officer) may make this demand "if they have reasonable grounds to suspect" that an offence has been committed or will be committed, and that the confirmation of service will assist in the investigation.[22] Clause 31 of Bill C-22 creates new section 20.22(1) of the CSIS Act to allow CSIS to make such a demand for the purpose of performing duties relating to "activities that may on reasonable grounds be suspected of constituting threats to the security of Canada" (section 12 of the CSIS Act) or for the collection of information concerning foreign states and persons (section 16 of the CSIS Act). **At committee stage, the House of Commons Standing Committee on Public Safety and National Security clarified that the confirmation of service demand deals with telecommunications services specifically, not any type of service in general.**

Unlike the "information demand" in Bill C-2 which can be made to any "person who provides services to the public," the "confirmation of service demand" in Bill C-22 is limited to telecommunications service providers. Bill C-22 amends both the *Criminal Code* and the CSIS Act to clarify that "telecommunication service provider" has the same meaning as in the *Telecommunications Act*.[23] As well, the information demand under Bill C-2 permits law enforcement and CSIS to demand a broader category of information than in Bill C-22, including whether services are provided, and whether specific information is held. By contrast, Bill C-22 allows law enforcement and CSIS to require telecommunications service providers only to confirm whether they are providing a service.

Moreover, Bill C-22 adds section 487.0121(3) to the *Criminal Code* and section 20.22(2) to the CSIS Act to clarify that a confirmation of service demand cannot be made if the confirmation discloses medical information or information that is subject to solicitor-client privilege, protections not found in Bill C-2's provisions relating to the information demand.

Under Bill C-22, new section 487.0121(5) of the *Criminal Code* and new section 20.22(3) of the CSIS Act indicate that the telecommunication service provider must have at least 24 hours to deliver the confirmation of service. As well, changes to the *Criminal Code* and the CSIS Act provide that the demand may include a non-disclosure condition. While amendments to the CSIS Act do not include further requirements relating to the use of a non-disclosure condition by CSIS, new section 487.0121(6) of the *Criminal Code* provides that the peace officer may impose such a condition for a period of up to one year, and "only if they have reasonable grounds to believe that the disclosure during that period would jeopardize the conduct of the investigation."

Bill C-22 adds sections 487.0121(8) to 487.0121(11) to the *Criminal Code* to provide for a review process, which allows telecommunication service providers to apply in writing to a judge to amend or revoke the confirmation of service demand. Bill C-22 also adds section 20.23 to the CSIS Act to establish a similar review process.

As well, new section 20.24 of the CSIS Act creates a process by which CSIS may make an application to a judge to order the telecommunication service provider to issue the confirmation. Clauses 32 to 34 of Bill C-22 amend the sections of the CSIS Act dedicated to the amendment or revocation of orders, specifically to address the amendment or revocation of confirmation of service demands and orders made under section 20.24, and to reflect other changes to the statute. Similar provisions are included in Bill C-2. **The House of Commons Standing Committee on Public Safety and National Security amended section 28(b.2) of the CSIS Act to clarify the regulatory power that applies to the new provisions. Rather than listing the various categories of applications for amendment or revocation that could be submitted regarding the new demands and orders, the provision now refers to applications submitted under sections 20.23 and 20.5.**

As well, Bill C-22 introduces new section 487.0121(11) of the *Criminal Code* and new section 20.25(1) of the CSIS Act to clarify that if a telecommunication service provider wants to voluntarily share a confirmation of service demand, additional authority such as a court order is not required. An equivalent provision is not included in Bill C-2. Clause 11 of Bill C-22 makes similar clarification for confirmations of service demand, as well as production orders and warrants, and confirms in new section 487.0195(4) of the *Criminal Code* that an order is not required for law enforcement to obtain information that is already available to the public. Similar provisions are included in clause 164 of Bill C-2.

