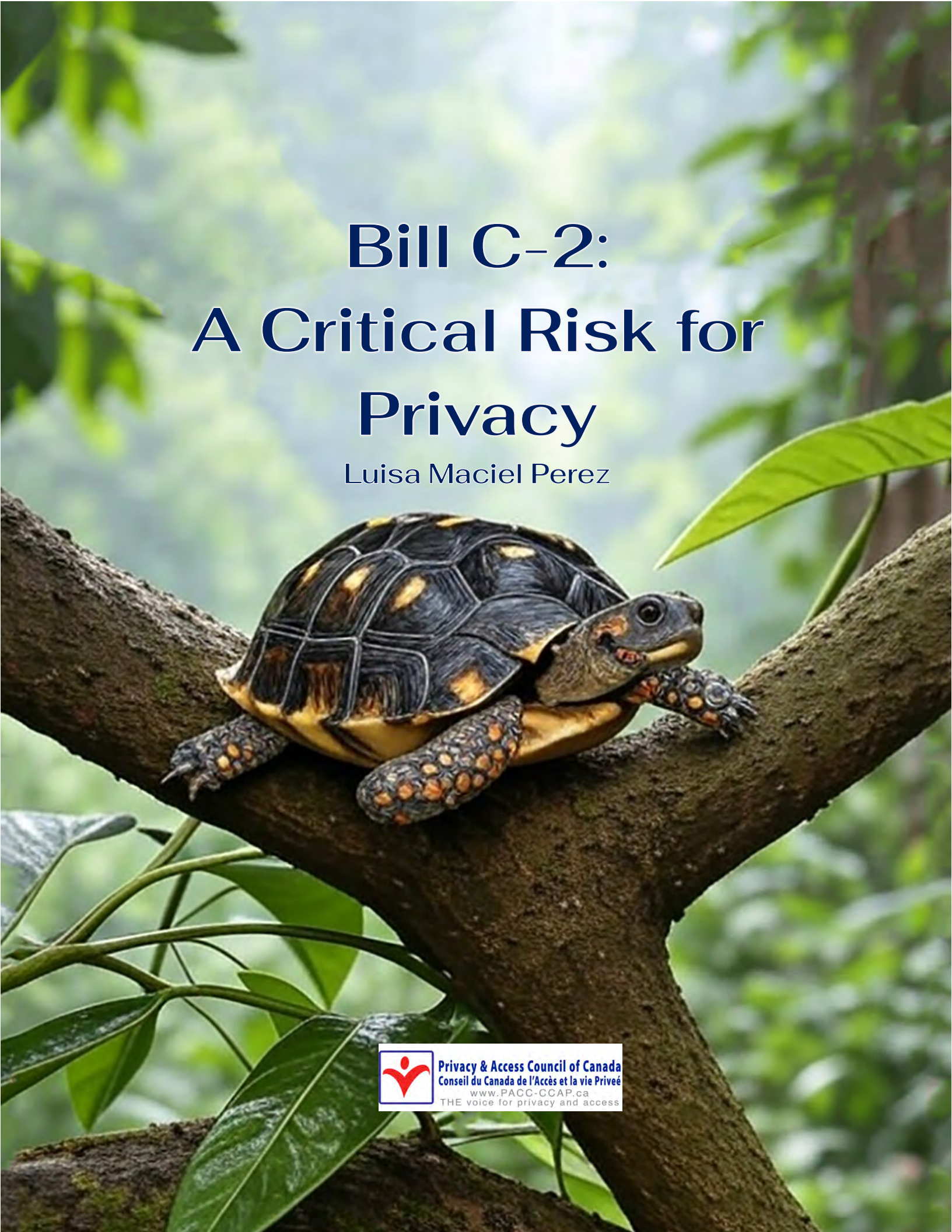
Bill C-2: A Critical Risk for Privacy

Luisa Maciel Perez



Privacy & Access Council of Canada
Conseil du Canada de l'Accès et la vie Privée
www.PACC-CCAP.ca
THE voice for privacy and access

Updates to this report
This is Version 1.0 of this report, which may be updated periodically.

About the author
This report was produced by the Privacy and Access Council of Canada, with Luisa Maciel Perez as lead author. With a background in law, Luisa seeks to use her expertise to educate about important issues affecting individuals' rights and freedoms.

Acknowledgements
We thank Luisa Maciel Perez for her dedication and insights. We also thank the staff and faculty at Dámh na nDaonnachtaí & na nEolaíochtaí Sóisialta, Ollscoil Chathair Bhaile Átha Cliath / Faculty of Humanities & Social Sciences, Dublin City University for their assistance in facilitating the collaboration between EMILDAI and PACC.

Note to readers
Every effort has been made to verify the accuracy of the information contained in this report. All information was believed to be correct as of September 2025.

Nevertheless, the Privacy and Access Council of Canada - Conseil du Canada de l'Accès et la vie Privée cannot accept responsibility for the consequences of its use for other purposes or in other contexts.

Quotation permitted. Contact Privacy and Access Council of Canada - Conseil du Canada de l'Accès et la vie Privée at media@pacc-ccap.ca regarding derivatives requests.

Table of Contents

BACKGROUND 1

BILL C-2: BROAD SCOPE, LOW THRESHOLD 1

A Clash with the Right to Privacy in Canada 5

Bill C-2: A Defiance to International Human Rights and Global Trends 10

The Risks of Mass Surveillance 22

CONCLUSION 30

REFERENCES 32

Background

On June 3, 2025, the Canadian Parliament tabled 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"[1].

The bill encompasses a wide array of amendments to several statutes[2]. Among the changes are modifications to the Criminal Code that raise serious privacy concerns due to the expansion of surveillance powers, as well as provisions that allow warrantless demands for data and information to any natural person or legal entity that provides services to the public.

This article aims to shed light on Bill C-2's provisions on the so-called lawful access to information. It will first address the key provisions on Part 14 of the bill and the immediate concerns they raise.

Bill C-2 shall then be analyzed under the national legal framework, most notably, on the right to respect one's privacy under PIPEDA, and the Supreme Court ruling in *R. v. Spencer*; and internationally, on international human rights standards such as the 13 Principles.

The bill's compatibility with global trends on mass surveillance practices will also be discussed, under the legal framework and jurisprudence of the European Court of Human Rights and the Court of Justice of the European Union.

Finally, this article aims to reveal the critical risks of mass surveillance raised by Bill C-2's provisions.

Bill C-2: broad scope, low threshold

Bill C-2 poses a significant risk to Canadians' privacy.

The main concerns arise from the amendments to the Criminal Code, established in Part 14. According to the bill[3], it is intended to "modernize certain provisions respecting the timely gathering and production of data and information during an investigation". When asked by the media, officials argued that such provisions were necessary to keep pace with the changing crime landscape[4] — a tacit acknowledgement that the bill establishes an expansion of the investigative

[1] 'C-2 (45-1) - An Act Respecting Certain Measures Relating to the Security of the Border between Canada and the United States and Respecting Other Related Security Measures' (*LEGISinfo*) <https://www.parl.ca/legisinfo/en/bill/45-1/c-2> accessed 13 June 2025.

[2] Parliament of Canada, Government Bill (House of Commons) C-2 (45-1) - An Act respecting certain measures relating to the security of the border between Canada and the United States and respecting other related security measures [C–2].

[3] N(2).

[4] Tunney C, 'Officials Defend Liberal Bill That Would Force Hospitals, Banks, Hotels to Hand over Data' (19 June 2025) <https://www.cbc.ca/lite/story/1.7565775?feature=related-link> accessed 26 July 2025.

and surveillance powers of law enforcement and the Canadian Security Intelligence Service (CSIS).

However, the necessity of modernizing to the Criminal Code cannot justify the violation of citizens' rights, including privacy.

Therefore, the provisions that raise such concerns deserve more attention and discussion from Parliament and shall be further analyzed here.

The first provision that stands out is clause 158, which amends section 487.012 of the Criminal Code[5]. It allows a peace officer or a 'public officer' to make a demand for information of any "person who provides services to the public"[6].

Right away, there is a new and ambiguous term in federal law: public officer. According to clause 156, it refers to a "public officer who is appointed or designated to administer or enforce a federal or provincial law" and whose duties include the enforcement of any Act of Parliament.

The ambiguity is evident. Bill C-2 uses the new term in the definition that is created to describe it. Thus, the term itself, public officer, remains undefined, due to this paradoxical nature of what came first, the term or its definition.

Leaving that obstacle aside, the definition of 'public service providers' also raises an issue: its limitless possibilities. As currently written, warrantless information demands can be made to anyone — in essence, even the bakery that provides bread to the City Council — because the term 'person' is undefined; therefore, it applies to both natural persons and legal entities.

This lack of boundaries is confirmed by officials who state that the bill's definition is indeed sweeping[7]. As they affirm, this would include not only car rental companies and hotels, but also financial institutions, medical professionals, hospitals, doctors, and so forth[8].

