
# Submission to the House of Commons Standing Committee on Public Safety and National Security regarding Bill C-26, An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts


## Canadian Civil Liberties Association

Daniel Konikoff | Interim Director – Privacy, Technology & Surveillance Program

Tashi Alford-Duguid | Staff Lawyer

Noa Mendelsohn Aviv | Executive Director and General Counsel


September 12, 2023


Canadian Civil Liberties Association

124 Merton St., Suite 400

Toronto, ON M4S 2Z2

Phone: 416-363-0321

Table of Contents



# Introduction

The Canadian Civil Liberties Association ("CCLA") is an independent, national, nongovernmental organization that was founded in 1964 with a mandate to defend and foster the civil liberties, human rights, and democratic freedoms of all people across Canada. Our work encompasses advocacy, research, and litigation related to the criminal justice system, equality rights, privacy rights, and fundamental constitutional freedoms. Working to achieve government transparency and accountability with strong protections for personal privacy lies at the core of our mandate.

In this submission, CCLA speaks to Bill C-26, the Government of Canada's telecommunications and cybersecurity legislation. This submission addresses the concerns Bill C-26 raises for human rights and civil liberties with a particular focus on privacy. Cybersecurity is an essential part of national security, and the digital ecosystem in which we increasingly live our lives needs to be safe, reliable, and secure from threats. Cybersecurity is also crucial for our democratic institutions, the economy, critical infrastructure, national defence, and the privacy of our online life. It is important that Canada take steps toward protecting the digital foundations on which modern life is built. However, in its current form, Bill C-26 risks undermining our privacy rights, due process, and the principles of accountable governance—all of which are part of the very fabric of our democracy. C-26 must not pass without substantial revisions to protect fundamental rights and due process.

This submission makes recommendations for how Bill C-26 can improve the way government and telecommunication companies define, handle, and protect individuals' personal information and thus protect individuals' right to privacy. Privacy is, after all, an essential component of individuals' personal sense of security, both off- and online, and stands to be positioned more centrally in C-26. CCLA believes that our recommendations enable the legislation to better fulfill its stated objectives: bolster cybersecurity across the financial, telecommunications, energy, and transportation sectors, and help organizations better prepare, prevent, and respond to cyber incidents.

The amendments outlined in this submission echo the Joint Letter of Concern that CCLA sent with civil society partners in September 2022.[1] In addition, our recommendations are consistent with those contained within the *Fixing Bill C-26 Recommended Remedies* package,[2] of which CCLA is a signatory, as well as with the recommendations in Christopher Parsons' report, *Cybersecurity Will Not Thrive in Darkne*ss.[3]

---

[1] McPhail, B. (September 28, 2022). "Joint Letter of Concern Regarding Bill C-26." *CCLA.* https://ccla.org/privacy/joint-letter-of-concern-regarding-bill-c-26/

[2] Fix 26 Coordination Group. (June 20, 2023). "Fixing Bill C-26: Recommended Remedies."https://drive.google.com/file/d/1pQn4-us3wf7qOIm2gI5scLQPGTaumkiO/view

[3] Parsons, C. (October 18, 2022). "Cybersecurity Will Not Thrive in Darkness: A Critical Analysis of Proposed Amendments in Bill C-26 to the *Telecommunications Act.*" *Citizen Lab* Research Report No. 158.

## Defining Personal Information

As it stands, Bill C-26 undermines privacy by empowering the government to collect broad categories of information from designated operators, at any time, subject to any conditions, or even no conditions at all. This may enable the government to obtain identifiable and de-identified personal information and subsequently distribute it to domestic, and perhaps foreign, organizations. Given the sensitivity of the information people in Canada provide to designated operators, this provision poses an extraordinary risk to individuals' privacy. Measures must be established to constrain the government's collection, use, and distribution of individuals' sensitive information.

