CANADIAN CIVIL LIBERTIES ASSOCIATION

ASSOCIATION CANADIENNE DES LIBERTÉS CIVILES

SUBMISSION TO THE HOUSE OF COMMONS STANDING COMMITTEE ON PUBLIC SAFETY AND NATIONAL SECURITY (SECU)

Study: Bill C-8, An Act Respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts

December 15, 2025

CANADIAN CIVIL LIBERTIES ASSOCIATION (CCLA)
Tamir Israel | Director, Privacy, Surveillance & Technology Program
Howard Sapers | Executive Director

124 Merton St, Suite 400
Toronto, ON M4S 2Z2
Phone: +1 416-363-0321
https://ccla.org

Overview

Bill C-8 creates a broad, open-ended framework by which the government will be able to issue orders to telecommunications service providers and other entities for the intended purpose of improving cybersecurity in Canada. While there are benefits to establishing a national framework for cybersecurity, these benefits are currently overshadowed by significant flaws in Bill C-8 that need to be addressed if Canada's framework for cybersecurity is to be balanced and proportionate.

Cybersecurity and civil liberties should be mutually reinforcing and even enhancing. However, depending on how cybersecurity frameworks are implemented, they can raise significant civil liberty concerns, a challenge captured by the OECD Policy Framework on Digital Security:

> Depending on how they are used, security measures can support or undermine human rights and fundamental values. For example, some security measures can enhance privacy protection, provide anonymity to whistle-blowers and protect human rights activists from authoritarian surveillance. They can also enable the illegitimate surveillance of citizens or employees, or prevent access to activists' content.[1]

Responsible frameworks for cybersecurity should therefore incorporate specific measures to ensure that they are applied in a manner that enhances, rather than undermines, human rights.

As the Intelligence Commissioner of Canada noted in his testimony before this Committee, the government will be accessing highly sensitive information that engages a reasonable expectation of privacy in the operation of this Bill.[2] While Bill C-8 represents an improvement in terms of safeguards since this regime was initially introduced as Bill C-26 in the previous parliament, additional safeguards are required if Bill C-8 is going to survive constitutional scrutiny.

Canadian Civil Liberties Association

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.

CCLA has reviewed and largely supports several briefs submitted to this Committee in its study of Bill C-8.[3] In our brief, we focus on Part 1 of Bill C-8 and address the following:

---

[1] OECD, Policy Framework on Digital Security, (2022) *DSTI/CDEP/SDE(2021)12/FINAL*, p 15, https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/12/oecd-policy-framework-on-digital-security_a0b1d79c/a69df866-en.pdf.

[2] Testimony of the Hon. Simon Noël, Intelligence Commissioner of Canada, before SECU, October 30, 2025, *45th Parl 1st Sess No 010*, https://www.ourcommons.ca/Content/Committee/451/SECU/Evidence/EV13724995/SECUEV10-E.PDF, pp 6 and 8:

> In my experience as IC—with over three years and 45 decisions rendered—for the CSE to analyze and understand a cyber-incident, it must have access to information about the incident. There may be situations where this information is only technical in nature and sharing it with the CSE raises no privacy concerns, as you were told when you met with other witnesses. However, to fully under-stand the cyber-incident, other situations may require the CSE to have access to information, including technical information, for which Canadians have a reasonable expectation of privacy. I've seen it. … I agree that it's technical information, but I also know that if you want a positive result on an incident of such importance, they need to go into the content. I've seen it in every cyber-operation I've been involved in.

[3] Kate Robertson, Submission to SECU in its Study on Bill C-8, *Citizen Lab*, published November 24, 2025, https://www.ourcommons.ca/Content/Committee/451/SECU/Brief/BR13741249/br-external/CitizenLab-e.pdf; CIRA, Submission to SECU in its Study on Bill C-8, published November 6, 2025, https://www.ourcommons.ca/Content/Committee/451/SECU/Brief/BR13712352/br-

- Ensure the Bill's data collection authorizations are proportionate.
- Ensure TSPs will not be ordered to expand their surveillance & cyber offence capabilities
- Add safeguards for people or websites who might be disconnected from the Internet
- Ensure an effective right of appeal for people impacted by the operation of the Bill

CCLA notes that a number of Bill C-8's flaws arise from the government's decision to implement Bill C-8 through executive orders as opposed to through an independent regulator, a choice that offers less flexibility in terms of the application of safeguards and stakeholder engagement.