Consequently, this also implies that warrantless demands can be made to internet service providers (ISPs) and companies that provide services to political parties. That will include disclosing information to opposition political parties, raising risks for the integrity of democracy.

[5] N(2).
[6] Idem.
[7] N(4).
[8] Idem.

As University of Ottawa law Professor Michael Geist[9] highlights, this alone could justify a constitutional challenge to the bill, given its broad scope.

Clause 158[10] allows a peace officer or 'public officer' to demand information from an unlimited number of individuals and organizations regarding whether a service is being provided or has been provided to any subscriber, client, account, or identifier. If confirmed to be positive, it also requires the information that the provider possesses or controls concerning said subscriber, client, account or identifier, including transmission data, and the location where the services are provided in Canada or abroad, and the date the services began or the period of time it was provided.

It is important to stress that Bill C-2 also introduces a new definition of subscriber information. Clause 157[11], which amends section 487.011 of the Criminal Code, encompasses the information the subscriber or client provided to receive the service, such as their name, pseudonym, address, telephone number and email address, the identifiers assigned to that person, and information on the service provided. So, in a very real scenario, a 'public officer' could ask a doctor for a patient's records or a financial institution for a client's finances, regardless of the sensitivity of the information, and the providers would be expected to comply with such demands made without any warrant or judicial oversight.

Schedule 1 of the Personal Information Protection and Electronic Documents Act (PIPEDA) is clear, at clause 4.3.4, that any information can be sensitive depending on the context and that some, such as medical and income records[12] almost always are. However, Bill C-2 does not limit in any way the information to be provided, implying sensitive information could be disclosed as any other.

Additionally, clause 158 establishes that providers of services to the public also reveal the name or identifier of any other that also provides or has provided services to that subscriber, client, account or identifier[13], creating a system that feeds back in itself. That would allow a general practitioner to [be required to] disclose a person's psychologist as a source of information. Leaving the law aside, the ethical boundaries of such disclosure are jeopardized, as are the professional's legislated obligations to maintain patient confidentiality.

[9] Geist M, 'Lawful Access on Steroids: Why Bill C-2's Big Brother Tactics Combine Expansive Warrantless Disclosure with Unprecedented Secrecy - Michael Geist' (20 June 2025) <https://www.michaelgeist.ca/2025/06/lawful-access-on-steroids/> accessed 23 June 2025.

[10] N(2).

[11] Idem.

[12] Branch LS, Personal Information Protection and Electronic Documents Act 2000 [S.C. 2000, c. 5].

[13] Idem.

With such a wide array of providers from whom information could be demanded, and the broad scope of the information itself, it would be reasonable to expect that the conditions for making such demands would be restricted to a few well-established situations or at least judicial oversight; but that is not the case. Pursuant to clause 158[14]of Bill C-2, a peace officer or 'public officer' merely needs to meet the very low threshold of 'reasonable grounds' that an offence under *any* Act of Parliament has been *or will be* committed, and that the requested information will assist in the investigation.

As Professor Michael Geist[15] describes it, "this is the lowest possible standard and the broadest possible scope extending far beyond just the Criminal Code." There is a clear incompatibility between the extent of the powers granted to law enforcement and appointed 'public officers' and the low threshold they must meet.

Beyond that is a real concern that Bill C-2 creates a system that is based on a lack of transparency, and reinforces that demands should be veiled by secrecy. That is because clause 158[16] allows for the non-disclosure of a demand, its existence, or some or all of its contents, for a period of up to one full year of its receipt by any and every person that provides services to the public. Similar to secret FISA court orders issued under the USA PATRIOT Act, Bill C-2 allows that information requests shall be kept secret by providers, including from the subscriber, client, account, or identifier it refers to.

As Geist[17] once more highlights, Canadians could be kept in the dark not only on an individual basis, but also in terms of the overall scope of the demands.

At the same time, clause 164 of the bill amends section 487.0195(2) of the Criminal Code to create a system that encourages the voluntary disclosure of information — without liability or responsibility, thus with impunity. The bill establishes that not even an information demand is required for the disclosure of information if law enforcement asks a person to provide it voluntarily, when that information is legally within its possession.

Law enforcement can then receive and act upon the requested information, without having to obtain a production order or warrant, with the provider shielded from any criminal or civil liability

[14] Idem.

[15] Geist M, '"Big Brother Tactics": Why Bill C-2's New Warrantless Disclosure Demand Powers Extend Far Beyond Internet and Telecom Providers' (*Michael Geist*, 18 June 2025) <https://mgeist.substack.com/p/big-brother-tactics-why-bill-c-2s> accessed 26 July 2025.

[16] N(2).

[17] N(8).

for having divulged the requested information. Geist[18] describes this as a safe harbor for providers.

For all those reasons, it is surprising that the Charter Statement prepared by the Department of Justice to inform public and Parliamentary debate on Bill C-2[19] concluded that the Bill is consistent with section 8 of the Canadian Chart of Rights and Freedoms[20], which establishes Canadians' right to be secure against unreasonable state overreach in general, and against unreasonable search and seizure in particular. However, as the Charter Statement itself declares, "it is not intended to be a comprehensive overview of all conceivable Charter considerations"[21], and so it is of utmost importance that Bill C-2's impact on privacy and human rights be explored in depth during the Parliamentary study.

In that sense, it is necessary to demonstrate the incompatibility of Bill C-2 with the national legal framework around the right to privacy.

A Clash with the Right to Privacy in Canada

Bill C-2 stands out for its provisions regarding the expansion of lawful access to information, which has sparked controversy.

The core issue revolves around whether the provisions envisioned by the bill to provide law enforcement and the Canadian Security Intelligence Service (CSIS) with timely access to data and information — accord with the right to privacy under the legal framework.

The Bill has garnered support from many of Canada's police chiefs, who argue that warrantless demands would collect only minimal information that can be essential in an investigation. Former director of CSIS, Richard Fadden, has publicly stated that a phone book once allowed police "to do more or less the same"[22]. However, upon further analysis, it is evident that the provisions in Bill C-2 go far beyond collecting the bare minimum information, and constitute surveillance practices. As Bill C-2 is written, the demands that can be made, without judicial approval, include *any* information, including transmission data[23], in relation to *any* subscriber, client, account, or identifier from *any* provider of services to the public.

[18] Idem.

[19] Government of Canada D of J, '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 - Charter Statement' (19 June 2025) <https://www.justice.gc.ca/eng/csj-sjc/pl/charter-charte/c2_2.html> accessed 26 July 2025.

[20] Legislative Services Branch, Constitution Act 1982 1982.

[21] N(18).

[22] N(4).

[23] According to s. 487.011 of the Criminal code: "transmission data means data that

As explained by Paul Bernal[24], Professor of Information Technology Law, School of Law at the University of East Anglia in the UK, the various leaks by Edward Snowden revealed new forms of surveillance. Amongst those are the focus of surveillance activities not only on content, but also on metadata and communications data, all of which are included in Bill C-2's provisions. This shift arises not because of a desire to protect privacy, but because metadata and communications data can be just as revealing, and more easily analyzed and processed[25].

Furthermore, these new surveillance practices described by Professor Bernal, also work alongside commercial data gatherers — entities, such as private companies and data brokers that access not only the raw data, but the profiling and analysis methods of commercial operators[26]. Once more, Bill C-2 allows demands to any provider and any information they have at their disposal, which would include commercial companies such as social media, search engines, ISPs, and data brokers — but also grocers, public libraries, car rental companies, veterinarians, and any other business that 'provides service' to the public.

As Tim McSorley, the national coordinator of the International Civil Liberties Monitoring Group[27], points out, the Bill's unclear language and boundless information demands are ripe for abuse. Thus, the argument that the bill would only allow the collection of 'bare minimum information' is misleading and unfounded.

On the contrary, what is evident is that Bill C-2 allows for the sweeping expansion of domestic surveillance by law enforcement and CSIS. As such, it undermines "more than a decade of Canadian privacy-related jurisprudence"[28].

The bill's provisions that facilitate so-called 'lawful access' to information directly clash with the right to privacy established by the Personal Information Protection and Electronic Documents

(a) relates to the telecommunication functions of dialing, routing, addressing or signaling;

(b) is transmitted to identify, activate or configure a device, including a computer program as defined in subsection 342.1(2), in order to establish or maintain access to a telecommunication service for the purpose of enabling a communication, or is generated during the creation, transmission or reception of a communication and identifies or purports to identify the type, direction, date, time, duration, size, origin, destination or termination of the communication; and

(c) does not reveal the substance, meaning or purpose of the communication. (données de transmission)"

Criminal Code 1985 [C–46].

[24] Bernal P, 'Data Gathering, Surveillance and Human Rights: Recasting the Debate' (2016) 1 Journal of Cyber Policy 243.

[25] Idem.

[26] Idem.

[27] N(4).

[28] Idem.

Act (PIPEDA)[29] and the Supreme Court of Canada ruling in *R. v. Spencer*[30], for the following reasons.

PIPEDA, which was enacted in 2000, establishes limited scenarios, or conditions, for the disclosure of personal information without the knowledge or consent of the individual it refers to, and none have the complete absence of oversight.