In general, the privacy of personal information is one of the keys to strong cybersecurity protections. Building privacy into cybersecurity legislation will go a long way toward ensuring the cybersecurity protections proposed in Bill C-26 are successful. Some degree of monitoring is required to protect telecommunications infrastructure from attack, but this should not come at the expense of personal privacy. There is no excuse for governments to surveil and analyze online activity without clear safeguards for personal privacy and individuals' fundamental rights.

One way to reasonably restrict the government's capacity to collect information is to refine how Bill C-26 conceives of information worth protecting. This would involve codifying personal and de-identified information as confidential. Personal information is any information that can be used to identify an individual through association or inference. Many kinds of information qualify as personal in their capacity to identify an individual; these, according to the European Union's (EU) General Data Protection Regulation (GDPR), include names, ID numbers, location data, online identifiers, or "factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity" of a person.[4]

Further, personal data can be anonymized or de-identified, but de-identified information requires additional protections. Anonymization involves permanently deleting identifying data, while de-identification involves stripping away and separating different bits of identifying information from one another or protecting identifying information through encryption or key (but not permanently deleting it). Anonymizing data is irreversible, while de-identified data can be *re*-identified. De-identified data requires greater protection than anonymized data, so Bill C-26 should ensure de-identified information is explicitly acknowledged as confidential.

As it stands, Bill C-26's proposed amendments to the *Telecommunications Act* do not designate personal and de-identified information as confidential under section 15.5(1). Nor for that matter does the *Critical Cyber Systems Protection Act (CCPSA),* which under section 6(1) does not flag personal or de-identified information as confidential. In order to protect this information, both Acts contained within C-26 need adjustment to better align with our privacy rights, freedoms, and democratic values.

**RECOMMENDED REMEDY - Telecommunications Act:**

1. Add after s. 15.5 (1)(c) the words:

(d) "information that is personal or de-identified."

[4] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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] OJ L 119/1.

## Handling Personal Information

Bill C-26 gives the Minister overbroad powers for handling personal information. Telecommunication companies, and companies likely to be designated under the *CCSPA*, collect, process, and store vast amounts of personal data and metadata, including call logs, messages, financial data, and location data. But as worded, Bill C-26 allows the Minister to share this type of personal information with anyone they designate (*TA 15.6)* or who is prescribed by regulations (*TA 15.6* and *CCSPA 23)*. It is one thing for government to ask designated operators for information about themselves and how they are complying with orders, but there needs to be a significantly higher standard when ordering companies to hand over information about their customers. This is especially important for telecommunication companies, given the high volume of personal information they hold about the public, and how telecommunications data can be used to identify individuals, track their movements, and monitor their communications.[5] Bill C-26 should better protect the privacy of personal information and communications by creating a more effective stopgap between this information and the Minister's ability to disclose it. The legislation should be amended so that the government must first obtain a relevant judicial order from the federal court before it can compel a telecommunications provider to disclose personal or de-identified information.

| **Telecommunications Act**<br>**Original Text** | **Telecommunications Act**<br>**Recommended Remedies:** |
|---|---|
| 15.5 (3)(c) the disclosure is necessary, in the Minister's opinion, to secure the Canadian telecommunications system, including against the threat of interference, manipulation or disruption. | 15.5 (3)(c) on application to the Federal Court, a judge is satisfied by information on oath that there are reasonable grounds to believe that the disclosure is necessary~~, in the Minister's opinion,~~ to secure the Canadian telecommunications system, ~~including~~ against the threat of interference, manipulation or disruption.<br><br>15.5 (3)(d) demonstrable exigent circumstances exist which, in the Minister's opinion, make the disclosure necessary to secure the Canadian telecommunications system against an urgent threat of interference, manipulation, or disruption. In such circumstances, the Minister shall within 30 days make an application to the Federal Court, and provide information under oath justifying the disclosure. |

Further, Parliament should strengthen the Bill's privacy protections when it comes to telecommunication providers and designated operators sharing information with foreign parties. In the proposed new section 15.7(1) of the *Telecommunications Act:*