2.1.4 Subscriber Information Production Order

Currently, law enforcement can obtain a general production order from the court to obtain subscriber information.[24] Clause 6 of Bill C-22 introduces production orders specifically for subscriber information under new section 487.0142 of the

PRELIMINARY VERSION
UNEDITED

Criminal Code. Such production order allows law enforcement to demand, by means of an *ex parte* application to a judge,[25] that a service provider produce a document **containing information about a subscriber. The House of Commons Standing Committee on Public Safety and National Security amended section 6 so that information that could be disclosed would be explicitly limited to the categories identified in the new definition of "subscriber information" set out in section 487.011 of the *Criminal Code*. Section 6, as amended at the committee stage, clarifies that the information requested must (1) be limited specifically to the information identified in the order, (2) relate to information that is specified in the order, and (3) be in the provider's possession or control when they receive the order.**

An oath must be made by the peace officer in Form 5.004 for the judge to grant the order if there are "reasonable grounds to suspect" that an offence had been or will be committed, and that the information will assist in the investigation. In comparison, the higher standard of "reasonable grounds to believe" is required for a judge to grant a general production order.

Subscriber information production orders established by clause 6 of Bill C-22 apply to any "person who provides services to the public," giving this tool a broader scope than the confirmation of service demands in clause 5 of the bill, which only applies to telecommunication service providers.

2.1.5 International Production Request

Clause 7 of Bill C-22 introduces new section 487.018 to the *Criminal Code* to allow law enforcement to make production requests to foreign telecommunications service providers. According to the Government of Canada, there is currently "no specific tool for Canadian law enforcement to ask foreign entities for subscriber information or transmission data that is held outside of Canada."[26]

Clause 7 of Bill C-22 allows a peace officer, by means of an *ex parte* application, to request that "a foreign entity that provides telecommunications services – or that provides services by a means of telecommunication – to the public" produce a document containing transmission data – as defined in section 487.011 of the *Criminal Code* – or subscriber information – as defined in clause 2 of Bill C-22. The judge may authorize the request if they are satisfied that there are "reasonable grounds to suspect" that an offence had been or will be committed, and that the information is in the foreign entity's possession and will assist in the investigation.

The provisions governing international production requests in Bill C-22 are similar in Bill C-2. However, in Bill C-2, the production request applies to "a foreign entity that

PRELIMINARY VERSION
UNEDITED

provides telecommunications services to the public" without including those providing services "by a means of telecommunication."

2.1.6 Exigent Circumstances

Currently a peace officer can conduct a search of a building, receptacle or place or use a tracking device (to track transactions or the movement of a thing) without a court order if an emergency – or exigent circumstances – make it impractical to obtain one.[27] Exigent circumstances include situations where the delay in obtaining a court order could lead to the loss of evidence or pose a threat to the safety of an individual. However, according to the Government of Canada, law enforcement does not currently "have a clear ability to seize digital information in emergency situations without court approval."[28]

Clause 14 of Bill C-22 amends section 487.11 of the *Criminal Code* to expand law enforcement's ability to conduct a search without a warrant in exigent circumstances, including to obtain location data of an individual through the use of a tracking device (section 492.1(2) of the *Criminal Code* on warrants for tracking data) and transmission data through the use of a transmission data recorder (section 492.2 of the *Criminal Code* on warrants for transmission data). Moreover, in exigent circumstances, new section 487.11(b) would authorize law enforcement to seize, without a court order:

- subscriber information, otherwise seized under Bill C-22's new provisions providing for subscriber information production orders (section 487.0142(1) of the *Criminal Code*);
- transmission data, otherwise obtained by an order made under section 487.016(1) of the *Criminal Code*; and
- tracking data, otherwise obtained by an order made under section 487.017(1) of the *Criminal Code*.

Clause 19 amends section 492.1 of the *Criminal Code* to broaden the scope of warrants for tracking data by authorizing peace officers to obtain tracking data relating to the location of a thing (not known at the time that the warrant is issued) that an individual uses, carries or wears (new section 492.1(2.1)).

Clause 20 also broadens the scope of section 492.2 of the *Criminal Code* to authorize peace officers to obtain transmission data that relates to means of telecommunication that are unknown at the time the warrant is issued. Bill C-22 adds section 492.2(2.1) to the *Criminal Code* to allow the judge to include any conditions that the judge "considers appropriate, including conditions to protect a person's interests" when issuing a warrant for transmission data. This provision is not included in Bill C-2.

PRELIMINARY VERSION
UNEDITED

The provisions on exigent circumstances in Bill C-22 are largely similar to those of Bill C-2.