I. Significant privacy concerns remain

Investigations of cybersecurity threats will frequently entail access to high volumes of sensitive personal data.[4] In many instances, addressing cybersecurity threats will involve sharing general indicators of compromise and these will not include personal data. However, in many other instances, cybersecurity investigations will require detailed assessments of compromised private communications or monitoring of Internet traffic to identify threats, and this necessarily involves the interception of private communications as well as of sensitive metadata.[5] For this reason, any responsible cybersecurity framework needs to include direct and explicit safeguards for the protection of privacy, and most do.[6]

Far from providing robust privacy safeguards, Bill C-8 allows for the override of safeguards already in place. Orders issued under Bill C-8 can, for example, override safeguards imposed by the CRTC, including privacy safeguards imposed on to TSPs by the Commission in the cybersecurity context.[7] While TSPs will

---

external/CanadianInternetRegistrationAuthority-e.pdf. See also: Canadian Civil Liberties Association, "Government Needs to Fix Dangerous Flaws in Federal Cybersecurity Proposal", September 26, 2025, https://ccla.org/privacy/fix-dangerous-flaws-in-federal-cybersecurity-proposal/; Christopher Parsons, "Cybersecurity Will Not Thrive in Darkness: A Critical Analysis of Proposed Amendments in Bill C-26 to the Telecommunications Act," *Citizen Lab*, October 18, 2022, https://citizenlab.ca/wp-content/uploads/2022/10/Report158-critical-analysis-telecom-act.pdf.

[4] OECD, Council Recommendation on Digital Security of Critical Activities, December 2019, OECD/LEGAL/0456, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0456, p 17: "Considering the sensitivity of the information to be exchanged, partnerships need to be based on trust."; Canadian Security Telecommunications Advisory Committee (CSTAC), "Information Sharing, Reporting and Privacy Standard for Canadian Telecommunications Service Providers", v 1.1, March 31, 2020, https://ised-isde.canada.ca/site/spectrum-management-telecommunications/sites/default/files/attachments/2022/CSTAC_CCCSTinformationSharingAndReporting2020_01EN.pdf, section 2(4) "Evaluate any actions that [TSPs] take to protect the security of their network against the privacy trade-offs to their customers."; Compliance and Enforcement and Telecom Decision CRTC 2022-170, https://crtc.gc.ca/eng/archive/2022/2022-170.htm, para 133: "… the Commission stated that botnets pose a significant threat to consumer privacy when they access personal information, and that blocking botnet communications can help protect consumers. However, this protection is achieved by monitoring Internet traffic. The consequences for consumer privacy caused by monitoring are important issues for any potential blocking framework to address."

[5] The testimony of the Intelligence Commissioner of Canada before this Committee is explicit and incontestable on this point.

[6] CSTAC, Security Best Practices for Canadian Telecommunications Service Providers, v 1.1, January 20, 2020: 3.2.3.15; 3.2; CSTAC, Information Sharing, Reporting and Privacy Standard for Canadian Telecommunications Service Providers", v 1.1, March 31, 2020, https://ised-isde.canada.ca/site/spectrum-management-telecommunications/sites/default/files/attachments/2022/CSTAC_CCCSTinformationSharingAndReporting2020_01EN.pdf, notably, section 1.2(4): "Limit information shared to only that required to resolve issues and avoid sharing of personal information."; Internet Engineering Task Force (IETF), RFC 6561: Recommendations for the Remediation of Bots in ISP Networks, March 2012, https://datatracker.ietf.org/doc/html/rfc6561, sections 4, 8 and 10: "The ISP should attempt to detect the presence of bots using methods, processes, and tools that maintain the privacy of the personally identifiable information (PII) of their customers."; CETD CRTC 2022-170, https://crtc.gc.ca/eng/archive/2022/2022-170.htm, para 141 and Appendix 1: "the Commission would expect TSPs to…ensure that confidential customer information collected, used or disclosed for the purpose of the blocking mechanism is limited to that which is essential for that purpose, and only for so long as it is necessary for that purpose, and that the information collected is not used or disclosed for any other purpose"; OECD, Council Recommendation on Digital Security of Critical Activities, December 2019, OECD/LEGAL/0456, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0456, section VIII(3)(e).

