BILL C-22

AN ACT RESPECTING LAWFUL ACCESS

ESTABLISHING A SURVEILLANCE ARCHITECTURE IN CANADA

BRIEF SUBMITTED BY



STANDING SENATE COMMITTEE ON NATIONAL SECURITY, DEFENCE AND VETERANS AFFAIRS

THE SENATE OF CANADA

OCTOBER 29, 2026

PRESENTATION OF THE LIGUE DES DROITS ET LIBERTÉS

The *Ligue des droits et libertés* is an independent, non-partisan, non-profit organisation that aims to defend and promote human rights by promoting their universality, indivisibility and interdependence. Since its creation in 1963, the LDL has influenced several government policies and bills, and contributed to the creation of instruments and institutions dedicated to the defence and promotion of human rights, such as the *Quebec Charter of Human Rights and Freedoms*, and the *Commission des droits de la personne et des droits de la jeunesse* (CDPDJ).

The LDL regularly intervenes in the public sphere to voice demands and denounce human rights violations before government authorities at the local, national and international levels. The LDL is also a member of the International Federation for Human Rights (FIDH). The LDL continues, as it has throughout its history, to fight against discrimination and all forms of abuse of power, in defence of civil, political, economic, social and cultural rights, which are universal, interdependent and indivisible.

The LDL hereby submits its brief to the House of Commons Standing Committee on Public Safety and National Security regarding Bill C-22, An Act Respecting Lawful Access, filed on March 12, 2025

INTRODUCTION

Bill C-22, the Legal Access Act, introduced by the government on March 12, 2026, establishes an unprecedented surveillance framework that could affect every digital tool Canadians use on a daily basis. This bill represents one of the greatest threats to the right to privacy in Canada in the past two decades.

C-22 contains sweeping new powers that could require any digital service provider to retain the metadata of every client in Canada for a period of one year, thereby infringing on the right to privacy of millions of people. The utterly excessive scope of C-22 poses a serious threat to civil liberties.

The fact that Canada's partner countries have adopted such provisions in no way justifies the establishment of a surveillance state and the abandonment of our democratic principles and constitutional rights. On the contrary, the abuses and excesses that accompany such provisions lead the *Ligue des droits et libertés* to call for the unequivocal rejection of this liberty-destroying bill.

PART 1 OF BILL C-22

Bill C-22 introduces significant amendments to the Criminal Code and the Canadian Security Intelligence Service Act (CSIS). The proposed amendments greatly expand the powers of law enforcement agencies (police officers and public officers) and CSIS to obtain subscriber information and transmission data (TD).

1. CONFIRMATION OF SERVICE DEMAND

Bill C-2 (the first version of C-22) would have allowed access to subscriber information without a warrant, pursuant to an information demand. The government has backed down on this point. Under Bill C-221, this is instead a "confirmation of service demand" that applies solely to a telecommunications service providers (TSP) and is limited to determining whether or not they are providing services to a subscriber.

Although the category of TSP is narrower than "any person providing services to the public," as was the case in C-2, in the digital age it remains broad: mobile operators, messaging platforms, social media platforms, cloud computing services, etc.

Thus, the scope of this new power remains a cause for concern, especially since it is not subject to judicial oversight. In fact, a "confirmation of service demand" can be issued based on mere suspicion (reasonable grounds to suspect) that an offence of a federal law (any offence) has been or will be committed and that the information will be useful to the investigation—all of which is assessed solely by the police officer and not confirmed by a judge. It should be noted that the evidentiary threshold of reasonable grounds to suspect is lower than the threshold of reasonable grounds to believe.

In addition, the order may be accompanied by a non-disclosure order lasting up to one year. The fact that information obtained under this "confirmation of service demand" may eventually be used to obtain a "order for subscriber information" (see next section) creates an escalation effect: a power exercised without judicial oversight becomes the gateway to the exercise of another power that allows for the collection of much more substantial information.