2.1.7 *Mutual Legal Assistance in Criminal Matters Act*

Clause 29 of Bill C-22 makes amendments to the *Mutual Legal Assistance in Criminal Matters Act* (MLAA).[29] This statute provides for the implementation of treaties for mutual legal assistance in criminal matters and provides Canada with the legal authority to obtain court orders on behalf of countries that are party to these agreements. Requests for assistance made under the MLAA may relate to such matters as foreign investigations, arrest warrants, production orders, search and seizure, the transfer of detained persons and the forfeiture of assets between Canada and partner countries.

Bill C-22 adds new section 22.07 to the MLAA on "Enforcement of Foreign Decisions for Production." The new section authorizes Canadian authorities to enforce decisions from partner countries requiring the production of specific electronic data held in Canada; namely transmission data or subscriber information. New section 22.07(1) of the MLAA provides that the Minister of Justice may authorize a "competent authority" to enforce the decision when a request of assistance is received. The term "competent authority" is defined in the MLAA as "the Attorney General of Canada, the attorney general of a province or any person or authority with responsibility in Canada for the investigation or prosecution of offences."[30]

New section 22.07(2) of the MLAA outlines that the competent authority must first make an *ex parte* application for the enforcement of the decision to a judge. The conditions that must be met for the judge to make the decision enforceable depends on the type of information that is requested (new section 22.07(3) of the MLAA). For transmission data, the judge must be satisfied that the conditions for making a transmission data production order, under section 487.016(2) of the *Criminal Code*, are met.[31] For subscriber information, the judge must be satisfied that the conditions to make a subscriber information production order, set out in the new section 487.0142(2) of the *Criminal Code*, are met.

Amendments to the MLAA establish time limits for the production of records containing transmission data or subscriber information (section 22.07(5) of the MLAA) and allow the judge to request that the competent authority transmit the information directly to a designated person in the partner country (section 22.07(7)(a) of the MLAA), who must then transmit the information to the partner country within five days from the production of the records (section 22.07(9) of the MLAA). The amendments to the MLAA also contain reporting requirements.

As well, section 22.07(10) of the MLAA refers to a *Criminal Code* offence punishable on summary conviction should the production order be contravened. As such, should a production order be breached without lawful excuse, the guilty party may be liable to a fine of not more than $250,000 or to imprisonment for a term of not more than two years less a day, or to both.[32]

The provisions governing international production requests in Bill C-22 are the same as in Bill C-2.

2.1.8 *Controlled Drugs and Substances Act* and *Cannabis Act*

Clause 37 amends the *Controlled Drugs and Substances Act*[33] and clause 28 amends the *Cannabis Act*[34]. These amendments pertain to certain *Criminal Code* provisions related to computer data and other additions to the *Criminal Code*, more specifically those governing the handling of electronic evidence under search warrants.

2.1.9 Coming into Force

Part 1 of Bill C-22 comes into force 180 days after Royal Assent.

2.2 PART 2: SUPPORTING AUTHORIZED ACCESS TO INFORMATION ACT (CLAUSES 41 TO 47 OF BILL C-22)

Part 2 of Bill C-22 consists of six clauses. Clause 41 enacts the SAAIA. Clauses 42 to 46 provide for various related and consequential provisions, including amendments to the *Intelligence Commissioner Act*, while clause 47 provides that the coming into force of these provisions is to be fixed by order of the Governor in Council. Although Part 2 of Bill C-22 draws largely from Part 15 of Bill C-2, the Strong Borders Act, it introduces certain notable differences, particularly with respect to oversight, transparency and the regulatory framework.

According to the Government of Canada, the purpose of the SAAIA is to facilitate lawful access by authorized persons to information held by ESPs, including in the context of police investigations or intelligence operations (section 3 of the SAAIA). To that end, the SAAIA applies to ESPs, defined as any person that provides

PRELIMINARY VERSION
UNEDITED

electronic services – including for the purpose of enabling communications – either to persons in Canada or in the course of business activities carried on in whole or in part in Canada (section 2 of the SAAIA).