[7] Bill C-8, proposed ss 15.2(9) and 15.8(2) of the *Telecommunications Act*. For relevant safeguards see: CETD CRTC 2022-170, https://crtc.gc.ca/eng/archive/2022/2022-170.htm,para 141 and Appendix 1.

still be required to comply with federal privacy laws, these laws permit TSPs to collect, use, retain and disclose personal information where "required by law", including under orders envisioned by Bill C-8.[8]

We note that the Committee has heard testimony that sought to minimize the privacy implications of Bill C-8. However, if the framework put in place by Bill C-8 did not intend to include access to personal or de-identified data at all, it would be simple to categorically exclude any access or interception from Bill C-8. As that is not the case, Bill C-8 needs to ensure the appropriate privacy framework is in place so that this highly sensitive personal data is not misused.

a. Strictly limit the minister's ability to intercept and access Internet traffic

Under Bill C-8, the government will be able to compel TSPs to intercept categories of Internet traffic despite the highly sensitive nature of this information.

Under proposed paragraph 15.2(2)(m), the government will be able to order a TSP to do any "specified thing" considered on reasonable grounds to be necessary for securing Canada's telecommunications networks. While proposed section 15.2(4) prevents the government from ordering TSPs to intercept "private communications" as this term is defined in Part VI of the *Criminal Code*, it does not impose any restrictions on the interception of metadata despite the heightened sensitivity of this type of customer Internet traffic.[9] As a result, TSPs can be compelled to intercept and retain significant amounts of their customer's Internet activities for cybersecurity purposes.

The limitation in proposed section 15.2(4) ignores the highly sensitive nature of metadata, which can be as revealing of our online activities and personal lives than the private communications being exempted from interception. This is reflected in our constitutional jurisprudence, which has recognized that metadata such as Internet browsing activity is highly sensitive and protected by section 8 of the *Charter*.[10]

CCLA would therefore recommend amending Bill C-8 to ensure it is not used to compel interception of sensitive internet traffic data.

Recommendation 1. Expand subsection 15.2(4) so that it excludes interception of metadata.

> 15.2(4) For greater certainty, despite subsection (2), the Minister is not permitted to order a telecommunications service provider to intercept **transmission data, tracking data,** a private communication or a radio-based telephone communication, as those terms are defined in section**s** 183**, 492.1 and 492.2** of the Criminal Code.

Bill C-8 grants the minister the broad power to compel interception and production of any information considered on reasonable grounds to be relevant for the exercise or enforcement of the

[8] *PIPEDA*, paragraphs 7(1)(e)(ii), (2)(d) and (3)(i); *Privacy Act*, sections 8(2)(b), 7(b) and 5(1).

[9] Bill C-8, proposed sections 15.2(4) of the *Telecommunications Act*. Part VI of the *Criminal Code* only applies to "private communications", which does not include "metadata". See discussion in: Tamir Israel & Christopher Parsons, "Gone Opaque? An Analysis of Hypothetical IMSI Catcher Overuse in Canada", Ver.2, August 2016, https://citizenlab.ca/wp-content/uploads/2016/09/20160818-Report-Gone_Opaque.pdf, pp 77-82; Craig Forcese, "Law, Logarithms, an Liberties: Metadata Collection Initiatives" in M. Geist, Ed *Law, Privacy and Surveillance in Canada in the Post-Snowden Era* (University of Ottawa Press, 2015), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2436615; *Re X*, 2017 FC 1047, para 100.

[10] See, e.g. *R v Cole*, 2012 SCC 53, paras 47-48.

Minister's powers under Part 1.[11] It uses a permissive "relevance" standard and fails to require orders to be necessary and proportionate. It also grants this power with no requirement for prior judicial authorization and therefore falls short of the constitutional minimum.

Under proposed section 15.4, the minister will also be able to require TSPs to provide information that is not under their possession or control, meaning that TSPs can be compelled to intercept and retain sensitive network traffic of Internet users.[12] The minister will also be able to require access to private communications and network metadata of Internet users that TSPs have intercepted in the course of their own cybersecurity activities.[13] Section 15.4 does not require prior judicial authorization, or limit the use of this power to situations that are necessary and proportionate.