2. PRODUCTION ORDER AND SUBSCRIBER INFORMATION

Subscriber information may be obtained pursuant to a Production order[2] issued by a judge. This order is addressed to any "person who provides services to the public". Its scope is therefore extremely broad. "Subscriber information" is also defined very broadly: name, address, phone number, email address, pseudonym, username, account number, and the services provided (types, time period, equipment used)[3]. This very sensitive information may be obtained on the basis of reasonable grounds to *suspect* that an offence of any federal law has been or will be committed. And simply by demonstrating that it will "*assist* in the investigation."

---

[1] Bill C-22, sections 5 and 31.
[2] Bill C-22, Section 6.
[3] Bill C-22, Section 4.

This represents an unacceptable lowering of the threshold applicable to this type of search since the Supreme Court's *Spencer* decision[4]. Currently, authorities can obtain subscriber information[5] through a general production order (GPO)[6], and the more stringent threshold of reasonable grounds to *believe* is required. Furthermore, in this context, the officer must demonstrate that the subscriber information "will afford evidence respecting the commission of the offence" and not merely that they will "assist the investigation," as proposed by Bill C-22. This represents a major setback for the protection of citizens' privacy.

In recent years, the Supreme Court has established, in the *Spencer* and *Bykovets* decisions[7], the importance to be attached to reasonable expectations of privacy in relation to online activity. In Spencer, the Court recognized "anonymity is an important safeguard for privacy interests online[8]." Reasonable expectations of privacy exist with respect to this information, and abandoning the standard of reasonable grounds to *believe* seriously undermines this fundamental right.

Our previous comments apply to the similar powers granted to CSIS under Sections 30 through 36 of Bill C-22.

3. COLLABORATION

Section 11 of Bill C-22 would amend the Criminal Code[9] to specify "for greater certainty" that no order is required for a peace officer *to ask* a person to "*voluntarily* provide […] information […] that the person is not prohibited by law from disclosing" (our emphasis). The person who cooperates ''does not incur any criminal or civil liability for doing so" and therefore would then enjoy an immunity. No limits are specified regarding the type of information covered. Does this include personal information, such as subscriber information? We're concerned it will.

In the *Spencer* decision[10], however, the Supreme Court ruled that a request by a police officer for subscriber information constitutes a search. The *Bykovets* decision reaffirms this principle.

> In *Spencer*, this Court determined that a reasonable expectation of privacy attaches to subscriber information — the name, address, and contact information — associated with an individual Internet Protocol (IP) address. A request for this information by the state is a "search" under s. 8 of the *Canadian Charter of Rights and Freedoms*[11].

---

[4] *R v Spencer*, 2014 SCC 43.
[5] "Since the Supreme Court of Canada decision in *R. v. Spencer* (2014), telecommunications providers generally only provide information if served with a court order." Government of Canada. Proposed Amendments to the Timely Access to Information Acts (Bill C-22—Part 1). https://www.justice.gc.ca/eng/csj-sjc/pl/c22/index.html
[6] Criminal Code R.C.S 1985, c. C-46, Section 487.014.
[7] *R v Bykovets*, 2024 SCC 6.
[8] *R v Spencer*, 2014 SCC 43, Section 78.
[9] Replacement of Section 487.0195.
[10] *R v Spencer*, op. cit., para 66. "In my view, in the totality of the circumstances of this case, there is a reasonable expectation of privacy in the subscriber information. […] A request by a police officer that an ISP voluntarily disclose such information amounts to a search."
[11] *R v Bykovets*, 2024 SCC 6, Section 2.

The amendments provided for in Section 11 could potentially circumvent these two rulings by exempting the voluntary exchange of subscriber information between a law enforcement officer and persons from judicial oversight.

Admittedly, there is one caveat: the provision of information is conditional on no legal rule prohibiting it. But why, in that case, grant the person civil or criminal immunity? This seems inconsistent. There is a real concern that, given this civil or criminal immunity, the person will make little or no effort to verify whether the disclosure of information is legally permitted.