At committee stage, the House of Commons Standing Committee on Public Safety and National Security clarified that the SAAIA does not change the authority to access information already provided for in other existing federal laws and assistance agreements. A clarification on limits to the obligations that could be imposed on ESPs was also added. In particular, this stipulates that the SAAIA cannot require an ESP to decrypt information that was encrypted by a user or guarantee its decryption, unless the encryption was provided by the ESP and it has the technical means necessary to decrypt the information (sections 2(2) to 2(4) of the SAAIA).

The SAAIA establishes two mechanisms by which obligations may be imposed on ESPs: first, through designation as a core provider, which triggers regulatory obligations; or second, through the issuance of a ministerial order. The SAAIA also provides for general obligations of assistance and confidentiality applicable to ESPs, an inspection and oversight regime, as well as administrative monetary penalties and criminal offences in cases of non-compliance.

2.2.1 Obligations of Core Providers – Regulations

The Governor in Council may designate certain classes of ESPs as "core providers" by adding them to the schedule of the SAAIA (section 5(1) of the SAAIA), though no classes of providers are currently set out in the schedule.

Section 5(2) of the SAAIA allows the Governor in Council to make regulations respecting the obligations of core providers, including with respect to technical capabilities, equipment and notices to be given to the Minister of Public Safety. In contrast to Bill C-2, Bill C-22 adds to this list the ability to require the retention of categories of metadata, including transmission data, as defined in section 487.011 of the *Criminal Code*,[35] for a maximum period **of six months.**[36]

This includes, for example, technical information relating to the time, duration or routing of a communication, without revealing the content of the communication.

Bill C-22 also introduces, in section 5(3) of the SAAIA, an element not found in Bill C-2. This section requires the Governor in Council to take into account several factors when making a regulation under section 5(2) of the SAAIA, including the benefits of the regulation to the administration of justice and national security, the capacity of core providers to comply, the costs associated with compliance, the potential impact on users of the services, impacts on privacy and cybersecurity, as well as any other factor considered relevant.

Section 5(4) of the SAAIA similarly introduces an element not found in Bill C-2 by establishing specific restrictions on the scope of section 5(2)(d), notably to ensure that regulations cannot require core providers to retain information revealing the content of communications, a person's web browsing history or a person's social media activities**. In addition, the House of Commons Standing Committee on Public Safety and National Security added sections 5(4.1) and 5(6), which further limit the scope of this regulatory power by requiring that the categories of metadata covered be essential for the purpose of investigations or for intelligence. It also clarified that authority to access personal information cannot be prescribed by regulation.**

Lastly, section 5(5) of the SAAIA contains a provision similar to section 5(3) of Bill C-2, establishing that a core provider is not required to comply with a regulatory obligation if doing so would require the provider to introduce a systemic vulnerability or prevent the provider from rectifying such a vulnerability in the electronic protections of the service. Moreover, Bill C-22 includes an explicit definition of "systemic vulnerability," meaning a vulnerability in the electronic protections of an electronic service **that**, **according to recognized international technical standards, creates a credible risk of unauthorized access to secure information.**[37]

Section 6 of the SAAIA allows a core provider to apply for a temporary exemption from certain regulatory obligations. The Minister of Public Safety may grant such an exemption, subject to terms and for a specified period, if the application is justified and contains the required information. The obligation does not apply during the review of the application. In the event of a denial, the minister may specify the day by which the provider must comply with the obligation. **Section 6 was amended at committee stage to allow the Minister to impose conditions regarding the disclosure of the existence or content of a temporary exemption and requiring that it render its decision within 90 days after an application is submitted, unless there is an agreement otherwise with the core provider.**

2.2.2 Obligations – Ministerial Orders

Section 7(1) of the SAAIA authorizes the Minister of Public Safety to impose, by order, any obligation that may be prescribed under section 5(2) and specify its duration. Under Bill C-22, however, the order comes into force only once it has been approved by the Intelligence Commissioner, who must provide a written decision to that effect (section 7(2) of the SAAIA), a requirement not found in Bill C-2. **The House of Commons Standing Committee on Public Safety and National Security also amended section 7 in order to add a ceiling of two years to the validity period of ministerial orders and to authorize the inclusion of provisions regarding the disclosure of their existence or content.**

PRELIMINARY VERSION
UNEDITED

As provided in Bill C-2, the Minister of Public Safety must take into account a range of factors before making an order, including the benefits to the administration of justice, feasibility, compliance costs and the impact on ESP users (section 7(3) of the SAAIA). Bill C-22 expands this list, however, by adding a distinct factor relating to privacy protection and cybersecurity (section 7(3)(e) of the SAAIA).

