CANADIAN CIVIL LIBERTIES ASSOCIATION

ASSOCIATION CANADIENNE DES LIBERTES CIVILES

SUBMISSION TO THE STANDING SENATE COMMITTEE ON NATIONAL SECURITY, DEFENCE AND VETERANS AFFAIRS REGARDING BILL C-26, *AN ACT RESPECTING CYBER SECURITY, AMENDING THE TELECOMMUNICATIONS ACT AND MAKING CONSEQUENTIAL AMENDMENTS TO OTHER ACTS*

CANADIAN CIVIL LIBERTIES ASSOCIATION

Anaïs Bussières McNicoll | Director, Fundamental Freedoms Program and Interim Director, Privacy, Technology and Surveillance Program

Noa Mendelsohn Aviv | Executive Director and General Counsel

NOVEMBER 13, 2024

Canadian Civil Liberties Association
124 Merton St., Suite 400
Toronto, ON M4S 2Z2
Phone: 416-363-0321
www.ccla.org

Overview

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.

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 thus important that Canada take steps toward protecting the digital foundations on which modern life is built.

However, cybersecurity should not undermine civil liberties. While the work accomplished by the Standing Committee on Public Safety and National Security did address some of the civil liberties concerns associated with Bill C-26, several issues still need to be tackled.

The attached joint submission on Bill C-26, which CCLA endorses, addresses key outstanding concerns through 4 categories of recommendations. These recommendations call on Bill C-26 to be amended to (1) prohibit the government from undermining encryption and communications security; (2) ensure that government orders cannot remain secret indefinitely; (3) address significant privacy shortcomings; and (4) ensure that all government departments and agencies use information obtained under Bill C-26 exclusively for the cybersecurity and information assurance activities for which the information is collected.

The recommended remedies address pressing concerns likely to undermine public trust 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.

Joint Civil Society Senate Submission on Bill C-26

Canadian Civil Liberties Association
Canadian Constitution Foundation
International Civil Liberties Monitoring Group
Ligue des Droits et Libertés
National Council of Canadian Muslims
OpenMedia
Privacy and Access Council of Canada
Prof Andrew Clement
Dr. Brenda McPhail

Table of Contents:

Executive Summary:

Honourable Senators,

As organizations and individuals committed to upholding civil liberties and the fundamental right to privacy, we share the Government of Canada's objective of strengthening cybersecurity across the public and private sectors, and supporting everyone in Canada to be better able to protect themselves against cyberattacks.

At the same time, however, the current form of Bill C-26, *An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts* ("Bill C-26" hereafter), contains significant flaws that may compromise civil liberties and cybersecurity — and, therefore, national security.

There is no reason why cybersecurity should come at the cost of civil liberties. Indeed, public trust is essential for cybersecurity to be a success, especially at a time when public trust in democratic institutions is eroding in Canada and across the globe. A bill which fails the democratic legitimacy test will fail to strengthen cybersecurity.

We first itemized our concerns in a September 2022 joint letter to former Public Safety Minister Marco Mendicino, and were encouraged to hear them reflected by Members of Parliament from all parties throughout Bill C-26's 2nd Reading debate.

We followed up by submitting a detailed package of Recommended Remedies (English, Francais) to MPs on the House of Commons Standing Committee on Public Safety and National Security (SECU). Several of us testified at the subsequent hearings to provide legislators with additional insights.

Throughout this work, we drew from the expert findings of Dr. Christopher Parsons, as set out in his October 2022 report *Cybersecurity Will Not Thrive in Darkness: A Critical Analysis of Proposed Amendments in Bill C-26 to the Telecommunications Act*, which was published by the Citizen Lab at the University of Toronto in October 2022.

While the work and dedication of SECU Committee members and other MPs from across the political spectrum have resolved some of the civil liberties concerns associated with the legislation, several significant and outstanding issues remain outstanding.

Given that there remain several areas of serious concern, and the constitutional role of the Senate, we believe that you have a critical role to play in ensuring that Bill C-26 delivers strong cybersecurity, while protecting privacy, ensuring accountability, and upholding the rights of everyone in Canada.