Section 8 of the *Charter* requires authorization from an independent person acting judicially before the government can interfere with a reasonable expectation of privacy.[14] Courts have recognized that when people participate in a highly regulated activity, such as driving a licensed vehicle or offering securities, there is a lower expectation of privacy in relation to that participation. This is the case where records are prepared in the context of a highly regulated business and do not engage aspects of digital identity that the constitutional right to privacy is intended to protect.[15]

Using the Internet is not a regulated activity and, in fact, engages significant privacy expectations. By failing to require prior judicial authorization before the minister can demand access to and interception of sensitive personal information, Bill C-8 falls far short of the constitutional minimum required by section 8 of the *Charter*. Bill C-8's broad production and interception authorization is also not limited in application to regulated entities such as TSPs, but instead applies to "any person", further expanding the significant intrusiveness of this power.

CCLA therefore recommends adding prior judicial authorization to Bill C-8's ministerial data access power, limiting this power so that it cannot be used to compel the interception of Internet users' traffic, so that it is limited in application to TSPs, and so that the power can only employed when it is necessary and proportionate to do so.

Under this recommendation, the minister will continue to be able to demand general indicators of compromise and other threat information under the possession and control of TSPs but will be required to obtain prior judicial authorization or to establish that exigent circumstances are in place before demanding production of personal information.

Recommendation 2. Limit the production authorization in s 15.4 to TSPs and ensure that personal information can only be obtained if proportionate, necessary and judicially authorized.

---

[11] Bill C-8, part 1, proposed section 15.4 of the *Telecommunications Act*.

[12] Bill C-8, part 1, proposed section 15.4 of the *Telecommunications Act*. By contrast, production and preservation orders in the *Criminal Code* are explicitly limited to information that is in the possession and control of service providers to prevent the use of these powers to intercept or retain information TSPs would not already have in their possession. See, eg, ss 487.012, 487.014, 487.016 and 487.017.

[13] TSPs are permitted to intercept private communications in the course of their own cybersecurity activities under section 184(c) of the *Criminal Code*. See also: *R v Jones*, 2017 SCC 60, para 59.

[14] *Hunter v Southam Inc*, [1984] 2 SCR 145.

[15] *British Columbia Securities Commission v Branch*, [1995] 2 SCR 3; *Thomson Newspapers Ltd v Canada (Director of Investigations and Research, Restrictive Trade Practices Commission)*, [1990] 1 SCR 425.

15.4 **(1)** The Minister may require any ~~**person**~~ **Telecommunications Service Provider** to provide to the Minister or any person designated by the Minister, within any time and subject to any conditions that the Minister may specify, any information **other than personal or de-identified information** that **is in its possession and control when it receives the order and that** the Minister believes on reasonable grounds is ~~**relevant**~~ for the purpose of making, amending or revoking an order under section 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.

(2) On *ex parte* application made by the Minister or any person designated by the Minister, a justice or judge may order any Telecommunications Service Provider to prepare and produce a document containing any information that is specified in the order and that is in its possession and control when it receives the order.

(3) Before making an order under (2), the justice or judge must be satisfied by information on oath that there are reasonable grounds to believe that:

(a) the order is necessary for the purpose of making, amending or revoking an order under section 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; and

(b) that the information is in the possession or control of the Telecommunications Service Provider.

(4) The Minister may require any Telecommunications Service Provider to provide any information if the conditions for obtaining an order under (2) exist but by reason of exigent circumstances it would be impracticable to obtain an order.

---

b. Ensure personal data obtained through the Bill is only disclosed where it is necessary to achieve cybersecurity objectives.

Proposed clause 15.5 of Bill C-8 creates a vehicle for placing limits on the dissemination of personal information obtained by the Minister through proposed section 15.4.

These restrictions are contingent on whether a TSP chooses to designate personal information of its customers as confidential and further chooses to protect that personal data from being disseminated broadly once it is obtained by the government. Privacy rights should not be contingent on a TSP's discretion.

Recommendation 3. Amend section 15.5 so that people's privacy cannot be violated at the discretion of service providers

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; **and**

(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**~~.

(1 bis) Any personal and de-identified information provided under section 15.4 is deemed to be confidential. ...

(3) Subject to subsection (4), no person shall knowingly disclose or knowingly permit to be disclosed any information that is designated **or deemed** as confidential. …

15.7 (1) Any information collected or obtained under this Act, other than information designated **or deemed** as confidential under ~~**sub**~~section 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.

Even where personal information is deemed to be confidential, it may still be disclosed to any entity if authorized by law or if the Minister is of the view that doing is necessary to secure the Canadian telecommunications system and it may be exchanged between a set of designated federal government entities if necessary for the purpose of overseeing the Minister's powers under Part 1 of Bill C-8.[16]

Recommendation 4.