Compensation may be provided to offset the compliance costs incurred by the ESP (section 7(4) of the SAAIA). As with regulatory obligations, a provider may be exempt if the obligation would create a "systemic vulnerability" or prevent the provider from rectifying such a vulnerability.

Before making an order under section 7(1), the Minister of Public Safety must give the ESP in question an opportunity to make representations (section 8 of the SAAIA). Unlike Bill C-2, Bill C-22 does not require the Minister of Public Safety to consult the Minister of Industry; instead, it provides that any order be transmitted to the Intelligence Commissioner for review and approval in accordance with the *Intelligence Commissioner Act* (section 9 of the SAAIA). **At the committee stage, the House of Commons Standing Committee on Public Safety and National Security also amended section 9 of the SAAIA in order to require that the orders approved and the information sent to the Intelligence Commissioner be sent to the National Security and Intelligence Review Agency (NSIRA) to support this agency in fulfilling its oversight mandate.**[38]

An order has effect for the period specified, unless revoked (section 10 of the SAAIA). **At the committee stage, the House of Commons Standing Committee on Public Safety and National Security removed the provisions that allowed for the validity period of an order to be extended without further review by Canada's Intelligence Commissioner. The committee also removed the requirement imposed on the Minister of Public Safety to review orders before they expire in order to determine whether it would be appropriate to extend their validity.** In the event of a conflict between an order and a regulation made under section 5, the order prevails (section 1**2** of the SAAIA).

2.2.3 Obligation to Assist and Confidentiality

ESPs are required to provide, on request, all reasonable assistance to assess or test devices that enable an authorized person to access information. Such requests may be made by persons authorized to do so under section 1**3** of the SAAIA and must be complied with within the time and in the manner prescribed.

Under Bill C-22, the request must be made by the minister or by any other person belonging to the prescribed classes of authorized requesters.[39] The request must also be in writing and set out its purpose as well as any applicable limits or conditions.

PRELIMINARY VERSION
UNEDITED

Lastly, Bill C-22 expressly provides that the assessment or testing must not grant access to personal information (section 1**3** of the SAAIA).

Section 1**4** of the SAAIA prohibits ESPs and any person acting on their behalf from disclosing various categories of information related to ministerial orders, unless authorized to do so by the SAAIA or the *Canada Evidence Act*. These prohibitions largely mirror those found in Bill C-2, with the exception of the prohibition relating to information about a systemic vulnerability, which is not included in Bill C-22. **The House of Commons Standing Committee on Public Safety and National Security added the new section 15 of the SAAIA in order to allow an ESP to obtain written authorization from the Minister of Public Safety to disclose certain information covered by a prohibition on disclosure. When the information is relevant to the performance of a regulatory authority's duties or functions, the Minister may impose conditions that the Minister considers reasonable and must grant this authorization.**

Section 16 of the SAAIA establishes a regime governing confidential information obtained by designated persons in the course of inspections conducted under sections 20 and 21 of the SAAIA as well as information obtained in an internal audit report under section 23. This regime is not provided for in Bill C-2.

The right of an ESP to seek judicial review of an order or decision is set out in section 17 of the SAAIA. As with section 16 of the SAAIA under Bill C-2, at least 15 days' written notice must be provided to the minister; however, section 17(2) specifies that the Federal Court has exclusive jurisdiction to hear such applications.

Section 18 of the SAAIA, as proposed in Bill C-22, empowers the Governor in Council to make regulations respecting the confidentiality of information, the security of facilities and requirements related to employees. These powers extend to the disclosure and protection of information under new sections 1**4** and 16 of the SAAIA as well as to security clearance requirements for employees and the facilities used for processing information that is the subject of a lawful access request. The corresponding regulation-making powers under section 17 of the SAAIA in Bill C-2 were more limited in scope.