These amendments jeopardize the right to online privacy. They provide protection for the provision of information left to the discretion of persons or private companies, and lead to a form of arbitrariness. In *Bykovets*, the Court emphasizes the importance of judicial review:

> Judicial oversight would also remove the decision of whether to reveal information — and how much to reveal — from private corporations and return it to the purview of the *Charter*.[12]

4. PUBLICLY AVAILABLE INFORMATION

Section 11 of Bill C-22 introduces another change to the Criminal Code. It states that no production order or warrant is required to "receive, obtain and act on any information that is available to the public". No definition of "publicly available information" is provided, nor are any limits set on its use.

Does this refer, in particular, to information obtained online? In the Clearview AI case[13], the Office of the Privacy Commissioner of Canada and its provincial counterparts ruled that personal information obtained from sources such as social media or professional profiles could not be used without the consent of the individual concerned, pursuant to privacy laws. As the Commission d'accès à l'information du Québec [Quebec Commission on Access to Information] noted in this decision:

> Even where personal information has been posted on a public website, it does not mean that the information may be used for other purposes without the consent of the person concerned. The fact that images are published on a website does not necessarily mean that their author has consented to their use by a third party.[14]

The commissioners therefore concluded that the facial recognition software developed by Clearview AI using photos taken from the internet—without consent—was illegal; and that it was equally illegal for the RCMP to use such software[15].

---

[12] *R v Bykovets*, 2024 SCC 6, Section 12.

[13] Joint investigation into Clearview AI, Inc. by the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the British Columbia Information and Privacy Commissioner's Office, and the Alberta Information and Privacy Commissioner's Office. PIPEDA Findings No. 2021-001. February 2, 2021. Online: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/

[14] Ibid., Section 46.

[15] Office of the Privacy Commissioner of Canada. "RCMP's use of Clearview AI's facial recognition technology violated *Privacy Act*, investigation concludes." Press Release. June 10, 2021. https://www.priv.gc.ca/en/opc-news/news-and-announcements/2021/nr-c_210610/

Allowing law enforcement agencies to make unlimited use of information available on the internet, simply because it is "accessible," poses serious risks:

Canadians must be free to participate voluntarily and actively in the regular, and increasingly digital, day-to-day activities of a modern society. They must be able to navigate public, semi-public, and private spaces without the risk of their activities being routinely identified, tracked and monitored.[16]

As the Supreme Court noted in *Bykovets*, "Canadians are not required to become digital recluses in order to maintain some semblance of privacy in their lives"[17].

The law should specifically outline the types of information that law enforcement agencies may use. The amendment proposed by Bill C-22 regarding publicly available information is far too broad. It could undermine the principles established in Clearview AI. At the very least, it should be made clear that the authority to obtain and act on publicly available information must be exercised in accordance with privacy laws.

5. EXPANDED POWERS IN THE EVENT OF "EXIGENT CIRCUMSTANCES"

Section 14 of C-22 proposes to amend section 487.11 of the Criminal Code and significantly expand the powers that may be exercised when "by reason of exigent circumstances it would be impracticable to obtain a warrant." Currently, in an emergency situation, an officer may, without a warrant, have the general search authority provided for in section 487, as well as the authority to place a tracking device on things, as provided for in section 492.1. If the amendment is adopted, in addition to these powers, police officers would be able to, *without a warrant*:

- Installing a tracking device on a person, a power provided for in section 492.1(2), which typically requires a warrant based on reasonable grounds to *believe*;
- Installing a transmission data recorder, a power provided for in section 492.2(1);
- Obtaining the disclosure of transmission data, a power provided for in section 487.016;
- Obtaining the disclosure of location data, a power provided for in section 487.017;
- As well as the new power under section 487.0142 regarding the disclosure of subscriber information.