According to section 7(3)(c) of PIPEDA, this type of disclosure is only allowed if "required to comply with a subpoena or warrant issued or an order made by a court, person or body with jurisdiction to compel the production of information, or to comply with rules of court relating to the production of records"[31]. It also requires that the requester must be a government institution or part of one that has lawful authority to obtain the information[32]. Therefore, judicial oversight is required, and no warrantless demand can be made under PIPEDA.

By contrast, as currently written, Bill C-2 does not impose any restriction on the information to be furnished to peace or public officers, even when the data might be sensitive. Clause 164 of Bill C-2 reinforces that no production order, warrant, or information demand is necessary for the disclosure of information by any provider of services to the public, that is, a voluntary disclosure.

More chilling yet is that Bill C-2 ensures a system absent of liability for those who disclose the information.

It must also be remembered that section 8 of the Canadian Charter of Rights and Freedoms establishes the right against unreasonable search and seizure[33]. These provisions were further analyzed in the *R v. Spencer* ruling in 2014 in which the Supreme Court of Canada (SCC) ruled that a request made by law enforcement to disclose information voluntarily amounts to a search[34], say for example, subscriber information from an ISP. As such, it must be reasonable to be lawful.

Upon analysis, the Court rightfully concluded that, although law enforcement might ask for information, they do not have the authority to compel compliance with their request, and so, they do not qualify as a lawful authority under s. 7(3)(c)(1) to obtain said information[35].

[29] N(12).

[30] *R v Spencer* [2014] Supreme Court of Canada 2014 SCC 43.

[31] N(12).

[32] Idem.

[33] N(20).

[34] *Idem*, para. 66.

[35] *Idem*, para 65.

According to the *Spencer* decision, PIPEDA only allows the disclosure of information upon the fulfilment of certain requirements, including the indication of lawful authority, and neither PIPEDA nor the Criminal Code create any search and seizure powers[36].

The Court's decision[37] in no way diminishes s. 7(3)(e) of PIPEDA, which allows for personal information to be disclosed or collected in exigent circumstances. However, Bill C-2 implies that peace or public officers would not be allowed to use the urgency of the situation as a reason for a lawful demand, given that clause 158(4) clearly states that the "time specified in the demand is to be not less than 24 hours"[38].

Consequently, the Supreme Court of Canada confirmed that a warrantless search is presumptively unreasonable[39] — something that directly clashes with the warrantless and broad information demands allowed by Bill C-2.

As Christopher Cornell, an independent researcher, highlights[40], there are some noticeable practical effects to the ruling of *R. v. Spencer*. First, it is necessary for law enforcement to have a warrant to obtain Canadians' personal information. Second, the warrant is dispensed with only when the information is required to help resolve an emergency that threatens the life, health, or security of an individual. Third, a warrant is necessary in all cases where the goal is to obtain personal information about Canadians' online activities.

In that sense, the new bill's provisions not only go against the legal requirements established for an information demand, but also Canadians' reasonable expectation of privacy regarding their information, including in the online environment, as highlighted by the Court.

As the SCC argues: "the disclosure of this information will often amount to the identification of a user with intimate or sensitive activities being carried out online, usually on the understanding that these activities would be anonymous"[41].

This reasonable expectation of privacy was reinforced by the Supreme Court in the ruling of in 2024[42]. This landmark decision states that although an IP address, as a "collection of numbers",

[36] *Idem*, para. 71.

[37] *Idem*, para. 74.

[38] N(2).

[39] *Idem*, para. 68.

[40] Cornell C, *'R. v. Spencer* and the Affirmation of Internet Privacy Rights in Canada' (2014) 20 Law and Business Review of the Americas, pp. 656-657.

[41] *Idem*, para. 66.

[42] *R v Bykovets* [2024] Supreme Court of Canada 2024 SCC 6.

is not of interest to law enforcement, it tends to reveal information about a user's online activity[43], and it "plays an integral role in maintaining privacy on the internet"[44].

As the Court states, this information can be deeply personal[45], including the user's lifestyle, personal choices, and intimate details[46], and therefore links to the user's identity, although it does not reveal it[47].

Bertina Lou, legal fellow at Just Access and student at University of Ottawa's English Common Law Program, describes an IP address as the first digital breadcrumb, because even if they reveal "little information by themselves […] when combined with other information, [they] have the potential to reveal a user's core biographical information"[48], similar to the subscriber information discussed in *R. v. Spencer*.

The ten years between the *Spencer* and *Bykovets* rulings saw an increase in the number of ways individuals can possess, disclose and disperse personal information online, and as a reflection, society grew accustomed to informational privacy and digital self-determination rights[49]. Therefore, the Supreme Court ruled that IP addresses attract a reasonable expectation of privacy and "given […] serious privacy concerns, the public's interest in being left alone should prevail over the relatively straightforward burden imposed on law enforcement"[50].

In that context, the SCC concluded that a request by the state for an IP address constitutes a search under s. 8 of the Charter[51] and that, as such, in order to not subject individuals to an unreasonable search, law enforcement must obtain a warrant granting authorization[52].

In other words, the expectation of privacy that Canadians have online is safeguarded by the requirement to obtain judicial pre-authorization. Thus, once more, it is evident that the warrantless demand of information permitted in Bill C-2 is incompatible with the Canadian legal framework on privacy. This also aligns with society's expectations that, in this highly digitalized

[43] *Idem*, para. 41.
[44] *Idem*, para. 90.
[45] Idem.
[46] *Idem*, para. 43.
[47] *Idem*, para. 80.
[48] Lou B, 'R. v. Bykovets: An Affirmation of Canadians' Right to Informational Privacy' 22 Canadian Journal of Law and Technology, p. 82.
[49] *Idem*, p. 87.
[50] N(43), para. 90.
[51] *Idem*, para. 92.
[52] N(49), p. 83.

world, private entities and other "third parties possessing more personal information than ever might owe individuals an obligation to preserve their privacy"[53].

So, the *R. v. Bykovets* decision acts as a new "robust defence affirmation of privacy and trust in the digital space" for Canadians, as observed by Anil Kappor[54] from the Canadian Civil Liberties Association.

For these reasons, the thesis established in *R. v. Spencer*, later reinforced by *R. v. Bykovets*, stands as the baseline for interpreting the right to privacy in Canada. And so, while those precedents must be observed by new legislation, for the establishment of a cohesive legal framework that protects its citizens and avoids any conflict or risk to their privacy, Bill C-2's provisions on 'lawful access to information' seem to ignore it.

Bill C-2: A Defiance to International Human Rights and Global Trends

It is clear, to this point, that Bill C-2 is far from being cohesive or compliant with the national legal framework on privacy rights, due to the provisions contained in Part 14. Similarly, it neither aligns with the international human rights framework nor the global trends on surveillance practices. This incompatibility shall now be exposed.

In September 2013, the "Necessary and Proportionate Principles" or "13 Principles" or "International Principles on the Application of Human Rights to Communications Surveillance"[55] were launched at the UN Human Rights Council in Geneva.

Born out of a year-long consultation process between civil society, privacy and technology experts, the principles delineate the international human rights law requirements to governments in the digital era[56]. Most notably, "they speak to a growing global consensus that modern surveillance has gone too far and needs to be restrained"[57], and provide a framework to help evaluate whether current or proposed surveillance laws and practices, such as Bill C-2, are consistent with human rights.

[53] *Idem*, p. 87.

[54] McNab A, 'Police Need Search Warrant to Get IP Address, Rules Supreme Court of Canada in 5-4 Split Decision' (*Canadian Lawyer*, 1 March 2024) <https://www.canadianlawyermag.com/practice-areas/criminal/police-need-search-warrant-to-get-ip-address-rules-supreme-court-of-canada-in-5-4-split-decision/384148> accessed 9 August 2025.

[55] Necessary & Proportionate, 'Necessary & Proportionate on the Application of Human Rights to Communications Surveillance' <https://necessaryandproportionate.org/images/np-logo-og.png> accessed 26 July 2025.

[56] Idem.

[57] Idem.

Considering that international human rights have a global binding effect, and that the principles apply to surveillance conducted within Canada or extraterritorially, regardless of their purpose, and not only to the state's obligation to respect and fulfil individual human rights but also to protect them from abuse by non-State actors, Bill C-2 shall be evaluated for compliance[58].

First, it is necessary to clarify that communications surveillance is a concept understood as the "monitoring, intercepting, collecting, obtaining, analyzing, using, preserving, retaining, interfering with, accessing or similar actions taken with regard to information that includes, reflects, arises from or is about a person's communications in the past, present, or future"[59].

For that concept, communications include all activities, interactions, and transactions by electronic means, for example, an IP address.

In light of that — and considering communications are inserted in the broad category of any information on a subscriber, client, account, or identifier that can be disclosed to a public or peace officer — the conduct and actions allowed under Bill C-2's provisions on so-called lawful access to information fall within the concept of communications surveillance.