We respectfully highlight the following four areas as priorities for your consideration:

Bill C-26: Priority Recommendations

1. **Prohibit the government from undermining encryption and communications security**
2. **Ensure that government orders cannot remain secret indefinitely**
3. **Fix Bill C-26's serious privacy failings**
4. **Restrict the CSE and other government agencies to using information obtained under Bill C-26 exclusively for cybersecurity and information assurance purposes**

In what follows below, we provide more detail on these priority recommendations. We look forward to discussing these recommendations further with members of the Senate when your scrutiny of Bill C-26 commences.

Recommendation 1: Prohibit the government from undermining encryption and communications security

Overview:

Bill C-26, as passed by the House of Commons, contains a dangerous loophole. Specifically, the new ministerial powers set out in section 15.2 (2) of the *Telecommunications Act* amendments could be used to deliberately or inadvertently compromise the security of telecommunications networks that people, governments, and businesses across Canada (and beyond) rely upon every day.

This is especially the case regarding s. 15.2 (2)(l) which gives the government the power to require telecommunications providers to *"implement specified standards in relation to its telecommunications services, telecommunications networks or telecommunications facilities."*

The danger is that such a broadly-worded power could be used to compel providers to adopt standards which *weaken*, rather than *strengthen*, encryption and privacy. As currently drafted, the statutory language endangers the freedom of people in Canada to communicate privately with one another, or businesses to safely engage in national and international commerce, or governments and elected representatives to enjoy private communications.

Cybersecurity experts, in Canada and elsewhere, have cautioned that the current statutory language endangers Canada's economy, its international relations, and the fundamental right to privacy of people across Canada:

- Writing for The Globe & Mail, Citizen Lab's Kate Robertson and Ron Deibert warn that the *"secretive, encryption-breaking powers"* in Bill C-26 *"threaten the online security of everyone in Canada,"* and that the bill *"empowers government officials to secretly order telecommunications companies to install backdoors inside encrypted elements in Canada's networks."*

- In his testimony to the parliamentary committee studying Bill C-26, Eric Smith, Senior Vice-President at the Canadian Telecommunications Association, referenced the *"very broad"* order-making powers in Bill C-26, stating that *"It could be requiring you not necessarily to take out equipment from your infrastructure, but to put certain equipment into your infrastructure, or to comply with certain standards. It could be weakening encryption, or it could be requiring you to intercept communications."*

- Citing the US as an example of government overreach that Canada should avoid, the Electronic Frontier Foundation stated that *"the U.S. experience offers a cautionary tale of what can happen when a government grants itself broad powers to monitor and direct telecommunications networks, absent corresponding protections for human rights,"* and warned that *"without adequate safeguards, Bill C-26 could open the door to similar practices and orders."*

Despite having received multiple briefs (e.g. here, here, here, and here) and hearing from several witnesses (e.g. here, here, here, and here) on this topic, SECU did not consider the matter during its clause-by-clause review of Bill C-26. The House of Commons also eschewed the opportunity to do so during Report Stage, despite urgings that Parliamentarians address them. Instead, Bill C-26 was rushed through Report Stage without any debate.

This flies in the face of the government's unequivocal statements throughout the SECU Committee review that Bill C-26's purpose is network security, not surveillance.

Recommendation:

The danger to Canadians' communications security can be addressed simply, by making it explicit in statute what kinds of standards are within and beyond the scope of the legislation:

Telecommunications Act **Current Text**	**Telecommunications Act** **Recommended Remedy:**
Scope and substance **15.2 (2.1)** The provisions of an order made under subsection (1) or (2) must, in scope and substance, be reasonable to the gravity of the threat of interference, manipulation, disruption or degradation. **For greater certainty** **15.2 (2.2)** For greater certainty, despite subsection (2), the Minister is not permitted to order a telecommunications service provider to *intercept a private communication* or a *radio-based telephone communication*, as those terms are defined in section 183 of the *Criminal Code*.	**Scope and substance** **15.2 (2.1)** The provisions of an order made under subsection (1) or (2) must, in scope and substance, be reasonable to the gravity of the threat of interference, manipulation, disruption or degradation. **For greater certainty** **15.2 (2.2)** For greater certainty, despite subsection (2), the Minister is not permitted to order a telecommunications service provider to *intercept a private communication* or a *radio-based telephone communication*, as those terms are defined in section 183 of the *Criminal Code*. **For greater certainty** **15.2 (2.3)** For greater certainty, despite subsection (2), the Minister is not permitted to make an order that would compromise the confidentiality, availability, or integrity of a telecommunications facility, telecommunications service, or transmission facility.