2.2.4 Administration and Enforcement

The Minister of Public Safety may, subject to conditions, designate persons for the purpose of verifying compliance with the SAAIA. The minister must provide that person with a certificate attesting to their designation. The designated person must, on request, produce the certificate to establish their authority in the course of their duties (section 19 of the SAAIA).

A designated person may enter any place, other than a dwelling-house, to verify compliance with the SAAIA if they have reasonable grounds to believe that anything relevant to that purpose is located in that place or that an activity regulated by the SAAIA is conducted in that place. They may examine, make copies of or remove any document or electronic data and use any equipment at the place to do so. The ESP's employees must give all reasonable assistance (section 20 of the SAAIA). A warrant is required to enter a dwelling-house without the occupant's consent (section 21 of the SAAIA), and force may be used only if authorized in the warrant and if a peace officer is present.

A designated person may also require an ESP to conduct an internal audit of its practices, documents and electronic data for any purpose related to verifying compliance or preventing non-compliance with the SAAIA (section 22 of the SAAIA). The ESP must comply with the requirement and provide a detailed report of the audit (section 23 of the SAAIA). If the designated person has reasonable grounds to believe **that there is or is likely to be a contravention of any provision of the SAAIA,** they may request the ESP to cease the activity in question and to take the necessary measures by imposing a compliance order (section 24 of the SAAIA). The ESP must comply with the order and notify the designated person once they have done so (section 25 of the SAAIA). **The House of Commons Standing Committee on Public Safety and National Security added to sections 24 and 25 of the SAAIA an exception that allows an ESP to not comply with a compliance order if it would require the provider to introduce a systemic vulnerability or prevent the provider from rectifying such a vulnerability.**

An ESP may request a review of the compliance order by the minister, but the order remains in effect during the review unless the minister decides otherwise. If no decision is made within 90 days of the request for review **by the ESP**, the order is deemed confirmed (sections 26 and 27 of the SAAIA). **An amendment adopted at committee added to section 27 the obligation to notify the NSIRA about the compliance orders issued, the requests for review submitted and the decisions made by the Minister of Public Safety in order to support the agency in fulfilling its oversight mandate.**

2.2.5 Administrative Monetary Penalties and Offences

The SAAIA provides for administrative monetary penalties (sections 28 to 31) and offences (sections 41 to 46), both of which are intended to ensure compliance with the Act but differ in their nature and consequences.

PRELIMINARY VERSION
UNEDITED

Administrative monetary penalties are not intended to punish but to promote compliance with the SAAIA (section 28 of the SAAIA), and they apply in respect of violations of certain statutory or regulatory provisions. They may result in fines of up to $50,000 for an individual and up to $250,000 for an entity, with each day that the offence is committed or continued constituting a separate offence (section 29 of the SAAIA).

The same types of violations, on summary conviction, may give rise to criminal offences carrying higher fines – up to $100,000 for an individual and $500,000 for an entity. Each day that the offence is committed or continued likewise constitutes a separate offence (section 41 of the SAAIA).

In both cases, a due diligence defence is available if the person establishes that they exercised due diligence (sections 29(4) and 41(4) of the SAAIA). In both cases as well, a violation or offence may be established on the basis of the acts or omissions of an employee or an agent or mandatary, whether or not the employee or agent or mandatary is identified (sections 30 and 42 of the SAAIA), and the directors or agents or mandataries of an entity may be held liable if they participated in the commission of the violation or offence (sections 31 and 43 of the SAAIA).

Additional specific offences are provided for obstruction (section 44 of the SAAIA) and for making false or misleading statements (section 45 of the SAAIA), with distinct fines (section 46 of the SAAIA).

2.2.6 Regulations

Section 47(1) of the SAAIA authorizes the Governor in Council to make regulations respecting various aspects of the implementation of the SAAIA, including fees payable to ESPs for assistance provided, record-keeping and reporting, the meaning of certain terms in the SAAIA as well as the form and manner of orders and reports under the SAAIA.

Section 47(2) of the SAAIA requires the Minister of Public Safety to review all regulations every five years after the day on which the first regulation is made. Section 47(3) requires that a public notice be published before the first regulation is made and at every review in order to solicit representations from the Attorney General of Canada, the attorney general of each province, core providers and ESPs subject to an order.