15.5 (4) 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 **Minister believes on reasonable grounds that** disclosure is necessary~~**, in the Minister's opinion,**~~ to secure the Canadian telecommunications system, including against the threat of interference, manipulation or disruption **and is proportionate to that objective**.

…

15.6 (1) Despite section 15.5, **the following persons and entities may collect information from and disclose information to each other, including confidential information,** to the extent that **the persons or entities believe on reasonable grounds that it** is necessary for any purpose related to the making, amending or revoking of an order under section 15.1 or 15.2 or a regulation under paragraph 15.8(1)(a) — or to verifying compliance or preventing non-compliance with such an order or regulation ~~**— the following persons and entities may collect information from and disclose information to each other, including confidential information**~~:

---

c. Prevent misuse of personal data obtained through Bill C-8

Bill C-8 does not place any restrictions on how personal data obtained through its provisions could be used for purposes unrelated to cybersecurity, including for the purpose of foreign intelligence and criminal investigations. This constitutes a significant expansion in the government's investigative capabilities. The use of personal data obtained through provisions proposed by Bill C-8 should be strictly limited to cybersecurity purposes.

Bill C-8 represents a significant expansion of the Communication Security Establishment's (CSE) ability to access personal data of people in Canada. The CSE is generally prohibited from directing

[16] Bill C-8, proposed ss 15.5(4)(c) and 15.6(1) of the *Telecommunications Act*.

its activities at people in Canada, including its cybersecurity activities.[17] The CSE is specifically restricted from conducting wide-ranging surveillance on Canadian internet traffic through a prohibition from acting on Canadian TSP networks without the written request from the operator of a given Canadian TSP and an authorization confirmed by the Intelligence Commissioner on the basis that the proposed CSE activity will be necessary and proportionate.[18]

Bill C-8 effectively bypasses all these critical safeguards—the Minister will be able to require, on advice from the CSE, access to personal data from Canadian TSP networks[19] and then further authorized to share this personal information with the Establishment.[20] As the CSE will not be acting under its authorization framework, it will not be required to limit its activities to what is necessary and proportionate to its objectives as would otherwise be the case.

CCLA supports the Intelligence Commissioner's recommendation that Bill C-8 be amended to ensure that the CSE's activities be conducted under the Bill be conducted under an authorization.[21]

Recommendation 5. Ensure the CSE's activities under Bill C-8 are duly authorized

> **15.6bis Despite sections 15.5(4) and 15.5, the Communications Security Establishment must not carry out any activities in furtherance of the administration of sections 15.1 to 15.9 of this Act unless it does so under a valid authorization issued under subsection (2).**
>
> **(2) The Minister may issue an authorization to the Communications Security Establishment that authorizes it to carry out activities in furtherance of the administration of sections 15.1 to 15.9 of this Act only if he or she concludes that there are reasonable grounds to believe that**
>
> **(a) any activity that would be authorized is reasonable and proportionate, having regarding to the nature of the objective to be achieved and the nature of the activities;**
>
> **(b) any information acquired under the authorization will be retained no longer than is reasonably necessary;**
>
> **(c) the consent of all persons whose information may be acquired could not reasonably be obtained;**
>
> **(d) any information acquired under the authorization is necessary to identify, isolate, prevent or mitigate harm to electronic information infrastructures designated under subsection 21(1) as being of importance to the Government of Canada that is a Telecommunications Service Provider;**
>
> **(e) the measures referred to in section 24 of the *Communications Security Establishment Act* will ensure that information acquired under the authorization that is identified as relating to a Canadian person or a person in Canada will be used, analysed or retained only if the information is essential to identify, isolate, prevent or mitigate harm to electronic information infrastructures designated under subsection 21(1) as being of importance to the Government of Canada that is a Telecommunications Service Provider.**

---

[17] *Communications Security Establishment Act,* SC 2019, c 13, s 76 ["*CSE Act*"], s 22(1) and (4) but subject to s 23(1)(b) and 23(3).

[18] *CSE Act*, ss 33(3) and 40(4).

[19] Bill C-8, proposed sections 15.4, 15.5(4)(c) and 15.6(1) of the *Telecommunications Act* and *CSE Act*, ss 23(1)(b)

[20] Bill C-8, proposed 15.5(4)(c) and 15.6(1) of the *Telecommunications Act*.