This recommendation is meant to ensure that the government is empowered to issue orders compelling telecommunications providers to *strengthen* the confidentiality and security of their networks, but not to *weaken* them.

This amendment is intended to prevent the government from ordering or demanding that telecommunications service providers deploy or enable (or have deployed or enabled)

lawful-access related capabilities or powers in the service of 'securing' infrastructure by way of adopting a standard. If the government wishes to pursue enhanced lawful interception powers, it should do so by way of separate legislative processes.

Across Canada, people and businesses rely on the strength and confidentiality of encrypted networks to keep their communications safe and secure. The critical importance of secure communications is reinforced by the fact that the Communications Security Establishment (CSE) recently introduced end-to-end encryption to Canada's Top Secret Network (CTSN) — see page 9 of CSE's recent annual report.

Whether it is the CSE, a large corporation, a small business, political representatives, or neighbours exchanging news and views, everybody in Canada must be able to have trust in the security of their communications. This recommendation will ensure precisely that.

Recommendation 2: Ensure that government orders cannot remain secret indefinitely

Overview:

The current language in Bill C-26 allows the government to keep secret any order made to telecommunications providers, and to operators designated under the *Critical Cyber Systems Protection Act* (*CCSPA*). Under the current wording of Bill C-26, as amended by the House of Commons, telecommunications providers and designated operators are prohibited from even disclosing the fact that an order was issued, let alone its contents.

We appreciate that secrecy might be warranted in certain circumstances; but secrecy should neither be the default nor be permitted to remain in place indefinitely. In a democracy, the government must ensure people can understand how it exercises its cybersecurity and other powers, how often, and to what effect, to ensure that decision-makers can be properly held to account.

The concern addressed by this Recommendation arose during the SECU Committee's clause-by-clause review, when Bloc Quebecois MP Kristina Michaud proposed an amendment — based closely on our submission to the committee — which would have required an order from the Federal Court as a check-and-balance against government overreach, so as to ensure the government cannot conceal disproportionately intrusive actions under cover of secrecy.

Government officials resisted this proposed amendment, and argued that it *"could lead to efficiency risks. For example, a Federal Court process would take at least a few weeks."* To support their argument, they pointed to serious cybersecurity incidents in which urgent government action had been required, and asserted that the proposed amendment might impede emergency responses.

MP Jennifer O'Connell, the government's parliamentary secretary for cybersecurity, echoed MP Michaud's concerns. She proposed an alternative amendment requiring notification of all orders, including confidential ones, to the National Security and Intelligence Committee of Parliamentarians (NSICOP) and the National Security and Intelligence Review Agency (NSIRA). The government's amendment passed, and is now reflected in s. 15.22 of the *Telecommunications Act*, and s. 20 (4) of the *CCSPA*.

Although the government's amendment was an important and positive step, **it falls far short of addressing the core problem: the potential for government cybersecurity orders to remain secret indefinitely, without the validity of such secrecy ever being reviewed by a court.**

Recommendation:

We acknowledge the concern that there will be occasions when the government needs to take swift cybersecurity actions, and may determine that the delay required to obtain a Federal Court order is excessive in the circumstances. Accordingly, **we suggest a revised amendment** to recognize the need for extraordinary action in genuinely exigent circumstances, which also ensures a court would review the validity of secrecy of all orders, within 90 days of each such order being issued.

This recommendation would impose a 90-day time limit on the confidentiality provisions of all orders, and any extension would require the government bringing an application to the Federal Court:

Telecommunications Act **Current Text**	**Telecommunications Act** **Recommended Remedies:**
Non-disclosure 15.1 (2) The order may also include a provision prohibiting the disclosure of its existence, or some or all of its contents, by any person.	**Non-disclosure** 15.1 (2)(a) The order may also include a provision prohibiting the disclosure of its existence, or some or all of its contents, by any person, for a period of up to 90 days after the day on which it is made. 15.1 (2)(b) (i) The Governor in Council may bring an application to the Federal Court for an order to extend the period during which the disclosure of some or all of the contents of the order issued under subsection (1) is prohibited. The Federal Court may make an order to that effect where it is satisfied that there are reasonable grounds to believe that the disclosure of some or all of the order would be injurious to international relations, national defence or national security or endanger the safety of any person. 15.1 (2)(b)(ii) The judge, in consideration of the principles of fairness and natural justice, shall appoint a special counsel from the list of persons referred to in subsection 85(1) of the *Immigration and Refugee Protection Act* for the purposes of contesting the Governor in Council's application.
Non-disclosure 15.2 (3) An order made under subsection (1) or (2) may also include a provision prohibiting the disclosure of its existence, or some or all of its contents, by any person.	**Non-disclosure** 15.2 (3)(a) An order made under subsection (1) or (2) may also include a provision prohibiting the disclosure of its existence, or some or all of its contents, by any person, for a period of up to 90 days after the day on which it is made. 15.2 (3)(b)(i) The Minister may bring an