As such, Bill C-2 should observe all 13 principles articulated in the Necessary and Proportionate Principles. Given Bill C-2's striking incompatibility, however, some principles deserve extra attention.

One is the legality principle, which establishes that a law must meet a standard of clarity and precision "that is sufficient to ensure that individuals have advance notice of and can foresee its application"[60].

However, as already exposed, Bill C-2 includes ambiguous and paradoxical terms, such as 'public officer', and obscure provisions, for example, regarding the limits of who constitutes providers of public services. Additionally, it is written in a way that fosters secrecy towards the affected individuals. For instance, section 158 establishes mandates non-disclosure for a period of up to one year. Therefore, non-compliance with the legality principle is evident; yet, it is not the only case. The clause does not guarantee transparency about the scope and use of the surveillance practices envisioned in Bill C-2, thus also putting the transparency principle in jeopardy[61]. In

[58] Necessary & Proportionate, 'International Principles on the Application of Human Rights to Communications Surveillance' (2014) <https://necessaryandproportionate.org/files/en_principles_2014.pdf> accessed 26 July 2025, p. 3.

[59] *Idem*, p. 4.

[60] *Idem*, p. 7.

[61] *Idem*, p. 10.

addition, there is no clear restriction on how the information gathered can be later used by surveillant officers.

More significantly, Bill C-2 is in direct conflict with the competent judicial authority principle. Clause 164, potentially the most controversial provision of the bill, states that "for greater certainty, no production order or warrant, or information demand […] is necessary for a peace or 'public officer' to receive information"[62]. However, the principle establishes, in a clear opposite direction, that any determination or request related to communications surveillance must be made by a competent judicial authority that is both independent and impartial[63].

The principle clearly states that this authority has to be separate from those conducting the surveillance, thus ruling out the possibility of a peace or 'public officer' being considered as such[64] — another principle Bill C-2 does not comply with in regards to lawful access to information.

Similarly, the right of the individual to be notified of the decision that authorizes surveillance is not respected. First, because a decision is not necessary. Secondly, because the non-disclosure clause does not fit into the exceptions to delay the notification envisioned by the principle, which are: ***(i)*** notification would jeopardize the purpose of surveillance or there is imminent danger, ***(ii)*** is authorized by a competent judicial authority, and ***(iii)*** notification as soon as the risk is lifted as recognized by the same authority[65]. As Bill C-2 is written, no such risks justify non-disclosure, just the sheer arbitrariness of the surveillant officer.

Moreover, Bill C-2 empowers peace or public officers to conduct mass surveillance, both online and offline, without any kind of oversight or adequate scrutiny. This sweeping power also goes against the principle of public oversight, which requires the establishment of independent mechanisms to ensure transparency and accountability[66].

Additionally, the proportionality principle described in the Necessary and Proportionate Principles and reflected in Canadian privacy laws and jurisprudence establishes that, before communications surveillance is envisioned, other less invasive techniques have to be exhausted or be considered futile. Bill C-2 lacks any requirement to take the least invasive option[67].

[62] N(2).
[63] N(59), p. 9.
[64] Idem.
[65] *Idem*, p. 9.
[66] *Idem*, p. 10.
[67] *Idem*, p. 8.

In light of all the above, it is evident that Bill C-2 is not in accordance with the international human rights framework set out in the 13 Principles, and thus, requires revision and modifications before becoming law.

Bill C-2's shortcomings are also apparent when analyzed from the perspective of other human rights frameworks and global trends on this matter, including the leading European framework and jurisprudence.

The European Convention on Human Rights (ECHR), also known as the Convention for the Protection of Human Rights and Fundamental Freedoms, is a supranational framework that applies to all signatories, namely, the member states of the Council of Europe[68]. Canada is an observer state to the ECHR.

It is important to stress that the Council is composed of 46 (forty-six) member states, not exclusive to the European Union[69]. Although not a member state, Canada is an observer state, which implies it can cooperate with the Council, willingly accept its guiding principles including those of human rights, and send observers to expert committees, conferences of specialized ministers, and the Parliamentary Assembly[70].

Its status as an observer state puts Canada in a special position to monitor the development of the works of the Council, and thus be inspired by their innovative developments in the human rights framework, in part due to the evolving interpretation of the Convention by the European Court of Human Rights (ECtHR), its enforcer per its Article 19[71].

For those reasons, the ECtHR's jurisprudence acts as a path towards effective and legal oversight, balancing individuals' human rights against the necessities of safety measures by the government. For those reasons, it shall be brought into light.

Before any case is presented, it is necessary to present the two rights from the ECHR that are at the center of the discussion on mass surveillance practices.

Article 8 establishes that every person has the right to respect for his or her private and family life, including their home and correspondence. Moreover, the Convention makes it clear that there shall be no interference by a public authority with the exercise of such a right, unless

[68] European Court of Human Rights, European Convention on Human Rights 1950.

[69] Council of Europe, '46 Member States of the Council of Europe - Portal' (*Portal*) <https://www.coe.int/en/web/portal/members-states> accessed 17 August 2025.

[70] Council of Europe, 'Canada - Observer State' (*Portal*) <https://www.coe.int/en/web/portal/canada> accessed 17 August 2025.

[71] N(67), p. 15.

authorized by law and necessary under special circumstances such as interests of public safety, prevention of disorder or crime, or the protection of others' rights[72].

Article 10 guarantees the right to freedom of expression. Similar to the Charter-protected rights that Canadians enjoy, this is not an absolute right since its exercise may be subject to formalities, conditions, restrictions, or penalties as prescribed by law[73].

In light of those articles, two ECtHR rulings shed light on the limits of mass surveillance and the overstepping committed by Bill C-2 in regards to human rights.

In January 2016, the European Court ruled on the case of *Szabó and Vissy v. Hungary*, which concerned Hungarian legislation on secret anti-terrorist surveillance. Although the Court recognized that it was expected that governments would resort to cutting-edge technologies (including mass surveillance of communications) to fight against present-day terrorism, the legislation had violated Article 8[74] – the right to privacy. The reasons why reveal a surveillance system similar to the one established by Bill C-2.

In essence, the Hungarian legislation did not provide sufficient safeguards to avoid abuse[75] or to provide individuals with adequate protection against arbitrary interference[76]. The Court noted that the scope of surveillance could apply to virtually anyone in Hungary[77]. As in the case of Bill C-2, where information can be gathered from any person, subscriber, client, account or identifier, Hungary's legislation employed an overly broad concept of targets, which implied that it could enable strategic and large-scale interception[78].

Furthermore, the likelihood of abuse also arises from the lack of strict necessity of the surveillance measures or safeguards in the legislation. Most notably, from the absence of prior judicial authorization as a requirement for the interception and a clear provision on the frequency of renewals of warrants issued by the Executive, whose oversight was deemed "eminently political and inherently incapable of ensuring the requisite assessment of strict necessity"[79].

[72] *Idem*, p. 10.

[73] *Idem*, p. 12.

[74] European Court of Human Rights, 'Factsheet Mass Surveillance', p. 3.

[75] Idem.

[76] European Court of Human Rights, 'Information Note on the Court's Case-Law 192 - Szabó and Vissy v. Hungary - 37138/14' <https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22002-10821%22]}> accessed 13 July 2025.

[77] N(74), p. 3.

[78] N(76).

[79] Idem.

Nevertheless, the Court established that prior judicial control could be temporarily waived in situations of extreme urgency, and it recognized that "any surveillance measures authorized *ex ante* by a non-judicial authority had to be subject to a *post factum* judicial review"[80].

As with other aspects, Bill C-2 does not fulfill the requirement for judicial oversight *ex ante*, or even *post factum* review.

Finally, the ECtHR ruling reinforced the obligation for domestic laws to provide a judicial-control mechanism that can be triggered by the target(ed) person, once notified of the surveillance measures applied[81]. Again, the non-disclosure clause of Bill C-2 hinders the implementation of such a safeguard.

In May 2021, the Grand Chamber of the ECtHR set the standards for bulk interception regimes in the ruling of *Big Brother Watch and Others v. United Kingdom*[82], and provided even more clarity about surveillance practices. In this decision, the Court held that both Article 8 and 10 of the ECHR were violated.

It shall be noted that bulk interception is a specific type of surveillance. Conceptually, it is an untargeted surveillance practice that "may operate by tapping into and storing large volumes of data drawn from the bearers carrying Internet communications"[83]. Although considered by the Court not in and of itself impermissible under the ECHR, it is not limitless[84]. Governments enjoy a wide margin of latitude regarding their decisions on what is necessary to guarantee national security[85]; however, the surveillance regime has to be subject to end-to-end safeguards[86].

Under that premise, the Court revealed the reasons why the surveillance regime of the United Kingdom (UK) violated Article 8.

First, bulk interception regimes require, at the domestic level, an assessment of their necessity and proportionality at every stage of the process[87].

Secondly, judicial authorization *ex ante* is not by itself necessary or sufficient to demonstrate compliance with Article 8 of the ECHR. Conversely, independent authorization is required for surveillance practices from the very first stage, when the object and scope of the interception

[80] Idem.