It is worth noting in particular that the authority to install without a warrant a tracking device on an individual—rather than on an thing—makes it possible to track an individual's movements in real time, all without any judicial authorization (currently required on the basis of reasonable grounds to *believe*), based solely on the officer's assessment that the urgency of the situation justifies it, and without the person in question ever being informed.

---

[16] Office of the Privacy Commissioner of Canada. "Police use of Facial Recognition Technology in Canada and the way forward". Online: https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/202021/sr_rcmp/

[17] *R v. Bykovets*, op. cit., Section 48.

6. PRODUCTION REQUEST TO A FOREIGN ENTITY

Section 7 of Bill C-22 amends the Criminal Code by the addition of a new section.[18] It would allow law enforcement agencies to request that "a foreign entity that provides telecommunications services - or that provides services by a means of telecommunication - to the public" disclose subscriber information and transmission data in its possession. The production request must be authorized by a judge based on the threshold of reasonable grounds *to suspect* an offence of a federal law and that the information will assist in the investigation.

It goes without saying that the criticisms we raised in item 1 regarding the use of a less stringent standard (reasonable grounds *to suspect*) in obtaining subscriber information and transmission data—rather than the threshold of reasonable grounds *to believe*—apply here as well.

7. MUTUAL LEGAL ASSISTANCE IN CRIMINAL MATTERS ACT (MLACMA)

Section 29 of Bill C-22 adds a new section 22.07 to the MLACMA. It would allow Canadian authorities to enforce foreign orders for the purpose of obtaining subscriber and transmission data held in Canada. The request for mutual legal assistance is submitted to the Minister of Justice, who designates a competent authority (the Attorney General of Canada or of a province) to file an application with a judge. The judge may declare the foreign decision enforceable if it meets—*with the necessary adaptations*—the requirements of 487.016(2) in the case of transmission data; and of 487.0142(2) in the case of subscriber information. This is based on reasonable grounds *to suspect* an offence and that the information will be useful.

Once again, the concerns we raised in item 1 regarding the use of a lower evidentiary standard in obtaining subscriber information and transmission data—rather than the reasonable grounds to *believe* standard—apply here, and all the more so, given that this involves the transfer of sensitive personal information to a foreign entity.

Furthermore, to meet the requirements of section 487.016(2) or 487.0142(2), there must be reasonable grounds to *suspect* an *offence of a federal law*. What about the enforcement of a foreign judgment? The section states "with the necessary adaptations". But what does that mean? Are we to allow the enforcement of foreign judgments for offenses that do not exist in Canada? Or, worse still, for acts that constitute the exercise of democratic rights in Canada but are considered crimes abroad? Professor Pierre Trudel sums up the problem very well:

> *Is it reasonable to allow U.S. law enforcement to obtain information about people in Canada? This could include information related to issues such as access to abortion, social reintegration services, or political protests.*[19] (our translation)

Section 29 paves the way for an increase in the exchange of personal information with countries that do not have the same legal framework and do not necessarily offer the same safeguards as Canada in terms of human rights and democracy. Such data sharing could jeopardize people's safety—as in the

---

[18] Article 487.0181

[19] Le Devoir, Professeur Pierre Trudel, columnist, *À la merci de la police de Trump*, August 19, 2025. https://www.ledevoir.com/opinion/chroniques/910500/chronique-merci-police-trump

case of Maher Arar for example[20]. The *Ligue des droits et libertés* opposes the expansion of cross-border data sharing, in the absence of a framework that ensures the protection of privacy and respect for fundamental rights.

8. AMENDMENTS THAT PAVE THE WAY TO FURTHER PRIVACY BREACHES

Bill C-22, like its predecessor, Bill C-2, also appears to be paving the way for a process to facilitate foreign entities' access to the data of Canadians. The provisions amending the MLACMA are intended, in particular, to meet the obligations arising from the ratification of the Second Additional Protocol to the Budapest Convention on Cybercrime (2AP). Officials at Justice Canada have acknowledged that the intent of certain provisions in Bill C-2, carried over into Bill C-22, was specifically to enable Canada to implement and ratify the 2AP. These provisions could also serve as a precursor to a potential Canada–U.S. bilateral agreement under the U.S. Cloud Act. However, these two instruments raise important concerns regarding privacy and fundamental rights.