[5] Parsons, C. (2015). "The Governance of Telecommunications Surveillance: How Opaque and Unaccountable Practices and Policies Threaten Canadians." Available at SSRN: https://ssrn.com/abstract=2901521 or http://dx.doi.org/10.2139/ssrn.2901521

> "Any information collected or obtained under this Act, other than information designated as confidential under subsection 15.5(1), may be disclosed by the Minister under an agreement, a memorandum of understanding or an arrangement in writing between the Government of Canada and the government of a province or of a foreign state, an international organization of states or an international organization established by the governments of states, or any institution of any such government or organization, if the Minister believes that the information may be relevant to securing the Canadian telecommunications system or the telecommunications system of a foreign state, including against the threat of interference, manipulation or disruption."

The provision's breadth and vagueness would allow not only for tremendous ministerial overreach, but it could also lead to privacy risks that cross provincial and national borders, resulting as well in potential risks to life and security for affected individuals and groups. CCLA strongly urges the amendment of the Bill to preclude the Minister from sharing personal or de-identified personal information to foreign governments or organizations, and that the Minister should inform telecommunications providers and designated operators when—and to whom—information may be disclosed when the receiving party is a foreign state, agency, organization, or party.

**RECOMMENDED REMEDY - Telecommunications Act:**

2. Add after s. 15.7 (1) the words:

"(2) Persons from whom the Minister, or person designated by the Minister, has collected information under section 15.4 shall be informed when, and to whom, such information has been disclosed when the receiving party is a foreign state, an international organization of states or an international organization established by the governments of states."

**RECOMMENDED REMEDY - CCSPA:**

3. Add after s. 27(1) the words:

"(2) Persons from whom the Minister, or person designated by the Minister, a responsible minister or a regulator has collected information under section 26(1) shall be informed when, and to whom, such information has been disclosed when the receiving party is a foreign state, or an international organization established by the governments of foreign states."

| **CCSPA**<br>**Original Text** | **CCSPA**<br>**Recommended Remedies:** |
|---|---|
| 26 (1) Subject to subsection (2), a person must not knowingly disclose confidential information or allow it to be disclosed to any agency, body or other person or allow any other agency, body or other person to have access to the information, except if | 26 (1) Subject to subsection (2), a person must not knowingly disclose confidential information, including information that is personal or de-identified, or allow it to be disclosed to any agency, body or other person or allow any other agency, body or other person to have access to the information, except if |

Finally, Bill C-26 lacks strong provisions around data retention periods. Data should only ever be kept for as long as they are useful, and storing data indefinitely can increase the risks and harms of potential data breaches.[6] Data retention periods are crucial for ensuring that any information obtained under either the *Telecommunications Act* or the *CCSPA* would be held only for so long as is necessary to make a legislative order, or to confirm compliance with such an order. CCLA recommends that the legislation be amended to make this data retention period as limited in duration as possible, and that the legislation include—to the extent that the legislation permits any data sharing—a requirement to attach data retention and deletion clauses in agreements or memoranda of understanding that are entered into with foreign governments or agencies.

**RECOMMENDED REMEDY - Telecommunications Act:**

4. Add after s. 15.7 (2) the words:

"**Data Retention Periods**
(3) Any information collected or obtained under this Act will be retained only for as long as necessary to make, amend, or revoke an order under section 15.1 or 15.2 or a regulation under paragraph 15.8(1)(a), or to verify the compliance or prevent non-compliance with such an order or regulation.

(4) Retention periods should be communicated to the person from whom the Minister, or person designated by the Minister under section 15.4, has collected the information.

(5) Any agreement, memorandum of understanding, or arrangement in writing between the Government of Canada and the government of a foreign state, an international organization of states or an international organization established by the governments of states, must include data retention and deletion clauses to ensure it is retained only for as long as is necessary for the purposes set out in subsection (1)."