[81] Idem.

[82] Zalnieriute M, 'Big Brother Watch and Others v. the United Kingdom' (2022) 116 American Journal of International Law 585.

[83] European Court of Human Rights and European Union Agency for Fundamental Rights, 'Mass Surveillance - ECtHR and CJEU Case-Law', p. 1.

[84] N(82), p. 586.

[85] Idem.

[86] N(74), p. 5.

[87] Idem.

are being defined[88]. And, considering bulk interception is untargeted and subsequent notification of individuals is thus not envisioned for such a system[89], *ex post facto* review and supervision are also required.

Oversight is yet again reinforced as a key safeguard for human rights in regards to mass surveillance.

So, the Court considered that the authorization of the bulk interception by the Executive, combined with the absence of search terms informing the type of communication sought after in the warrant, and no prior authorization for using search terms that linked to an individual, constitutes a violation of the right to privacy under the ECHR framework[90].

In other words, broad access to data on individuals without oversight constitutes a flagrant violation of privacy. This is exactly the powers Bill C-2 provides to peace officers and public officers.

Nonetheless, in the Hungarian case, the Court also ruled a violation of the right to freedom of expression – Article 10 of the ECHR – due to a lack of sufficient safeguards for confidential journalistic material[91].

The ECtHR rightfully recognized that there are "no requirements either circumscribing the intelligence services' power to search for confidential journalistic or other material (for example, by using a journalist's email address as a selector), or requiring analysts, in selecting material for examination, to give any particular consideration to whether such material was or might be involved"[92]. Once, not only data, but also metadata can be furnished and analyzed, journalistic confidentiality is put at risk and, with it, the confidentiality of sources and the very freedom of expression of the press[93].

Thus, being similar to the UK's bulk interception scheme in that sense, Bill C-2 can also foster a violation of the right to freedom of expression.

Therefore, the issue affects not only individuals' privacy to their information, but also the protection and safety of professional confidentiality, which goes beyond that of journalists to

[88] Idem.

[89] European Court of Human Rights, 'Information Note on the Court's Case-Law 221 - Big Brother Watch and Others v. the United Kingdom - 58170/13, 62322/14 and 24960/15' <https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22002-12080%22]}> accessed 17 August 2025.

[90] N(74), p. 5.

[91] Idem.

[92] N(92).

[93] Idem.

sources, including also lawyers to clients and doctors to patients. Consequently, Bill C-2 does not simply violate human rights from a legal perspective, but also from an ethical one.

Unfortunately, these are not the only shortcomings of the Bill in regards to the European framework and jurisprudence about mass surveillance.

Bill C-2 is also incompatible with the Charter of Fundamental Rights of the European Union (CFREU). This document, which is binding on the member states of the EU with equal legal power to an EU Treaty, is responsible for enshrining the most important personal freedoms and rights of citizens across the region[94].

The CFREU was declared in 2000 and came into force in 2009, promoting human rights within the EU as a goal[95]. In the matter of mass surveillance, two of those rights are constantly debated.

Article 7 establishes the right of respect for private and family life, including personal home and communications[96]. In writing, this provision of the CFREU is essentially a copy of the first part of Article 8 of the ECHR, which demonstrates a reiterated desire and goal to protect one's privacy in Europe.

Article 8 of the CFREU reinforces this by establishing the right to the protection of personal data concerning an individual[97]. More particularly, this provision guarantees that data must only be processed fairly and for specified purposes on a legitimate basis laid down by law, such as consent, and that the data subject has the right to access the data collected and the right to have it rectified[98].

Not surprisingly, the CFREU makes compliance with the rules of Article 8 conditional on control by an independent authority[99]. By contrast, Bill C-2 does not envision any oversight mechanism regarding the so-called lawful access to information; thus, an incompatibility is once again flagrant.

Nevertheless, it is not the only one. The Court of Justice of the European Union (CJEU) issued two emblematic rulings, known as *Schrems I* and *Schrems II*, regarding the invalidation of an

[94] Citizensinformation.ie, 'Charter of Fundamental Rights' <https://www.citizensinformation.ie/en/government-in-ireland/european-government/eu-law/charter-of-fundamental-rights/> accessed 22 August 2025.

[95] Idem.

[96] Charter of Fundamental Rights of the European Union 2012 [2012/C 326/02].

[97] *Idem.*

[98] *Idem.*

[99] Idem.

adequacy decision due to the USA's governmental surveillance practices and the risk they pose to data collected in the EU.

Before delving deeper into each case, it is first necessary to briefly tackle the concept of an adequacy decision and its procedure. According to the General Data Protection Regulation (GDPR)[100], the ruling legal document on data protection in the EU, the transfer of personal data from the EU to a third country may only occur under certain conditions. The first one is the existence of an adequacy decision per Article 45 of the GDPR. Issued by the European Commission (EC), this decision states that the third country, a territory or one or more specified sectors of that country, must ensure an adequate level of protection to the data. If such a decision exists, no specific authorization for the transfer is required[101].

For that reason, the adequacy decision is the easiest mechanism to govern the international transfer of data out of the EU and a benefit to those who possess it, once in its absence, additional safeguards and derogations are applicable – Articles 46 and 49[102].

In the process of assessing the adequacy of the level of protection, the EC takes into account several elements, including the rule of law, respect for human rights and fundamental freedoms – Article 45(2)[103].

The modification of any of those elements may result in a lower protection of personal data than in the EU, and consequently, adequacy status not being attained, or worse, an existing adequacy status being revoked or not renewed.

This is exactly the subject of the *Schrems I* and *Schrems II* cases. Both rulings reveal how Bill C-2 is a setback in terms of mass surveillance in regards to the right to privacy.

In 2000, the European Commission issued Decision 2000/520, declaring that the United States of America (USA) ensured an adequate level of protection of data, with the Safe Harbour framework.

Upon the shocking revelations of Edward Snowden, in 2013, Maximilian Schrems, then an Austrian student, today a lawyer, lodged a complaint with the Data Protection Commissioner (DPC) – enforcer of the GDPR in Ireland as data protection authority – asking the latter to prohibit

[100] Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) 2016 [2016/679]/

[101] Idem.

[102] *Idem.*

[103] *Idem.*

Facebook Ireland from transferring his personal data to the USA[104]. Schrems argued that, once the data was transferred, it was subject to indiscriminate surveillance and interception on a large scale by the National Security Agency (NSA) and other federal agencies, such as the Federal Bureau of Investigation (FBI)[105]. However, the Commissioner rejected the complaint as unfounded, and Mr. Schrems then brought an action in the High Court of Ireland. The latter, recognizing that the discussion would involve fundamental EU law, referred questions to the CJEU[106], which eventually issued the famous ruling in 2015.

The High Court had already stressed that the right to privacy, under Article 7 of the GDPPR, "would be rendered meaningless if the State authorities were authorized to access electronic communications on a casual and generalized basis without any objective justification based on considerations of national security or the prevention of crime that are specific to the individual concerned and without those practices being accompanied by appropriate and verifiable safeguards"[107].

The CJEU's rationale could also perfectly describe the surveillance regime established by Bill C-2 and its undesired negative effect on the right to privacy of Canadians.

In *Maximilian Schrems v. Data Protection Commissioner*, also known as *Schrems I*, the CJEU stated clearly that the adequacy decision did not contain any finding on existing rules in the USA to limit any interference with fundamental rights of those whose data was transferred out of the EU[108].

In fact, the Court concluded that, in regards to data transferred from member states to the USA, American authorities were able to both access it and process in a way "incompatible, in particular, with the purposes for which it was transferred, beyond what was strictly necessary and proportionate to the protection of national security"[109].

The CJEU once more reinforced that legislation involving interference with the fundamental rights of Articles 7 and 8 of the CFREU must lay down clear and precise rules on the scope and application of surveillance measures, imposing minimum safeguards, for the protection against the risk of abuse or unlawful access to data[110] — criteria that Bill C-2 does not meet.

[104] Case C-362/14 - Maximillian Schrems v Data Protection Commissioner (Court of Justice of the European Union (CJEU)), §28.
[105] *Idem*, §31.
[106] *Idem*, §§29 and 34.
[107] *Idem*, §34.
[108] *Idem*, §88.
[109] *Idem*, §90.
[110] *Idem*, §91.

Therefore, the Court concluded that the essence of the fundamental right to respect for privacy was compromised by "legislation permitting the public authorities to have access on a generalized basis to the content of electronic communications"[111] and declared the adequacy decision invalid[112] — similar to Bill C-2's broad powers and low threshold.

In the following year, 2016, the Privacy Shield framework was developed to replace the invalidated[113] Safe Harbor and overcome its shortcomings.

Although similar to its predecessor in nature, Privacy Shield was a self-certification system based on compliance by US organizations with a set of principles. The scheme included a section to address the use of data transferred from the EU, by US public authorities for national security and law enforcement purposes[114].

In the same year, following the judgment of *Schrems I*, the EC adopted a new adequacy decision, following the Privacy Shield framework – Decision 2016/1250[115].