[21] Testimony of the Hon. Simon Noël, Intelligence Commissioner of Canada, before SECU, October 30, 2025, *45th Parl 1st Sess No 010*, https://www.ourcommons.ca/Content/Committee/451/SECU/Evidence/EV13724995/SECUEV10-E.PDF, p 6.

II. Prevent TSPs from expanding their ability to conduct surveillance & blocking

Several elements of Bill C-8 can be used to order TSPs to adopt new intrusive surveillance capabilities they currently do not possess. In some instances, these new surveillance capabilities will undermine cybersecurity.

a. Prevent the Bill from undermining Cybersecurity by weakening encryption

Bill C-8 can be used to undermine cybersecurity by weakening essential technical safeguards, notably encryption. Robust encryption is critical to any efforts to secure telecommunications systems. Despite this technical reality, government agencies have repeatedly failed to prioritize cybersecurity over surveillance and sought to bypass encryption in various ways that undermine the security of everyone.[22]

Bill C-8 includes a number of powers that could be used to secretly compromise encryption in TSP networks with the objective of facilitating surveillance. Bill C-8 empowers the government to prohibit a TSP from upgrading any specified product or service as a means of impeding the adoption of a more robust form of encryption[23] or require a TSP to adopt any specified standard, which includes keeping in place weaker encryption standards.[24] Bill C-8 also empowers the government to order a TSP to do or refrain from doing any "specified thing", a broad open-ended power that could be used to undermine security in numerous ways with the objective of facilitating surveillance.[25]

CCLA recommends that Bill C-8 be amended to ensure that its broad open-ended powers are not used to undermine encryption.

Recommendation 6. Amend section 15.2 to ensure that no order issued under it can undermine cybersecurity.

> **15.2 (2.3) For greater certainty, despite subsection (2), the Minister is not permitted to make an order that would have the effect of degrading, removing, defeating or bypassing any technical safeguard including encryption.**

[22] Lex Gill, Tamir Israel & Christopher Parsons, "Shining a Light on the Encryption Debate: A Field Canadian Field Guide", May 2018, https://citizenlab.ca/wp-content/uploads/2018/05/Shining-A-Light-Encryption-CitLab-CIPPIC.pdf; Kate Robertson & Ron Deibert, "Ottawa Wants the Power to Create Secret Backdoors in our Networks to Allow for Surveillance", May 29, 2024, *The Globe and Mail*, https://www.theglobeandmail.com/opinion/article-ottawa-wants-the-power-to-create-secret-backdoors-in-our-networks-to/; Harold Abelson, Ross Anderson, Steven M Bellovin, Josh Benaloh, Matt Blaze, Witfield Diffie, John Gilmore, Matthew Green, Susan Landau, Peter G Neumann, Ronald L Rivest, Jeffrey I Schiller, Bruce Schneier, Michael Specter & Daniel J Wetzner, "Keys under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications", MIT-CSAIL-TR-2015-026, July 6, 2015, https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf; "Government Needs to Fix Dangerous Flaws in Federal Cybersecurity Proposal", September 26, 2025, https://ccla.org/privacy/fix-dangerous-flaws-in-federal-cybersecurity-proposal/. Christopher Parsons, "The Governance of Telecommunications Surveillance: How Opaque and Unaccountable Practices and Policies Threaten Canadians", (Telecom Transparency Project, 2015) https://christopher-parsons.com/wp-content/uploads/2022/07/1d2f2-the-governance-of-telecommunications-surveillance_-how-opaque-and-unaccountable-practices-and-policies-threaten-canadians-parsons-2015.pdf.

[23] Bill C-8, proposed paragraph 15.2(2)(g) of the *Telecommunications Act*.

[24] Bill C-8, proposed paragraph 15.2(2)(l) of the *Telecommunications Act*.

[25] Bill C-8, proposed paragraph 15.2(2)(m) of the *Telecommunications Act*.

b. Limit expansion of intercept & cyberattack capabilities

As noted above, TSPs cannot be ordered to intercept private communications under Bill C-8. But they can be ordered to adopt new capabilities that would enhance their ability to intercept private communications.

Under Bill C-8, service providers can be compelled to install highly intrusive surveillance and capabilities for cybersecurity purposes. Once these capabilities are in place, Bill C-8 fails to ensure that their use is limited to cyberdefence. CCLA is particularly concerned that the capabilities imposed through Bill C-8 will be used by security agencies to achieve objectives that are unrelated to cybersecurity.