PART 2 OF BILL C-22

Part 2 enacts the *Supporting Authorized Access to Information Act.*

Under the guise of "facilitat[ing] the exercice […] to access to information"[21] by law enforcement and national security officials, Bill C-22 establishes an unprecedented system of mass surveillance, even though there has been no demonstration that existing powers are insufficient.

1. CORE PROVIDERS

Under 5(2), C-22 allows the Governor in Council to require, by regulation, core electronic service providers to develop, implement, and maintain operational and technical capabilities that enable an authorized person to access information. These provisions effectively place electronic service providers at the service of law enforcement agencies and divert the services they offer to the public for surveillance purposes.

It should be noted that the list of core electronic services providers in appendix to the Act is empty and that the Governor in Council may, by regulation, "amend the schedule by adding, amending, or deleting a class of electronic service providers"[22]. In a complete lack of transparency, the Act would thus be enacted without the legislature or the public having the slightest idea of the scope of services that will eventually be covered. This is all the more concerning given that the definition of an electronic service provider encompasses all "persons that […] provide an electronic service, *including* for the purpose of enabling communications"[23] (emphasis added). The law therefore makes it possible to subject electronic service providers whose primary function is not to facilitate communication.

---

[20] Radio-Canada. Maher Arar blanchi, *La GRC blâmée*, September 18, 2006.
[21] Bill C-22, Summary.
[22] Bill C-22, Part 2, Section 5 (1).
[23] Bill C-22, Part 2, Section 2 (1).

The definition of an electronic service is also very broad: "a service—or a feature of a service—that involves the creation, recording, storage, processing, transmission, reception, emission, or making available of information in electronic or digital or any other intangible form by an electronic, digital, magnetic, optical, biometric, acoustic or other technological means—or a combination of any such means."[24]

In today's digital world, virtually every organization that Canadians do business with falls under these definitions. Bill C-22 will allow the government to arbitrarily compel countless entities that the public relies on to become tools at the government's disposal for obtaining information about their customers.

Core service providers may be required to retain certain categories of metadata for a period of six months, *including* transmission data as defined in section 487.011 of the Criminal Code. Under Section 487.011, transmission data refers to data that both "relates to the telecommunication functions of dialling, routing, addressing or signalling […] and identifies or purports to identify the type, direction, date, time, duration, size, origin, destination, or termination of the communication." This data is not trivial. They reveal a great deal about our activities (social connections, travel, etc.) and are protected by privacy laws.

Furthermore, the law leaves open the possibility that this metadata may not be limited to transmission data. Under Bill C-22, this data will be collected on individuals—potentially a significant portion of Canada's population—who are not the subject of any investigation. This data will be accessible to law enforcement and CSIS based on mere reasonable grounds to *suspect*, whereas it should only be accessible to law enforcement in the context of specific investigations with a court warrant based on reasonable grounds to *believe*. Bill C-22 is an attack not only on privacy but also on the presumption of innocence.

2. MINISTERIAL ORDERS

C-22 goes even further. Under 7(1), the Minister may issue orders with respect to service providers, valid for a period of up to two years, whether or not they are core service providers, imposing on them the same obligations as those imposed on core services providers by regulation. However, the retention of information under ministerial orders is not subject to the same restrictions as that imposed by regulation under 5(4). The information covered by the ministerial orders does not explicitly exclude the content of communications, a person's web browsing history, or a person's social media activities. Taken together, this information amounts, for all practical purposes, to total surveillance of a person's life. Orders issued under subsection 7(1) take precedence over any inconsistent regulations issued under subsection 5(2), and they can be required to remain confidential.