Lastly, section 48 of the SAAIA provides that the regulations may establish classes of ESPs and distinguish among them on the basis of the service provided and on the size of their subscriber base in Canada.

PRELIMINARY VERSION
UNEDITED

2.2.7 Annual Report

Compared to Bill C-2, Bill C-22 provides, in section 49 of the SAAIA, that the minister must publish an annual report on the administration of the SAAIA. The report must include the number of orders made and the number of orders not approved by the Intelligence Commissioner, the classes of ESPs to which they apply, the obligations imposed, the compliance measures taken and the requests for assistance made under section 14 of the SAAIA. The report, with redactions as necessary, must be made public within 60 days, while a full, unredacted version must be provided to the National Security and Intelligence Committee of Parliamentarians and the National Security and Intelligence Review Agency.

2.3 PART 3: PARLIAMENTARY REVIEW (SECTION 48 OF BILL C-22)

2.3.1 Parliamentary Review

Part 3 of Bill C-22 provides for a parliamentary review of the Act three years after it comes into force. According to a Government of Canada backgrounder, this parliamentary review further increases transparency.[40]

NOTES

1. Bill C-22, An Act respecting lawful access, 45th Parliament, 1st Session.
2. House of Commons, Standing Committee on Public Safety and National Security, *Bill C-22, An Act respecting lawful access*, Firth report, June 2026.
3. Government of Canada, *Lawful access*.
4. *Criminal Code*, R.S.C. 1985, c. C-46; and *Canadian Security Intelligence Service Act*, R.S.C. 1985, c. C-23.
5. Government of Canada, *Lawful access*.
6. Ibid.
7. Council of Europe, *Convention on Cybercrime*, 23 November 2001.
8. Council of Europe, *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence*, 12 May 2022.
9. United States, *Consolidated Appropriations Act, 2018*, Public Law 115–141, 155th Congress, 132 Stat. 348.
10. For more information, see Michael Fekete and John Salloum, "Data sovereignty in light of the CLOUD Act: back to the future?," *Osler*, 7 October 2025; and Canadian Bar Association, "How to address Canada's digital data disclosures with the U.S.," *CBA National*, 31 January 2025.
11. United States, Department of Justice, *CLOUD Act Resources*.
12. Ibid.
13. Bill C-2, An Act respecting certain measures relating to the security of the border between Canada and the United States and respecting other related security measures, 45th Parliament, 1st Session.

PRELIMINARY VERSION
UNEDITED

14. Public Safety Canada, *Supporting Authorized Access to Information Act (Bill C-22 – Part 2)*, Backgrounder.

15. *Protecting Canadians from Online Crime Act*, S.C. 2014, c. 31.

16. *National Security Act, 2017*, S.C. 2019, c. 13.

17. Department of Justice Canada, *Proposed changes to laws on timely access to information (Bill C-22 – Part 1)*, Backgrounder.

18. *R. v. Vu*, 2013 SCC 60 (CanLII).

19. "Reasonable grounds to believe" is the threshold in the *Criminal Code* authorizing a search warrant in Canada. In *R. v. Storrey*, [1990] 1 S.C.R. 241, the Supreme Court of Canada explains that the person who exercises a power based on "reasonable grounds to believe" must "subjectively have reasonable and probable grounds" on which to exercise that power, and those grounds must be "justifiable from an objective point of view."

20. *R. v. Spencer*, 2014 SCC 43, para. 11.

21. According to the Supreme Court of Canada's decision in *R. v. Bykovets*, an Internet Protocol (IP) address is

> a unique identification number. IP addresses identify Internet-connected activity and enable the transfer of information from one source to another. They are necessary to access the Internet. An IP address identifies the source of every online activity and connects that activity (through a modem) to a specific location. And an Internet Service Provider (ISP) keeps track of the subscriber information that attaches to each IP address.

22. In paragraph 75 of *R. v. Kang-Brown*, 2008 SCC 18, the Supreme Court of Canada provided the following definition of "reasonable grounds to suspect":

> "Suspicion" is an expectation that the targeted individual is possibly engaged in some criminal activity. A "reasonable" suspicion means something more than a mere suspicion and something less than a belief based upon reasonable and probable grounds.