	application to the Federal Court for an order to extend the period during which the disclosure of some or all of the contents of the order issued under subsection (1) or (2) is prohibited. The Federal Court may make an order to that effect where it is satisfied that there are reasonable grounds to believe that the disclosure of some or all of the order would be injurious to international relations, national defence or national security or endanger the safety of any person. 15.2 (3)(b)(ii) The judge, in consideration of the principles of fairness and natural justice, shall appoint a special counsel from the list of persons referred to in subsection 85(1) of the *Immigration and Refugee Protection Act* for the purposes of contesting the Minister's application.

A similar situation applies to the *Critical Cyber Systems Protection Act (CCSPA)*, which allows the government to keep secret any order made to designated operators. This is particularly problematic given there is no automatic public notification mechanism for new orders. Again, while there are certainly situations in which secrecy might be appropriate, secrecy should not be the default in a robust democracy such as Canada's.

The following suggested amendment would permit designated operators to disclose the existence of a direction, but not its content, except to the extent necessary to comply with the direction:

CCSPA **Current Text**	**CCSPA** **Recommended Remedies:**
Prohibition against disclosure 24 Every designated operator that is subject to a cyber security direction is prohibited from disclosing, or allowing to be disclosed, the fact that a cyber security direction was issued and the content of that direction, except in accordance with section 25.	**Prohibition against disclosure** 24 Every designated operator that is subject to a cyber security direction is prohibited from disclosing, or allowing to be disclosed, ~~the fact that a cyber security direction was issued and~~ the content of that direction, except in accordance with section 25.
Disclosure — when allowed 25 (1) A designated operator that is subject to a cyber security direction may disclose the fact that the direction was issued and its content only to the extent necessary to comply with the direction.	**Disclosure — when allowed** 25 (1) A designated operator that is subject to a cyber security direction may disclose ~~the fact that the direction was issued and~~ its content only to the extent necessary to comply with the direction.

Finally, the Standing Joint Committee for the Scrutiny of Regulations plays a key role in Canada's democratic process. Bill C-26 should be amended such that the Standing Joint Committee for the Scrutiny of Regulations is able to obtain, assess, and render a verdict, which must promptly be made public, on any regulations that are promulgated under the proposed draft reforms to the *Telecommunications Act* and *Canada Cyber Systems Protection Act*.

The Committee should also be empowered to obtain, assess, and render a verdict, which must promptly be made public, on regulations pertaining to the *Telecommunications Act* and that are modified pursuant to s. 18 of the *Statutory Instruments Act*.

The following clauses in Bill C-26, which exempt the legislation from the *Statutory Instruments Act*, should be either deleted, or amended to make clear that the *Statutory Instruments Act* applies:

- Section 15.3 (3) of the *Telecommunications Act* amendments
- Sections 22 (1), 34 (2), 36 (3), 43 (2), 45 (3), 52 (2), 54 (3), 61 (2), 63 (3), 70 (3), 73 (4), 80 (2), and 82 (3) of the *CCSPA*

Incorporating the above recommendations will greatly improve transparency and, accordingly, public confidence and trust in how the government uses the sweeping new powers it is granting itself.

Recommendation 3: Fix Bill C-26's serious privacy failings

Overview:

Since Bill C-26 was first revealed in June 2022, privacy has continued to be one of our foremost concerns. In our September 2022 Joint Letter to the then Public Safety Minister Marco Mendicino, we warned that:

> *"Bill C-26 empowers the government to collect broad categories of information from designated operators, within any time and subject to any conditions. This may enable the government to obtain identifiable and de-identified personal information and subsequently distribute it to domestic, and perhaps foreign, organizations."*

We recognize that some progress has been made on this front as Bill C-26 progressed through the House of Commons, such as:

- Telecommunications providers, which retain vast quantities of Canadians' most sensitive information, can now define personal and de-identified information as "confidential" — with the effect of imposing significantly stronger protections for its handling, storage, and safeguarding.