Capabilities adopted by Canadian TSPs for the purpose of addressing cybersecurity threats have already been co-opted to block content for other purposes, including to address alleged intellectual property infringement.[26] Without additional safeguards in place, capabilities imposed on TSPs by means of Bill C-8 may have far-reaching implications that extend well beyond its cyber-defence objectives.

Under Bill C-8, the minister can impose any condition on a TSP's use of different types of equipment and compel a TSP to implement specified standards.[27] Under proposed paragraph 15.2(2)(l), the Minister will be empowered to impose Deep Packet Inspection capabilities onto a TSP's use of different types of network equipment for the purpose of monitoring cybersecurity activity. Deep Packet Inspection is a highly intrusive network technology that many Canadian TSPs have decided not to adopt out of respect for the privacy of their users.[28] Under proposed paragraph 15.2(2)(c), TSPs can be compelled to adopt any standard, including any of a number of standards that would require TSPs to expand their ability to intercept private communications.[29]

Recommendation 7. Amend 15.2 to prevent adoption of intercept capabilities:

> **15.2(4)*bis* For greater certainty, the Minister is not permitted to order a telecommunications service provider to introduce new capabilities related to the extraction, interception or organization of information.**

[26] *Teksavvy Solutions v Bell Media*, 2021 FCA 100.

[27] Bill C-8, proposed paragraphs 15.2(2)(c) and (l) of the *Telecommunications Act*.

[28] *Rogers Media v Doe*, 2022 FC 775, para 314 and ORDER, clause 15.1: "Any personal information collected to achieve the objectives of this order, or collected through any Deep Packet Inspection (DPI) or other system adopted to achieve the objectives of this order, will be used solely for the purposes of providing notice to customers, will not be disclosed, and will only be retained as long as is strictly necessary to ensure the integrity of the customer notification obligation."; Telecom Regulatory Policy CRTC 2009-657, paras 96-105.

[29] United States, Federal Bureau of Investigation, National Domestic Communications Assistance Center, "Lawful Intercept Standards", September 24, 2019, https://ndcac.fbi.gov/file-repository/listandardscip-1.pdf/view, archived at: https://web.archive.org/web/20251211060730/https://ndcac.fbi.gov/file-repository/listandardscip-1.pdf/view; Christopher Parsons, "The Governance of Telecommunications Surveillance: How Opaque and Unaccountable Practices and Policies Threaten Canadians", (Telecom Transparency Project, 2015) https://christopher-parsons.com/wp-content/uploads/2022/07/1d2f2-the-governance-of-telecommunications-surveillance_-how-opaque-and-unaccountable-practices-and-policies-threaten-canadians-parsons-2015.pdf.

III. Add safeguards for people, websites or services that might be disconnected from the Internet

Under proposed section 15.2, a TSP can be ordered to disconnect targets of the order from accessing the Internet or mobile networks where there are reasonable grounds to believe doing so is necessary to secure Canadian telecommunications systems against cyberthreats. It can be used to disconnect websites or people and to render services inaccessible at the network layer.

In its testimony before this Committee, the government has explicitly acknowledged that Bill C-8 includes the power to disconnect people from the Internet, while downplaying the significance of this new power.[30] However, the proposed section is drafted broadly. Cyberthreats commonly emerge from compromised devices, meaning people could be disconnected under Bill C-8 without warning.

The regime imposed by Bill C-8 does not require notifying end users they are to be disconnected or to assist in taking whatever steps might be necessary to facilitate their reconnection. To the contrary, in light of Bill C-8's extensive secrecy provisions, TSPs could be wholly prohibited from telling their customers why they have been disconnected.[31]

The operation of this provision could lead to significant consequences in particular for people who are disconnected from the telecommunication network under this section on the basis that their home computers, routers, smart devices or mobile phones have been compromised by bad actors without their awareness.[32]

Subsection 15.2(1) can also be used to block people in Canada from accessing public websites where the Minister considers it necessary to secure the Canadian telecommunications system. The public should be promptly notified in the event that this occurs.

CCLA recommends that Bill C-8 be amended to require individual notification for people whose internet access is blocked as well as public notification for any blocked websites.