Nevertheless, a new complaint was lodged by Mr. Schrems to the DPC, once more requesting the suspension of the transfer of his data held by Facebook Ireland to Facebook Inc., in the US, under standard contractual clauses. The DPC escalated the matter to the High Court of Ireland, which eventually referred questions to the CJEU[116].

The judgment of *Data Protection Commissioner v. Facebook Ireland Ltd. and Maximilian Schrems*, known as *Schrems II*, confirmed the understanding of the CJEU of the right to privacy under mass surveillance regimes[117], and shall be further analyzed.

According to the CJEU, the adoption of an adequacy decision is dependent on an adequate level of protection for data, as recognized in Articles 7 and 8 of the CFREU[118] that address the rights of privacy and data protection.

The CJEU then once more recognized that the mere act of communication of personal data to a third party, such as a public authority — a peace or 'public officer' under Bill C-2 — or the

[111] *Idem*, §94.

[112] Idem, §104.

[113] Tzanou M, 'Schrems I and Schrems II: Assessing the Case for the Extraterritoriality of EU Fundamental Rights' (Social Science Research Network, 13 October 2020) <https://papers.ssrn.com/abstract=3710539> accessed 22 August 2025, p. 12.

[114] Idem.

[115] Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems (Court of Justice of the European Union (CJEU)).

[116] N(113), p. 13.

[117] N(114).

[118] *Idem*, §169.

retention or access of data by those parties, regardless of their purpose[119], constitutes interference with the aforementioned fundamental rights. Therefore, limitations on the exercise of such rights may only occur when provided for by law, with a clear scope of limitation[120], which does not happen in Bill C-2.

So, the CJEU establishes a test to assess the proportionality of surveillance measures concerning the compromise of rights: ***(i)*** interference must be strictly necessary; ***(ii)*** the legislation that authorizes interference must lay down clear and precise rules on the scope and application of the measure; and ***(iii)*** the legislation must impose minimum safeguards[121].

If the test is applied to Bill C-2, there is a clear failure of all requirements. Once interference is not proven to be a last resort and strictly necessary, there are ambiguous rules and a broad scope of application, with unlimited targeted individuals and no safeguards such as independent judicial oversight, it is inevitable to conclude that Bill -2 does not fulfill the proportionality requirement.

That is similar to the findings of the CJEU on the surveillance programs of the USA in the case of *Schrems II*. In light of the GDPR and CFREU, the Court held that the law in question did not impose any limitation on the power conferred to implement surveillance programs for foreign intelligence information, nor guarantee non-US persons would not be targeted by such programs[122].

Furthermore, the access to data by US authorities without any judicial review "does not, in any event, delimit in a sufficiently clear and precise manner the scope of such bulk collection of personal data"[123] Thus, the surveillance measures are ruled disproportionate and incompatible with the already disclosed EU Charter rights, leading the CJEU to declare the Privacy Shield adequacy decision invalid[124].

In essence, both *Schrems I* and *Schrems II* confirm that national security, including the protection of national borders, cannot justify broad, unclear and limitless surveillance measures, especially without judicial oversight. Additionally, the rights of individuals to their privacy and to the protection of their data can only be limited under specific conditions, ruled by law, with adequate safeguards.

[119] *Idem*, §171.
[120] *Idem*, §175.
[121] *Idem*, §176.
[122] *Idem*, §180.
[123] *Idem*, §183.
[124] *Idem*, §§ 184 and 203.

In short, as already discussed, Bill C-2 does not comply with such requirements.

Accordingly, it is clear that, in addition to Bill C-2's provisions being incompatible with and in direct violation of the right to privacy established by Canada's legal framework as established by *R. v. Spencer*, it also defies the international human rights framework — a violation of the Necessary & Proportionate Principles —the position of the European Court of Human Rights (ECtHR) and the Court of Justice of the European Union (CJEU).

All of those facts combined can already satisfy an urgent request for review and modification of Bill C-2's current provisions by Parliament, or afterward, if the Bill is enacted as it is, an intervention before the Supreme Court of Canada (SCC).

Nonetheless, it is still necessary in this discussion to shed light on other somewhat unapparent aspects of Bill C-2's provisions: the risks of mass surveillance.

The Risks of Mass Surveillance

Professor Paul Bernal wisely recognizes that surveillance itself[125] is harmful.

It is quite evident, upon analysis, that Bill C-2, if enacted into law, shall produce negative effects that can be far greater than its positive ones. As demonstrated, it violates Canadian's fundamental and human rights to privacy and protection of data, and creates a system of secret, limitless surveillance as well as legal and ethical uncertainty.

But the harmful nature of those surveillance measures goes well beyond those aspects.

As Bernal explains, the menace of surveillance arises from the development of systems and laws that allow data to be gathered. Ideally, surveillance ought to be subject to a balancing exercise between the necessity of the measures and the rights of individuals[126] — which Bill C-2 does not contemplate.

Once a surveillance system is put into place and data is gathered, both are vulnerable to intentional and accidental misuse, loss, and compromise by authorities and others. Vulnerability comes in many forms: misuse, misappropriation, malfeasance, hacking, loss, corruption or error, etc. The risks are especially relevant in the case of mass surveillance because the "systems themselves are vulnerable: build a back door into a system and it is not only those [peace or public officers] who are intended to use it who can use it as a way to access that system"[127].

[125] N(24), p. 250.

[126] *Idem*, p. 251.

[127] *Idem*.

So, considering surveillance can both improve security and damage it and increase risks, additional safeguards are essential to ensure data confidentiality, integrity, and availability (CIA) – known as the information security triad. But, once again, Bill C-2 does not provide for the needed safeguards.

Furthermore, the risks of surveillance are not limited to privacy. As Bernal explains, to impose such a limitation would make the risks of surveillance seem less significant, because there is a clear impact on human rights that goes beyond "the obvious-seeming intrusions into privacy"[128]. This is because privacy not only underpins other rights, but also because of the diffuse way the internet is currently used[129].

In the author's assessment, surveillance impacts other rights in addition to Articles 8 and 10 – right to respect for private and family life, and freedom of expression, respectively – of the European Convention of Human Rights (ECHR).

The less obvious impacts of surveillance can be seen when considering Article 6 of the ECHR[130], which establishes the right to a fair trial, similar to clause 11 of the Canadian Charter of Rights and Freedoms (CCRF)[131]. As Bernal reveals, surveillance can interfere that right by undermining the confidentiality of journalists' communications with their sources and lawyers' correspondence with their clients[132].

However, most strikingly, surveillance can directly and potentially prejudicially influence justice due to the access to information and the ability to use it by both police and prosecuting authorities[133].

The right to freedom of thought, conscience, and religion, established in Article 9 of the ECHR[134] and clause 2 of the CCRF[135], is another aspect impacted by surveillance. This is because surveillance can lead to the identification of an individual's religion, politics, philosophy, language, ethnic origins — all data that could constitute sensitive data under the Canadian legal

[128] *Idem*, p. 252.
[129] *Idem*.
[130] N(68), p. 9.
[131] N(20).
[132] N(24), pp. 255-256.
[133] Idem.
[134] N(68), p. 11.
[135] N(20).

framework — and consequently lead to the monitoring of an individual's online and offline activities and further limit or control such activities, whether individual or in a group[136].

This also implies a potential violation of the freedom of assembly and association under Article 11 of the ECHR[137], clause 2 of the CCFR[138] and Section 2 of the Canadian Charter of Rights and Freedoms. As Professor Bernal notes, surveillance can be significantly dangerous when communications, mainly the internet, are used to coordinate meetings and assemble online or offline, as it allows not only the monitoring of these activities, but also the ability to prevent meetings from happening, and target and identify individuals or groups[139].

This is, of course, a risk to democracy itself. It goes beyond freedom of assembly, once it is closely connected to the right to freedom of expression.

In that sense, according to Bernal, the "knowledge of the existence of surveillance […] also tends to produce more conformist behaviour, which would impact directly on willingness to exercise freedom of both assembly and association and hence those freedoms themselves"[140].

Finally, surveillance also impacts the prohibition of discrimination, guaranteed by Article 14 of the ECHR[141], clause 15(1) of the CCFR[142], and various Canadian human rights and labor laws. This is due to surveillance being able to identify key details of an individual, leading to a profile of who they are — age, religion, nationality, hobbies, associations, etc. — which can then be used by third parties to make decisions and control options available to that individual[143].

Combining surveillance and profiling can automate discrimination. For example, an automated process or filter used by law enforcement can be programmed flag individuals to surveil more closely, due to race, religion or other[144] reasons.

Nevertheless, the risks of mass surveillance are not restricted to an outright violation of Canadian's fundamental rights and international human rights.

[136] N(24), p. 253.
[137] N(68), p. 13.
[138] N(20).
[139] N(24), p. 256.
[140] Idem.
[141] N(68), p. 13.
[142] N(20).
[143] N(24), pp. 257-258.
[144] *Idem*, p. 258.