- The *Privacy Act* now explicitly applies to the extensive information-sharing provisions in both the *Telecommunications Act* amendments and the *CCSPA*.

However, Canadians' privacy continues to be put in jeopardy as a result of Bill C-26's statutory language. Some of the most glaring problems are:

- The government can still disclose confidential information, obtained from telecommunications providers, to anyone, without first obtaining an order from the Federal Court. The government argued that this power was required to avoid delayed responses to emergencies; however, our proposed amendment (set out below), ameliorates these concerns.

- The SECU Committee created a legislative inconsistency in failing to pass an amendment that would have explicitly defined personal and de-identified information as "confidential" for the *CCSPA*, as it did for the *Telecommunications Act*.

- The SECU Committee had sought to protect Canadians' privacy by limiting data retention periods (ref: amendment by Kristine Michaud). However, this amendment was overturned without debate at the Report Stage, with the effect of enabling potentially indefinite retention of Canadians' personal information

We strongly encourage you to systematically address these fundamental shortcomings during your study of Bill C-26, and implement the following recommendations:

3.1 - Ensure that prior judicial approval is required, except in genuinely exigent circumstances, to obtain confidential information:

As currently drafted, Bill C-26 allows the Minister to require the disclosure of confidential information — including personal and de-identified information — from designated providers. This sweeping power must be subject to checks and balances to prevent the Minister from collecting and subsequently disclosing potentially injurious information without first obtaining an order from the Federal Court. Otherwise, businesses and individuals across Canada will be exposed to the serious risk of having their most sensitive information inappropriately disclosed.

The legislation should be amended so that — before the government can compel a telecommunications provider to disclose personal or de-identified information — it must first obtain a relevant judicial order from the Federal Court, stipulating that the information collected pursuant to such order is to be used exclusively for the purposes of making, amending, or revoking an order under s. 15.1 or 15.2 or a regulation under paragraph 15.8(1)(a), or of verifying compliance or preventing non-compliance with such an order or regulation.

Recognizing that there will be occasions in which information must be disclosed on an urgent basis, our recommendations include an accommodation for genuinely exigent circumstances, including provision for retroactive review by the Federal Court.

Telecommunications Act **Original Text**	**Telecommunications Act** **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. 15.5 (3)(d) if the conditions set out in subsection (c) for obtaining a Federal Court order exist, but by reason of exigent circumstances involving an imminent need to secure the Canadian telecommunications system against the threat of interference, manipulation, or disruption, it would be impracticable to obtain a Federal Court order. In such circumstances, the Minister shall within 30 days make an application to the Federal Court, and provide information under oath justifying the disclosure.

3.2 - Resolve the inconsistency between the CCSPA and the Telecommunications Act regarding the handling of personal information, including de-identified information:

As noted above, the *Telecommunications Act* now explicitly defines personal and de-identified information as "confidential" in s. 15.5 (1)(d). This is a critically important improvement over the original draft.

However, the legislative wording should also make clear that personal information *includes* de-identified information, because the definition of "personal information" carries important *Privacy Act* protections.

Telecommunications Act **Current Text**	**Telecommunications Act** **Recommended Remedies:**
15.5 (1) A person who provides any of the following information under section 15.4 may designate it as confidential: **(a)** information that is a trade secret; **(b)** financial, commercial, scientific or technical information that is confidential and that is treated consistently in a confidential manner by the person who provided it; **(c)** information the disclosure of which could reasonably be expected to **(i)** result in material financial loss or gain to any person, **(ii)** prejudice the competitive position of any person, or **(iii)** affect contractual or other negotiations of any person; or **(d)** personal information and de-identified information.	**15.5 (1)** A person who provides any of the following information under section 15.4 may designate it as confidential: **(a)** information that is a trade secret; **(b)** financial, commercial, scientific or technical information that is confidential and that is treated consistently in a confidential manner by the person who provided it; **(c)** information the disclosure of which could reasonably be expected to **(i)** result in material financial loss or gain to any person, **(ii)** prejudice the competitive position of any person, or **(iii)** affect contractual or other negotiations of any person; or **(d)** personal information ~~and~~ including de-identified information.
Definitions **(1.1)** The following definitions apply in paragraph (1)(d). ***de-identify*** means to modify personal information so that an individual cannot be directly identified from it, though a risk of the	**Definitions** **(1.1)** The following definitions apply in paragraph (1)(d). ***de-identify*** means to modify personal information so that an individual cannot be directly identified from it, though a risk of the