Bill C-8 does not require that these disconnection powers be applied already identified people. It could therefore be used to impose Artificial Intelligence or algorithmically driven blocking mechanisms despite the propensity for these types of mechanisms to produce false positives.[33] Bill C-8 lacks the appropriate mechanisms to ensure these types of tools are properly audited and will

---

[30] Testimony of the Hon. Gary Anandasangaree, Minister of Public Safety, before SECU, November 6, 2025, *45th Parl 1st Sess No 010*, https://www.ourcommons.ca/Content/Committee/451/SECU/Evidence/EV13738359/SECUEV12-E.PDF:

> What is accurate is that, in very limited circumstances, when an individual who may have access to the Internet through a service provider has posed a risk to the safety and security of our critical infrastructure and demonstrated the type of continued behaviour that could harm our critical infrastructure and thereby many other systems, there is, in very limited scope, the ability to terminate their Internet services. It is in exceptional circumstances; it's not on a routine basis.

[31] Bill C-8, proposed s 12.2(5) of the *Telecommunications Act*.

[32] Compliance and Enforcement and Telecom Decision CRTC 2022-170, https://crtc.gc.ca/eng/archive/2022/2022-170.htm, paras 58 "In reality, most end-users with a malware-infected device are unaware of the infection Even when notified, they often lack the technical competency to remediate the issue". By contrast to the general framework for network layer blocking of botnet traffic, under Bill C-8 the government will be able to order end device disconnection of specific users.

[33] *Rogers Media v Doe*, 2022 FC 775, paras 253, 258 and 319; CETD CRTC 2022-170, paras 174-176.

not lead to over-blocking of end users or content. It is therefore an inappropriate vehicle for imposing this type of disconnection requirement.

CCLA therefore further recommends that Bill C-8 be amended to compel individualized assessments before any specific user or website is disconnected from the telecommunications system.

Recommendation 8.

15.2(5) 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.

15.2(5*bis*) Despite any provision included in an order further to subsection 15.2(5), any order issued under subsection 15.2(1) that:

(a) prevents a person in Canada from accessing the telecommunications system will include a requirement to promptly notify that person of the order; or

(b) prevents access to a publicly available online resource through a Telecommunications Service Provider will include a requirement to promptly notify the public of the order.

IV. Include a right to *de novo* review by anyone impacted by Bill C-8

Bill C-8 creates no statutory appeal. Bill C-8 does not include any procedural safeguards for any individual or stakeholder impacted by its framework.

Contrary to other regulatory processes under the *Telecommunications Act* or other statutes, individuals and stakeholders impacted by government orders or regulations issued under Bill C-8 have no right to participate in the generation of the orders in question and in many instances will not even be made aware that such orders are being contemplated in time to provide relevant information that would inform those orders.

Judicial review is not an acceptable appeal mechanism in this context, as judicial review is focused on assessing the reasonableness of the decision being advanced rather than on whether that decision is premised on correct determinations of fact and law.[34] The ability to adduce evidence at judicial review is also highly limited, as the underlying assumption behind a judicial review proceeding is that impacted individuals have had an opportunity to place their evidence before the primary decision-maker.[35]

Despite this lack of safeguards, ministerial orders or regulations issued under part 1 of Bill C-8 are only subject to judicial review under a deferential standard and with limited ability to adduce evidence. This is despite the fact that action under Bill C-8 can have significant implications for individuals or for the telecommunications system more broadly.

CCLA recommends that Bill C-8 be amended to allow for *de novo* judicial review of any order that directly impacts individuals.

[34] *Canada (Minister of Citizenship and Immigration) v Vavilov*, 2019 SCC 65, para 125.

[35] See, for example, *Sharma v Canada (Attorney General)*, 2018 FCA 48, paras 7-9.

Recommendation 9. Amend Bill C-8 to include a statutory appeal for any person impacted by an order or regulation issued under the bill.

15.9 (1) Anyone directly affected by an order issued under section 15.1 or 15.2 or a regulation made under paragraph 15.8(1)(a) may apply to the Federal Court for a hearing regarding any matter in which the order or regulation was made.

(2) The Minister may appear as a party to any hearing applied for under subsection (1).

(3) In an application under subsection (1), the Federal Court may exercise any of its powers under section 18.1 of the *Federal Courts Act*.

(4) The following rules apply to ~~**judicial review proceedings in respect of an order made under section 15.1 or 15.2 or a regulation made under paragraph 15.8(1)(a) applications under subsection (1) 15.9 (1)**~~ **applications under (1):**

END OF DOCUMENT