In paragraph 27 of *R. v. Chehil*, 2013 SCC 49, the Supreme Court of Canada stated that

> while reasonable grounds to suspect and reasonable and probable grounds to believe are similar in that they both must be grounded in objective facts, reasonable suspicion is a lower standard, as it engages the reasonable possibility, rather than probability, of crime.

23. Section 2(1) of the *Telecommunications Act* defines the term "telecommunications service provider" as a "a person who provides basic telecommunications services, including by exempt transmission apparatus." *Telecommunications Act*, S.C. 1993, c. 38, s. 2(1).

24. *Criminal Code*, R.S.C. 1985, c. C-46, s. 487.014.

25. An *ex parte* application means an application made without notice to the other party concerned by the application.

26. For service providers in foreign countries with which Canada has a mutual legal assistance agreement, law enforcement may currently proceed through the Mutual Legal Assistance Treaty process. Under this process, a request must first be submitted to Canada's Department of Justice before being forwarded to the foreign state so that the request can be directed to the foreign service provider. See Department of Justice Canada, *Proposed changes to laws on timely access to information (Bill C-22 – Part 1)*, Backgrounder; and Department of Justice Canada, *Mutual Legal Assistance Requests Made by Canada*.

27. *Criminal Code*, R.S.C. 1985, c. C-46, s. 487.11. The term "exigent circumstances" was interpreted by the Supreme of Canada in paragraph 33 of *R. v. Paterson*, 2017 SCC 15, as "not merely convenience, propitiousness or economy, but rather *urgency*, arising from circumstances calling for immediate police action to preserve evidence, officer safety or public safety."

28. Department of Justice Canada, *Proposed changes to laws on timely access to information (Bill C-22 – Part 1)*, Backgrounder.

29. *Mutual Legal Assistance in Criminal Matters Act*, R.S.C. 1985, c. 30 (4th Supp.).

30. Ibid., s. 2(1).

PRELIMINARY VERSION
UNEDITED

31. The judge must be satisfied that there are reasonable grounds to suspect that "an offence has been or will be committed," and that the "will assist in the investigation of the offence." *Criminal Code*, R.S.C. 1985, c. C-46, ss. 487.016(2)(a) and 487.016(2)(b).

32. Ibid., s. 487.0198.

33. *Controlled Drugs and Substances Act*, S.C. 1996, c. 19.

34. *Cannabis Act*, S.C. 2018, c. 16.

35. Under section 487.011 of the *Criminal Code*, "transmission data" means data that relates to the telecommunication functions of dialling, routing, addressing and signalling and that identifies certain characteristics of a communication without revealing its substance, meaning or purpose. According to the Office of the Privacy Commissioner of Canada, metadata is data that provides information about other data and describes the context in which it is used. For example, the time a message is sent and the destination number of the text message are transmission data, while the device model and the technical identifier of the message are metadata.

36. At the committee stage, the House of Commons Standing Committee on Public Safety and National Security amended paragraph 5(2)(d) in order to reduce this period from one year to six months.

37. At the committee stage, the House of Commons Standing Committee on Public Safety and National Security amended this definition in order to include a criterion based on recognized international technical standards, to replace the concept of "substantial risk" with "credible risk" and to exclude certain risks relating to the exercise of legal powers regarding access to information under any other Act of Parliament.

38. The National Security and Intelligence Review Agency is an independent organization that is responsible for reviewing the activities of the Government of Canada in terms of national security and intelligence. In particular, its mandate includes reviewing activities carried out by federal departments and agencies in order to assess their legality, reasonableness and need, as well as to draw conclusions and make recommendations in this respect (s. 8(1)(a) to 8(1)(c)).

39. Section 1**3** of the Supporting Authorized Access to Information Act, as set forth in Bill C-22, provides that an applicant may be one of the following persons: the Minister, an employee of the Canadian Security Intelligence Service, a person appointed or employed under Part I of the *Royal Canadian Mounted Police Act* or a person referred to in section 10 of that Act, a civilian employee of another police force or a peace officer as defined in section 2 of the *Criminal Code*.

40. Public Safety Canada, *Supporting Authorized Access to Information Act (Bill C-22 – Part 2)*, Backgrounder.