individual being identified remains. (*dépersonnaliser*) ***personal information*** has the same meaning as in section 3 of the Privacy Act. (*renseignements personnels*)	individual being identified remains. (*dépersonnaliser*) ***personal information*** has the same meaning as in section 3 of the Privacy Act. (*renseignements personnels*) **(1.2)** Any information provided under section 15.4 that is personal information, including any de-identified information, shall be deemed to be confidential.

Furthermore, for the avoidance of doubt, the *CCSPA* should be brought into line with the revised *Telecommunications Act* in proactively defining personal information, including de-identified information, as confidential:

CCSPA **Current Text**	**CCSPA** **Recommended Remedies:**
Definitions ***confidential information*** means any information obtained under this Act in respect of a critical cyber system that (a) concerns a vulnerability of any designated operator's critical cyber system or the methods used to protect that system and that is consistently treated as confidential by the designated operator; (b) if disclosed could reasonably be expected to result in material financial loss or gain to, or could reasonably be expected to prejudice the competitive position of, a designated operator; or (c) if disclosed could reasonably be expected to interfere with contractual or other negotiations of a designated operator. (*renseignements confidentiels*)	**Definitions** ***confidential information*** means any information obtained under this Act in respect of a critical cyber system that (a) concerns a vulnerability of any designated operator's critical cyber system or the methods used to protect that system and that is consistently treated as confidential by the designated operator; (b) if disclosed could reasonably be expected to result in material financial loss or gain to, or could reasonably be expected to prejudice the competitive position of, a designated operator; or (c) if disclosed could reasonably be expected to interfere with contractual or other negotiations of a designated operator. (*renseignements confidentiels*) (d) information that is personal information, including de-identified information.

Finally, personal information, including de-identified information, should *always* be deemed to be confidential, rather than that decision being left to the discretion of the entity providing it. This should be accomplished by adopting Recommendation 10 of Citizen Lab's Submission to this Committee:

Telecommunications Act **Current Text**	**Telecommunications Act** **Recommended Remedies:**
Exception **15.5 (3)** Information that is designated as confidential may be disclosed, or be permitted to be disclosed, if (a) the disclosure is authorized or required by law; (b) the person who designated the information as confidential consents to its disclosure; or (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.	**Exception** **15.5 (3)** Information that is designated as confidential may be disclosed, or be permitted to be disclosed, if (a) the disclosure is authorized or required by law; (b) the person who designated the information as confidential consents to its disclosure, or in the case of personal or de-identified information, the person to whom the information relates consents to its disclosure. (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.

3.3 - Ensure that Data Retention Periods are attached to telecommunications providers' data and to foreign disclosures of information:

Bill C-26 must be amended to make clear that information obtained from telecommunications providers, or operators designated by the *CCSPA*, 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) of the *Telecommunications Act*, or Section 20 of the *CCSPA*, or to verify the compliance or prevent non-compliance with such an order or regulation.

An amendment applying data retention periods to information collected from designated operators under the *CCSPA* that was initially passed by the SECU committee during its clause-by-clause review was later reversed — without debate — at Report Stage.

This begs the question — if the government claims it needs to collect information for the specific purpose of making orders, why is it opposed to restricting its retention to the period for which it is necessary for that purpose?

We urge your committee to ensure that data retention periods apply to the *Telecommunications Act* and the *CCSPA*, and that such clauses also apply to any information disclosures to foreign governments, organizations, and entities*:*

RECOMMENDED REMEDY - Telecommunications Act:

1. 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:

1. Add after s. 26(3) the words:

"**Data Retention Periods**
(4) 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.

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

(6) 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)."