**RECOMMENDED REMEDY - CCSPA:**

5. Add after s. 26(2) the words:

"**Data Retention Periods**
(3) Any information collected or obtained under this Act will be retained only for as long as necessary to make, amend, or revoke an order under section 20, or to verify the compliance or prevent non-compliance with such an order or regulation.

(4) Retention periods should be communicated to the person from whom the Governor in Council has collected the information.

(5) Any agreement, memorandum of understanding, or arrangement in writing between the Government of Canada and the government of a foreign state, an international organization of states or an international organization established by the governments of states, must include data retention and deletion clauses to ensure it is retained only for as long as is necessary for the purposes set out in subsection (1)."

[6] Office of the Privacy Commissioner of Canada. (2021). "Personal Information Retention and Disposal: Principles and Best Practices." *OPC.* https://www.priv.gc.ca/en/privacy-topics/business-privacy/safeguards-and-breaches/safeguarding-personal-information/gd_rd_201406/

## Ensuring Accountability for Mishandled Information

Bill C-26 lacks key accountability measures for privacy issues. Accountability is a core principle of effective government and should similarly be a core principle of Bill C-26.

A key accountability concern pertaining to privacy is that Bill C-26 does not allow individuals to seek relief if the government mishandles personal or de-identified information. Allowing for this recourse is an important step toward accountability for privacy violations. CCLA recommends that Bill C-26 be amended to enable individuals to seek relief if the government or a party to whom the government has disclosed their personal or de-identified information negligently loses control of that information and where that loss of control impacts the individual.

**RECOMMENDED REMEDY - Telecommunications Act:**

6. Add after s. 15.7 (2) the words:

**Private Right of Action**
(3) Any person who is affected by an act or omission by the government, or by a person or entity to whom the government has disclosed their confidential information, has a cause of action for damages for loss or injury suffered as a result of the contravention if

a. The government, or the person or entity to whom the government has disclosed their confidential information, loses control of that information, and
b. That loss of control materially affects or prejudices that person.

**Limitation period or prescription**
(4) An action must not be brought later than two years after the day on which the person becomes aware of the loss of control over the confidential information.

**Court of competent jurisdiction**
(5) An action referred to in subsection (3) may be brought in the Federal Court or a superior court of a province.

**RECOMMENDED REMEDY - CCSPA:**

7. Add after s. 27 (2) the words:

**Private Right of Action**
(3) Any person who is affected by an act or omission by the government, or by a person or entity to whom the government has disclosed their confidential information, has a cause of action for damages for loss or injury suffered as a result of the contravention if

c. The government, or the person or entity to whom the government has disclosed their confidential information, loses control of that information, and
d. That loss of control materially affects or prejudices that person.

**Limitation period or prescription**
(4) An action must not be brought later than two years after the day on which the person becomes aware of the loss of control over the confidential information.

**Court of competent jurisdiction**
(5) An action referred to in subsection (3) may be brought in the Federal Court or a superior court of a province.

## Conclusion

In its current form, Bill C-26 undermines personal privacy and violates due process. Privacy and due process are not only essential to cybersecurity and the protection of our critical infrastructure but are also part of the very fabric of our democracy. The Bill gives government the power to collect broad categories of information about people, without adequate protections for information that should be deemed confidential. The Bill also threatens personal privacy and creates other serious risks and dangers to people by allowing government to distribute this sensitive information to domestic and foreign organizations without proper checks and balances. And the Bill contains inadequate mechanisms for people to seek appropriate redress in cases where their private information has been mishandled and abused.

In this submission, CCLA has recommended remedies to address these concerns while still enabling the legislation to fulfill its stated goals: bolstering cybersecurity across the financial, telecommunications, energy, and transportation sectors, and helping organizations better prepare, prevent, and respond to cyber incidents. We urge the Committee Members to adopt these proposals for strengthening Bill C-26.