Clause 183[145] of Bill C-2 allows the Minister to make arrangements to enforce a foreign state's decision to compel the production of information, such as transmission data or subscriber information, to an individual in Canada. So, although not explicitly, the bill provides a way for new and expanded data-sharing with the United States and other countries[146], as clarified by Kate Robertson from the Citizen Lab.

It is relevant because of the potential impact of Bill C-2 on data-sharing obligations between Canada and the United States, especially considering that the bill is being tabled at a time when both countries have entered into negotiations on matters of trade and security[147].

More precisely, regarding the current negotiations on the 2AP Treaty and the CLOUD Act, which shall be explained further.

The Second Additional Protocol to the Budapest Convention, also known as 2AP, is a law enforcement data-sharing treaty to which the United States is already a signatory. It allows law enforcement to bypass existing mutual legal assistance frameworks between countries, expediting international data-sharing and increasing the volume of requests[148].

In other words, the treaty would allow a signatory country to "seize, share, retain, and use potentially large volumes of private data from public or private entities in respect of both digital and non-digital information"[149].

It has already been thoroughly discussed that the broad powers of access to an individual's information and other mass surveillance measures are a critical threat to fundamental human rights such as privacy.

In that sense, the 2AP Treaty, as Robertson points out, can propel the elimination and reduction of safeguards that are critical to mutual legal assistance by law enforcement.

Similarly, the CLOUD Act, an acronym for Clarifying Lawful Overseas Use of Data Act, is a bilateral data-sharing agreement between Canada and the United States under the latter's legislation[150].

[145] N(2).

[146] Robertson K, 'Unspoken Implications: A Preliminary Analysis of Bill C-2 and Canada's Potential Data-Sharing Obligations Towards the United States and Other Countries' (Citizen Lab, University of Toronto 2025) <https://citizenlab.ca/2025/06/a-preliminary-analysis-of-bill-c-2/> accessed 26 July 2025.

[147] *Idem.*

[148] *Idem.*

[149] *Idem.*

[150] *Idem.*

If signed into law, it would "expose public and private entities in Canada to data demands directly from U.S. intelligence agencies, without the involvement of the Canadian Courts"[151].

Once again, it has been much discussed that without any safeguards, mass surveillance powers granted by Bill C-2 incur a violation of both national and international legal frameworks on the right to privacy and more, and therefore, such facts may not be disregarded by Parliament.

For example, Robertson highlights the risk of information on a certain individual who has obtained services from an abortion clinic in Canada being disclosed to American law enforcement in a state where, since the Dobbs decision of the US Surpreme Court[152], such an act is considered a crime[153].

Therefore, although both 2AP and the CLOUD Act are envisioned to provide reciprocal data-sharing and may result in significant constitutional and human rights risks, Bill C-2 opens the door to US authorities gaining access to a broad range of sensitive and other information to an unlimited number of targets, without judicial oversigh;, and the Treaty and CLOUD Act would allow all that to be shared internationally.

So, on Canada's side, it is like data-sharing became a borderless process between the country and the USA. Conversely, from the latter's perspective, it is like there is a digital wall in place, where they could benefit from data shared from Canada, but not have the reciprocal duty to disclose equivalent information, due to their own national safeguards and interests.

This puts Canada in a virtual state of data subordination to the USA, a position that challenges its own data sovereignty.

Lastly, Bill C-2 might also result in great financial risks in two different ways.

First, there is the risk of numerous financial compensations from the government to individuals impacted by the state's information-sharing practices, as occurred in the Maher Arar case.

As Robertson points out, "Canadian authorities know first-hand the tragic consequences that is inappropriate data sharing with foreign authorities can inflict even on innocent persons"[154].

In short, the story is as follows. In 2002, Maher Arar, a Canadian citizen, was arrested by American authorities at New York City's JFK airport, while changing planes to return to Canada after visiting

[151] *Idem.*

[152] *Dobbs v. Jackson Women's Health Organization*, 597 U.S. 215, www.supremecourt.gov/opinions/21pdf/19-1392_6j37.pdf

[153] *Idem.*

[154] *Idem.*

his wife's family in Tunisia[155]. He was held in the USA for 12 days and then secretly transferred to Syria, where he endured degrading and inhumane conditions, being interrogated and tortured for a year. Mr. Arar was then released without charge and returned home to Canada in 2003[156].

The reasons for his first arrest in the USA are at the core of the issue and were explored by the Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, established in 2004 by the Canadian government to investigate the acts that led to his rendition to torture[157].

In 2006, Commissioner O'Connor, the person mandated to conduct such the inquiry, released a report that confirmed "the Royal Canadian Mounted Police (RCMP) provided American authorities with information portraying Mr. Arar unfairly as an Islamic Extremist despite having no basis for describing him that way" and that "it was very likely that these communication sled to the US decision to detain Mr. Arar and rendition him to Syria"[158]. The Supreme Court of Canada subsequently stated, in its ruling of *Andrew Gordon Wake v Attorney General of Canada on behalf of the United States of America and Attorney General of British Columbia*, that the "torture of Maher Arar in Syria provides a particularly chilling example of the dangers of unconditional information sharing"[159].

However, the danger is not only putting Canadian citizens at mental and bodily harm, or violation of their fundamental and human rights; it also creates a significant financial risk when the state must provide financial compensation to the individual for such an egregious mistake.

In this case, in 2007, Mr. Arar received a formal public apology from the Prime Minister on behalf of the Canadian government, and CAD $11.5 million in compensation for the direct and indirect role of Canadian officials in his rendition to torture in Syria[160].

With Bill C-2's provisions regarding access to broad information under a low threshold and no judicial oversight, disclosure of information to foreign governments is very likely to occur, attracting a duty to compensate innocents for any wrongdoing arising from such data-sharing, and resulting in diminished trust in government and increased damage to Canada's public image worldwide. The financial impact on Canada's economy for such acts is incalculable.

[155] 'The Maher Arar Case' (*Amnesty International*, 6 February 2017) <https://amnesty.ca/legal-brief/case-maher-arar/> accessed 23 August 2025.

[156] *Idem.*

[157] Idem.

[158] Idem.

[159] Andrew Gordon Wake v Attorney General of Canada on behalf of the United States of America and Attorney General of British Columbia [2014] Supreme Court of Canada (SCC) 2014 SCC 72, §104.

[160] *Idem.*

Secondly, there is also a financial risk in an eventual invalidation of Canada's adequacy decision.

First issued in 2001, the adequacy decision considered that Canada provides an adequate level of protection for personal data[161], allowing for the transfer of data out of the EU to said country without any authorization per Article 45 of the GDPR[162].

In 2024, the European Commission issued a new decision renewing the adequacy status for personal data transferred from the EU to recipients subject to PIPEDA, confirming its applicability solely to commercial operators[163].

However, if Bill C-2 is enacted into law, there is a high probability that the adequacy decision will be ruled invalid, as evidenced as possible in the cases of *Schrems I* and *Schrems II*.

An adequacy decision takes into account the respect for human rights and fundamental freedoms, which Bill C-2's provisions neither comply with nor respect.

Furthermore, the mass surveillance scheme created by Bill C-2's provisions is similar to those challenged in the CJEU's cases, that is, of broad access to information, regardless of their sensitivity, without judicial oversight and on a limitless number of targets, veiled by secrecy. The similarity alone could lead to a review of the status of protection of data in Canada and the invalidation of its adequacy status.

In that scenario, the loss of this adequate status can result in incalculable financial damage to Canada's commercial operators.

That is because, whatever their size, to transfer data out of the EU, they will now have to apply additional safeguards per Article 46 of the GDPR[164], such as develop binding corporate rules, apply standard contractual clauses or get a code of conduct approved. Or, in the absence of those, rely on derogations for specific scenarios per Article 49[165].

Any of these scenarios will increase compliance costs including legal and technical expertise easily borne by big corporations; but the financial burden for individuals and small organizations might lead to economic instability or even bankruptcy.

---

[161] Commission Decision of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act (notified under document number C(2001) 4539) 2001 (OJ L).

[162] N(100).

[163] European Commission, REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the first review of the functioning of the adequacy decisions adopted pursuant to Article 25(6) of Directive 95/46/EC 2024, p. 9.

[164] N(100).

[165] *Idem*.

It is important to stress that nowadays, in a digital world and global market, anyone could be in commercial relations in the EU and gather data from the region. In fact, the EU is Canada's second-largest trading partner, only after the United States[166]. And obviously, trade relations do include the exchange and transfer of data. Therefore, the impact on Canada's internal economy can be critical and long-lasting, and must be considered by the Parliament when studying Bill C-2.

Finally, all of the above demonstrate that the risks of surveillance go beyond the practices themselves, as harmful to fundamental and human rights, actually creating a digital wall between the USA and Canada, challenging the country's data sovereignty, and potentially impacting the economy.

[166] 'EU Trade Relations with Canada' (24 June 2025) <https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/canada_en> accessed 26 July 2025.

Conclusion

Bill C-2 arises from the necessity to better ensure the security of the border between Canada and the United States and reinforce security measures.