Recommendation 4: Restrict the CSE to using information obtained under Bill C-26 exclusively for cybersecurity and information assurance purposes

Overview:

In its current form, Bill C-26 would authorize the Communications Security Establishment (CSE) — Canada's signal intelligence and cybersecurity agency — to obtain and analyze security-related data from companies that Canadians entrust with their most sensitive personal information — including telecommunications providers, federally-regulated financial institutions, energy providers, and every other entity designated under the *CCSPA*.

Bill C-26 amounts to a dramatic expansion of CSE's information collection powers. This is problematic, because the CSE's use of the information it collects is currently not constrained to the cybersecurity aspect of its mandate, and any uses would be largely subject to after-the-fact review rather than real-time oversight.

The government assures us that the CSE's new information collection powers are necessary for cybersecurity purposes, but it does not follow that it is either necessary or proportionate to use these expanded powers across all aspects of the CSE's mandate. As highlighted in a recent article by law professor Matt Malone, published by the Centre for International Governance Innovation, *"This diverges markedly from the thrust of the CSE's enabling legislation, which seeks to impose greater accountability over certain conduct through prior authorization and review obligations."*

In short, Bill C-26 risks eroding the careful protections in the *Communications Security Establishment Act* against allowing the CSE in some aspects of their mandate from directing actions at Canadians or persons in Canada, or collecting information that interferes with the reasonable expectation of privacy of a person in Canada, as protected by our *Charter*.

This is not a theoretical threat. It is clear from the testimony of CSE officials during SECU's clause-by-clause review that the CSE fully intends to use information it gathers for both offensive and defensive purposes, and also intends to share information it collects with its Five Eyes partners.

Asked to comment on a Bloc amendment which would have constrained CSE's use of information it gathers, CSE's Stephen Bolton (Director General, Strategic Policy) replied:

> *"Information collected by CSE pursuant to one aspect of its mandate* ***can be used by CSE under another aspect of the mandate*** *as long as it meets specific conditions set out in the* CSE Act. *Information related to security programs will enable CSE and its cyber centre to gain a better understanding of the supply chain risk of designated operators as well as the intentions of a foreign entity via its penetration into respective sectors.*

> *Without being able to leverage CSE's mandate as a whole, CSE's understanding of foreign actors' intentions against our critical infrastructure and the proper strategic mitigations would be greatly diminished.* ***Any limitation would also reduce CSE's collaboration with our Five Eyes partners****."* *[emphasis added]*

In other words, the CSE claims that not only are its new information-collection powers in Bill C-26 required for cybersecurity purposes, it also aims to use them to support international relations with other nations' signals intelligence agencies. While our alliances are important, Canadians' personal information should not be the coin to maintain these relations.

These risks to privacy and democratic accountability are exacerbated by the CSE's long track record of failing to embrace transparency. This includes the CSE's failure to cooperate with the National Security and Intelligence Review Agency in its investigations or to act on with its recommendations.

For example, the CSE has previously rejected recommendations by the National Security and Intelligence Review Agency (NSIRA) that it *"obtain additional legal advice on its internal sharing of information between the foreign intelligence and cybersecurity aspects of the mandate, explicitly in relation to compliance with the Privacy Act,"* claiming in 2021 that it had already received legal advice on the matter from the Department of Justice.

Despite CSE's 2021 refusal, NSIRA repeated its recommendation in its most recent review published January 2024, finding that *"CSE's internal sharing of information between the FI and cybersecurity aspects of the mandate has not been sufficiently examined for compliance with the Privacy Act."*

In short, as presently drafted, C-26 risks continuing a situation where the CSE interprets its mandates -- now supercharged with even more Canadians' personal information -- in manners that have been found non-compliant with the *Privacy Act* by their reviewer. The Senate has a role and obligation to prevent such a mishandling of Canadians' often most sensitive information, especially given the CSE's long track record of failing to cooperate with its review agencies.

Recommendation:

Bill C-26 must be amended to ensure that all government departments and agencies, including the CSE, use information obtained under Bill C-26 exclusively for the cybersecurity and information assurance activities for which the information is collected.

Such information should not be permitted to be used for additional purposes, such as signals intelligence and foreign intelligence activities, cross-department assistance unrelated to cyber-security, or active or defensive cyber operations. These restrictions should apply to all agencies, including but not limited to those under the purview of the Minister of Public Safety and Emergency Preparedness.

