UNIVERSITY OF TORONTO

munk school
OF GLOBAL AFFAIRS & PUBLIC POLICY

Submission to the Standing Committee on Public Safety and National Security of Bill C-8, *An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts*

Submission by Kate Robertson, Senior Research Associate
Citizen Lab, Munk School of Global Affairs & Public Policy
University of Toronto

Part 1. Overview

1. This brief sets out targeted recommendations to respond to constitutional deficits in Bill C-8 that were not addressed during the study and amendment of Bill C-26. By way of overview, two priorities should be the focus of this committee's study and amendment of Bill C-8: the need for a judicial warrant requirement for the bill's warrantless collection powers, and the need to integrate protection for encryption and communications security.

2. First, Bill C-8 proposes very broad information collection and sharing powers. Although government officials have often asserted that those powers will not be applied to the personal information of people in Canada, the text of the legislation is explicit that personal information would be collected without a warrant. The Intelligence Commissioner of Canada further testified before the Senate in respect of Bill C-26, and stated: "In my experience as IC, when CSE conducts cybersecurity activities, there will be the collection of information in which there is a reasonable expectation of privacy. This means there is effectively a seizure of private information."

3. Addressing **the warrantless nature of this collection power should be this committee's priority in studying the legislation**. The Intelligence Commissioner's testimony highlighted that "[t]he glaring absentee in this bill is the Canadian public. The information that is collected is Canadians' personal information." The warrantless seizure of private information is a significant constitutional issue. The Intelligence Commissioner testified:

> In all cases I've known, you need a warrant. You can obtain it from the justice of the peace, you can obtain it from the Federal Court, and you can obtain from a quasi-judicial officer. **In the present bill, there is no such warrant requirement** — …Normally, that would go against the *Charter*.
>
> I've read the *Charter* Statement by the minister, and I haven't seen anything in that statement that would give a justification under section 1 of the *Charter*. …In this case, it's totally absent.

4. It must be noted that while government officials have previously asserted that other safeguards have been added to address privacy risks, these new safeguards **are not applicable to the Ministerial collection powers at issue**:

   - A new Parliamentary reporting obligation that was added during the study of Bill C-26 is not applicable to the information collection power (s. 15.81 of Part 1);
   - New provisions requiring notice to NSIRA and NSICOP are not applicable to the information collection power;
   - The stipulation that Bill C-8 does not authorize the interception of private communications is not applicable to the collection of numerous categories of sensitive data that may be seized

under the Minister's collection power under s. 15.4. As the Privacy Commissioner of Canada emphasized during testimony on Bill C-26, the legislation could result in the inappropriate sharing of subscriber account information, communication data, website visits, metadata, location data and financial data.[1]

5. A Federal Court warrant requirement over the collection power in s. 15.4 (recommended by myself and other witnesses and civil society organizations during the study of Bill C-26), should be prioritized to address this core constitutional issue. This recommendation is discussed in Part 2 of this brief.

6. Secondly, **an amendment should be prioritized to prevent Bill C-8's broad order-making powers from undermining encryption and communications security in Canada's telecommunication networks**. By contrast, in June 2025, the federal government tabled Bill C-2 (the *Strong Borders Act*), which also proposes to grant broad ministerial powers to order changes in the telecommunication networks in Canada (Part 15 of Bill C-2). In tabling the legislation, the federal government acknowledged that a statutory provision is required to prevent orders from being used to compromise encryption and undermine communications security. (A clause is currently proposed in Bill C-2, but its text has received criticism for being vague and undefined.)

7. In contrast, **there is no protection in Bill C-8 for encryption and communications security**. In this brief, Part 3 addresses this by proposing to add an interpretive clause to s. 15.2 clarifying that "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." The phrase "confidentiality, availability, or integrity" is a widely recognized term (it is used, for example, by federal agencies, the Canadian Centre for Cyber Security, and Public Safety Canada) to describe the three essential elements of strong cybersecurity. This recommendation was also made in Recommendation 1 in the Joint Civil Society Brief on Bill C-26.

8. This brief expands upon both of these priorities, and sets out a total of nine recommendations to address the constitutional and cybersecurity risks that remain in Bill C-8:

    - **Part 2: Bill C-8 and the *Canadian Charter of Rights and Freedoms* ("*Charter*")**: Part 2 of this Brief discusses the nexus between Bill C-8 and the *Charter*. It focuses, in particular, on the impact of Bill C-8 on freedom of expression (Subsection 2(b)) and privacy (Section 8). The *Charter* implications of the proposed legislation should be a central consideration for this Committee, and throughout the Parliamentary process ahead. Part 2 also provides substantive analysis and recommendations for amendments to address thematic deficiencies in Bill C-8.

    - **Part 3: Bill C-8's encryption-undermining powers:** Part 3 addresses the need for amendment to ensure that the federal government is not authorized to compel network operators to compromise the integrity of encryption and communications security.

[1] SECU proceedings on Bill C-26, Testimony of the Privacy Commissioner of Canada Phillipe Dufresne, February 15, 2024.