An order becomes valid upon approval by the Intelligence Commissioner. Under the CSIS Act, the Minister "determines clases of Canadian data sets for which collection is authorized if the Minister dconcludes that the querying or exploitation of data sets in the class could lead to results that are relevant." Such information may be collected without a court order if approved by the Intelligence

[24] Ibid.

Commissioner. The purpose of Bill C-22 is to make these datasets available to CSIS by requiring a broader range of providers—beyond the core providers—to provide information—beyond what can be obtained through regulations—to CSIS.

The individuals subject to this surveillance are not being monitored as part of a criminal investigation, are unaware that they are under such surveillance, and have no legal recourse. The only protection against abuse is the requirement that orders be approved by the Intelligence Commissioner, a process that takes place in secret. It should be noted that the Intelligence Commissioner must make decisions based solely on information provided by intelligence agencies and the Minister.

3. OBLIGATION TO ASSIST

The Governor in Council may make regulations requiring core service providers to maintain "operational and technical capabilities, including capabilities related to extracting and organizing information that is authorized to be accessed"[25] and to ensure "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."[26] The electronic service provider may be required to decrypt any information if the encryption was provided by that provider and it has the necessary information to decrypt the information.

These provisions require service providers to maintain backdoors that allow authorized persons to access the information held by service providers. The Act provides that a provider is not required to comply with a provision of a regulation if, according to recognised international technical standards, this creates a 'credible' risk that an unauthorised person might gain access to the information. What constitutes a 'credible' risk is undefined and arbitrary, as it is unclear which so-called 'recognised international standards' the bill refers to. In its amended form, Bill C-22 goes even further than the version tabled in March 2026, as the protection against systemic vulnerabilities does not apply where the information relates to a person subject to a warrant. How can a system be vulnerable for one category of users without affecting the protection of all users?

But that is not the issue. Any vulnerability introduced into data systems is unacceptable. Experience has shown just how adept malicious actors—whether private or state-sponsored—can be at uncovering flaws in computer systems. The latest advances in artificial intelligence only serve to reinforce our fears. It is unrealistic to assume that a backdoor intended for authorized users could not potentially be exploited by an unauthorized person. The introduction of any vulnerability must be ruled out. These provisions of Bill C-22 are dangerous and unacceptable.

[25] Bill C-22, Part 2, Section 5 (2) a).
[26] Bill C-22, Part 2, Section 5 (2) b).

CONCLUSION

Like many other groups, the *Ligue des droits et libertés* is calling for the withdrawal of Bill C-22 on the following grounds:

1. The ability of authorities to access a wide range of personal information from any public service provider based on mere reasonable grounds *to suspect* that violation of any federal law has been or will be committed;
2. Civil and criminal immunity for the voluntary disclosure of information;
3. The excessive expansion of powers allowing police officers to bypass judicial authorization on the basis of the concept of an "emergency situation," which is left to their discretion;
4. The lack of guidelines in the authorization for police officers to use publicly available information; and the lack of a definition of what constitutes such information;
5. The use of the low evidentiary threshold of reasonable grounds to *suspect* when exchanging information with foreign states and entities;
6. Easier access by foreign entities and authorities to Canadians' data, particularly in light of the ratification of the Second Additional Protocol to the Budapest Convention on Cybercrime and a bilateral agreement with the United States under the Cloud Act;
7. The power to arbitrarily compel countless providers of services used by the public to become tools at the state's disposal for obtaining information about their customers;
8. The requirement that service providers retain highly sensitive data on citizens in order to make that data available to CSIS in absolute secrecy;
9. The requirement that service providers install backdoors putting citizens' data at risk of being hacked.

Bill C-22 grants law enforcement agencies excessive search and surveillance powers that are neither necessary, neither reasonable, nor proportionate, and establish a harmful surveillance architecture that constitutes a serious invasion of privacy.