Telecommunications Act **Original Text**	**Telecommunications Act** **Recommended Remedies:**
1. ADD after s.15.6 (2) the words: "15.6 (3) Any information shared in accordance with section 15.6 can only be used by the recipient person for purposes exclusively relevant to securing the Canadian telecommunications system against the threat of interference, manipulation or disruption."	

CCSPA **Original Text**	**CCSPA** **Recommended Remedies:**
Guidance from Communications Security Establishment 16 An appropriate regulator may provide to the Communications Security Establishment any information, including any confidential information, respecting a designated operator's cyber security program or any steps taken under section 15, for the purpose of requesting advice, guidance or services from the Communications Security Establishment in accordance with the mandate of the Communications Security Establishment, in respect of the exercise of the appropriate regulator's powers or the performance of its duties and functions under this Act.	**Guidance from Communications Security Establishment** 16 An appropriate regulator may provide to the Communications Security Establishment any information, including any confidential information, respecting a designated operator's cyber security program or any steps taken under section 15, for the purpose of requesting advice, guidance or services from the Communications Security Establishment in accordance with the cybersecurity and information assurance mandate of the Communications Security Establishment as set out in section 17 of the *CSE Act*, in respect of the exercise of the appropriate regulator's powers or the performance of its duties and functions under this Act.
2. ADD after s.23 (1) the words: "(2) Any information shared in accordance with subsection (1) can only be used by the recipient person for the purposes set out in section 5."	
Confidential information 26 (3) Any confidential information that is disclosed or allowed to be accessed under subsection (1) must be treated as confidential.	**Confidential information** 26 (3) Any confidential information that is disclosed or allowed to be accessed under subsection (1) must be treated as confidential. **Restriction - use:** 26 (4) Information disclosed subject to subsections (1) or (2) must be used exclusively for purposes related to the protection of vital services, vital systems or critical cyber systems.

References & Resources:

Key resources:

- Full text of Bill C-26 (as passed at Third Reading by the House of Commons)
- C-26 Legislative Summary (Library of Parliament)
- Oct 2023 Civil Society Joint Submission to the House of Commons Standing Committee on Public Safety and National Security (aussi en français)
- Testimony to SECU Committee from: Professor Andrew Clement, Kate Robertson / Citizen Lab (Part 1, Part 2), Matt Hatfield / OpenMedia, Joanna Baron / Canadian Constitution Foundation, Sharon Polsky / Privacy & Access Council of Canada
- Testimony to SECU Committee from the Office of the Privacy Commissioner of Canada
- Sept 2022 Civil Society Joint Letter (PDF) (aussi en français)
- Citizen Lab / Dr Chris Parsons report: Cybersecurity will not thrive in darkness (PDF)

Media coverage:

- Centre for International Governance Innovation (op-ed by Matt Malone): As Drafted, Canada's New Cybersecurity Law Opts for Secrecy over Security
- The Globe and Mail: Ottawa wants the power to create secret backdoors in our networks to allow for surveillance
- iPhoneinCanada: Feds Want Secret Backdoors for Network Surveillance: Experts
- National Observer / Centre for International Governance Innovation (op-ed by Sharon Polsky): The Road to Digital Hell is paved with Good Intentions
- The Hub: Trudeau promised radical transparency. Instead, he has exacerbated closed government (op-ed by Matt Malone)
- Michael Geist Podcast: Interview with Citizen Lab's Kate Robertson on Bill C-26
- Global News: Contentious Liberal plan to overhaul cybersecurity faces more scrutiny
- Canadian Press: Federal cybersecurity bill threatens privacy, transparency, civil society groups say (Jim Bronskill)
- News Forum - Canadian Justice: Bill C-26, Cybersecurity & Civil Liberties (Host Christine Van Geyn interviews Dr Brenda McPhail (CCLA) and OpenMedia's Rosa Addario)
- CTV News Power Play: Interview with Dr Chris Parsons
- Canadian Press: Liberal cybersecurity bill a 'bad law' that must be amended, research report warns (Jim Bronskill)
- IT World Canada: Proposed telecom cybersecurity law gives Canadian government too much secret power: Researcher
- Policy Options: Don't give CSE more powers until it submits to effective review (Dr Chris Parsons)
- Hill Times: Canadians' privacy could take a serious hit this coming legislative session (Ken Rubin)
- Toronto Star (Op-Ed by OpenMedia): MPs must say no to agency request for powers to spy on your bank and travel records