Although envisioned as an act to expand the power of the so-called lawful access to information, it in fact, creates the opposite: a system of mass surveillance practices by peace or public officers on any information regarding any individual, veiled by secrecy, that violates both the national legal framework on the right to privacy, as well as several international human rights and global trends on mass surveillance.

Upon analysis, it has been revealed that Bill C-2's provisions are immediately concerning, from the use of ambiguous terms, unclear wording and potentially a limitless number of targets and broad information collection, without any oversight mechanism or requirement to obtaining judicial authorization.

The surveillance scheme envisioned is also incompatible with national law – PIPEDA – and jurisprudence on the right to privacy, particularly given to the absence of safeguards required by the Supreme Court of Canada, in the ruling of *R. v. Spencer*.

From an international perspective, the provisions of Bill C-2 are a violation to international human rights, under the 13 Principles framework, and directly incompatible with the rulings of the European Court of Human Rights (ECtHR) in *Szabó and Vissy v. Hungary* and *Big Brother Watch and Others v. United Kingdom* and the Court of Juste of the European Union (CJEU) in *Schrems I* and *Schrems II*.

Consequently, the so-called lawful access provisions are in fact an unlawful mass surveillance system that raises many critical risks. Most obvious is the violation of Canadians' fundamental rights under the Charter of Rights and Freedoms and international human rights under the 13 Principles, mainly the right to privacy — unreasonable search and seizure — but also many others, such as freedom of expression.

However, Bill C-2 might also drastically impact the data-sharing relationship between Canada and other countries, most notably the United States.

In the specific scenario of ongoing discussions on the 2AP Treaty and the CLOUD Act, the enactment of Bill C-2 could result in the creation of a digital wall between Canada and the United States, with uneven data sharing obligations, creating a direct threat to Canada's data sovereignty due to a virtual state of data subordination to the USA.

Moreover, Bill C-2 creates two main financial risks. One being a government's duties to compensate any individual who might be impacted by the state's inadequate information-sharing practices, and the other, the compliance cost of incurred by commercial operators in the eventual invalidation of Canada's adequacy decision and its impact on the internal economy.

In conclusion, this study reveals that Bill C-2's provisions, as currently written, should not be enacted into law, as they are contrary to fundamental democratic principles and the rule of law.

Surveillance practices may indeed be valuable to governments in light of today's world threats. However, the necessity to provide security does not override Canadians' fundamental rights, especially through a law such as Bill C-2 that overlooks the many critical risks it creates.

There is a legal framework to mass surveillance schemes, guided by safeguards and judicial oversight, that Bill C-2 could follow but, as it stands today, the proposed law violates fundamental and human rights, especially privacy, with immeasurable impact.

References

Andrew Gordon Wake v Attorney General of Canada on behalf of the United States of America and Attorney General of British Columbia [2014] Supreme Court of Canada (SCC) 2014 SCC 72

Bernal P, 'Data Gathering, Surveillance and Human Rights: Recasting the Debate' (2016) 1 Journal of Cyber Policy 243.

Branch LS, Personal Information Protection and Electronic Documents Act 2000 [S.C. 2000, c. 5].

'C-2 (45-1) - An Act Respecting Certain Measures Relating to the Security of the Border between Canada and the United States and Respecting Other Related Security Measures' (*LEGISinfo*) <https://www.parl.ca/legisinfo/en/bill/45-1/c-2> accessed 13 June 2025.

Case C-362/14 - Maximillian Schrems v Data Protection Commissioner (Court of Justice of the European Union (CJEU)).

Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems (Court of Justice of the European Union (CJEU)).

Citizensinformation.ie, 'Charter of Fundamental Rights' <https://www.citizensinformation.ie/en/government-in-ireland/european-government/eu-law/charter-of-fundamental-rights/> accessed 22 August 2025.

Charter of Fundamental Rights of the European Union 2012 [2012/C 326/02].

Commission Decision of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act (notified under document number C(2001) 4539) 2001 (OJ L).

Council of Europe, '46 Member States of the Council of Europe - Portal' (*Portal*) <https://www.coe.int/en/web/portal/members-states> accessed 17 August 2025.

Council of Europe, 'Canada - Observer State' (*Portal*) <https://www.coe.int/en/web/portal/canada> accessed 17 August 2025.

Cornell C, '*R. v. Spencer* and the Affirmation of Internet Privacy Rights in Canada' (2014) 20 Law and Business Review of the Americas 649.

Criminal Code 1985 [C–46].

European Commission, REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the first review of the functioning of the adequacy decisions adopted pursuant to Article 25(6) of Directive 95/46/EC 2024.

European Court of Human Rights, European Convention on Human Rights 1950.

European Court of Human Rights, 'Factsheet Mass Surveillance'.

European Court of Human Rights, 'Information Note on the Court's Case-Law 192 - Szabó and Vissy v. Hungary - 37138/14' <https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22002-10821%22]}> accessed 13 July 2025.

European Court of Human Rights, 'Information Note on the Court's Case-Law 221 - Big Brother Watch and Others v. the United Kingdom - 58170/13, 62322/14 and 24960/15' <https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22002-12080%22]}> accessed 17 August 2025.

European Court of Human Rights and European Union Agency for Fundamental Rights, 'Mass Surveillance - ECtHR and CJEU Case-Law'.

'EU Trade Relations with Canada' (24 June 2025) <https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/canada_en> accessed 26 July 2025.

Geist M, '"Big Brother Tactics": Why Bill C-2's New Warrantless Disclosure Demand Powers Extend Far Beyond Internet and Telecom Providers' (*Michael Geist*, 18 June 2025) <https://mgeist.substack.com/p/big-brother-tactics-why-bill-c-2s> accessed 26 July 2025

Geist M, 'Lawful Access on Steroids: Why Bill C-2's Big Brother Tactics Combine Expansive Warrantless Disclosure with Unprecedented Secrecy - Michael Geist' (20 June 2025) <https://www.michaelgeist.ca/2025/06/lawful-access-on-steroids/> accessed 23 June 2025.

Government of Canada D of J, '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 - Charter Statement' (19 June 2025) <https://www.justice.gc.ca/eng/csj-sjc/pl/charter-charte/c2_2.html> accessed 26 July 2025.

Parliament of Canada, Government Bill (House of Commons) C-2 (45-1) - An Act respecting certain measures relating to the security of the border between Canada and the United States and respecting other related security measures [C–2].

Legislative Services Branch, Personal Information Protection and Electronic Documents Act 2000 [S.C. 2000, c. 5]

Legislative Services Branch, Constitution Act 1982.

Lou B, '*R. v. Bykovets*: An Affirmation of Canadians' Right to Informational Privacy' 22 Canadian Journal of Law and Technology.

McNab A, 'Police Need Search Warrant to Get IP Address, Rules Supreme Court of Canada in 5-4 Split Decision' (*Canadian Lawyer*, 1 March 2024) <https://www.canadianlawyermag.com/practice-areas/criminal/police-need-search-warrant-to-get-ip-address-rules-supreme-court-of-canada-in-5-4-split-decision/384148> accessed 9 August 2025.

Necessary & Proportionate, 'International Principles on the Application of Human Rights to Communications Surveillance' (2014) <https://necessaryandproportionate.org/files/en_principles_2014.pdf> accessed 26 July 2025.

Necessary & Proportionate, 'Necessary & Proportionate on the Application of Human Rights to Communications Surveillance' <https://necessaryandproportionate.org/images/np-logo-og.png> accessed 26 July 2025.

Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) 2016 [2016/679].

Robertson K, 'Unspoken Implications: A Preliminary Analysis of Bill C-2 and Canada's Potential Data-Sharing Obligations Towards the United States and Other Countries' (Citizen Lab, University of Toronto 2025) <https://citizenlab.ca/2025/06/a-preliminary-analysis-of-bill-c-2/> accessed 26 July 2025.

R v Spencer [2014] Supreme Court of Canada 2014 SCC 43.

R v Bykovets [2024] Supreme Court of Canada 2024 SCC 6.

'The Maher Arar Case' (*Amnesty International*, 6 February 2017) <https://amnesty.ca/legal-brief/case-maher-arar/> accessed 23 August 2025.

Tunney C, 'Officials Defend Liberal Bill That Would Force Hospitals, Banks, Hotels to Hand over Data' (19 June 2025) <https://www.cbc.ca/lite/story/1.7565775?feature=related-link> accessed 26 July 2025.

Tzanou M, 'Schrems I and Schrems II: Assessing the Case for the Extraterritoriality of EU Fundamental Rights' (Social Science Research Network, 13 October 2020) <https://papers.ssrn.com/abstract=3710539> accessed 22 August 2025.

Zalnieriute M, 'Big Brother Watch and Others v. the United Kingdom' (2022) 116 American Journal of International Law 585.

Privacy & Access Council of Canada
Conseil du Canada de l'Accès et la vie Priveé
Suite 330 • Unit 440 • 10816 Macleod Trail SE
Calgary • Alberta • Canada • T2J 5N8