Part 2. Bill C-8 and the *Charter*

9. In 2022, Citizen Lab published *Cybersecurity Will Not Thrive in Darkness: A Critical Analysis of Proposed Amendments in Bill C-26 to the Telecommunications Act* ("*Cybersecurity Will Not Thrive in Darkness*").[2] The report was authored by Dr. Christopher Parsons.[3] Dr. Parsons critically examined the proposed draft legislation under Bill C-26, including identified deficiencies. In doing so, Dr. Parsons provided necessary historical and international context surrounding the federal government's proposed telecommunications sector reform. Canada is not the first of its allies to introduce new government powers as a result of heightened concern and awareness surrounding real and pressing risks to critical infrastructure. However, Dr. Parsons identified that although the draft legislation may advance important goals, it contained thematic deficiencies that risked undermining its effectiveness. This report is set out in **Appendix B**.

10. The following recommendations integrate the analysis in *Cybersecurity Will Not Thrive in Darkness*, and address subsequent developments since the report was published, including the study and amendment of Bill C-26 by the Standing Committee on Public Safety and National Security (SECU):

Freedom of Expression and Section 2(b) of the *Charter*

11. The current draft of Bill C-8's excessive secrecy and confidentiality provisions jeopardizes the right to freedom of expression under section 2(b) of the *Charter*. The principles of open courts and open government are components of free expression. Denial of access to government information may effectively preclude meaningful public discussion on a matter of public interest. Where restrictions on access substantially impede meaningful discussion and criticism about matters of public interest, the government must reasonably justify its infringement of the freedom of expression.[4]

12. The government's *Charter* statement focuses on the speech of the commercial entities who will be directly regulated under Bill C-8. The *Charter* statement posits that because restrictions on commercial speech do not tend to implicate the core values of section 2(b), restrictions can be more easily justified.[5] However, this analysis does not account for whether individuals' *Charter* rights will be impeded, failing to distinguish between commercial actors and individuals who use telecommunication services. The excessive secrecy and confidentiality provisions in the bill also restrict the public's and media's right to know and access information.

---

[2] Christopher Parsons, "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, University of Toronto, Oct. 2022.
[3] This report was also published at the time that Dr. Parsons was a senior researcher at the Citizen Lab. As such, the report's conclusions and recommendations also do not necessarily reflect those of Dr. Parsons' current employer.
[4] *Ontario (Public Safety and Security) v. Criminal Lawyers' Association*, 2010 SCC 23; *ARPA Canada and Patricia Maloney v R.*, 2017 ONSC 3285. This inquiry involves a balancing of any countervailing considerations (such as a privilege) that might militate against disclosure.
[5] Department of Justice Canada, "*Charter* Statement: Bill C-26: An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts", December 14, 2022.

13. The recent Citizen Lab report, *Finding You: The Network Effect of Telecommunications Vulnerabilities for Location Disclosure*, highlights several ways in which excessive secrecy surrounding telecommunications oversight has itself endangered the public. The authors note historical deficiencies in oversight and accountability of network security, which have led to geolocation-related threats associated with contemporary networks:

> Decades of poor accountability and transparency have contributed to the current environment where extensive geolocation surveillance attacks are not reported. This status quo has effectively created a thriving geolocation surveillance market while also ensuring that some telecommunications providers have benefitted from turning a blind eye to the availability of their network interconnections to the surveillance industry.[6]

14. Citizen Lab's research highlights the substantial public interest in enabling the media, security researchers, civil society, and the public to access information about telecommunications policies and regulations. As security researchers have noted, "the most promising route to full accessibility [in cybersecurity] lies in collaboration between vendors, advocacy groups, and the government."[7] Civil society and the broader business community can press "regulators, policy makers, and politicians to actively compel telecommunications providers to adopt appropriate security postures to mitigate the pernicious and silent threats associated with geolocation surveillance,"[8] and other similar security risks.

15. While some confidentiality will be appropriate to ensure that unresolved security vulnerabilities are effectively brought into control, the powers in Bill C-8 go further than what is required to accomplish cybersecurity and national security objectives.

16. **In light of unresolved deficits concerning excessive secrecy, I recommend the following:**

- **Recommendation 1: Non-Disclosure Orders Should Be Time Limited.** Bill C-8 proposes gag provisions with respect to Orders in Council or Ministerial Orders, which are not limited either temporally (i.e., how long is secrecy necessary?) or substantively (i.e., what circumstances justify secrecy?). The legislation should be amended to include time constraints surrounding non-disclosure orders. If the Minister requires additional time beyond the time limit, I agree with the *Joint Civil Society Senate Submission on Bill C-26* that the government should be required to obtain a federal court order to authorize any further extension of the non-disclosure order.[9]

- **Recommendation 2: The Circumstances Purporting to Justify Confidentiality in a Non-Disclosure Order Should Be Defined In The Legislation.** In the *Canada Evidence Act*, the

[6] Gary Miller and Christopher Parsons. "Finding You: The Network Effect of Telecommunications Vulnerabilities for Location Disclosure," Citizen Lab Research Report No. 171, University of Toronto, Oct. 2023. Dr. Parsons was a senior researcher at the Citizen Lab at the time the report was being produced. While the report's findings will be the subject of comments and recommendations in this brief, those comments do not necessarily reflect those of his current employer.

[7] Karen Renaud and Lizzie Coles-Kemp, "Accessible and Inclusive Cyber Security: A Nuanced and Complex Challenge", SN Computer Science (2022) 3: 346, at p. 2 of 14.

[8] *Finding You*, *supra* at p. 33.

[9] *Joint Civil Society Senate Submission on Bill C-26*, at p. 8.

Act constrains secrecy to where it is justified on grounds that disclosure "would be injurious to international relations or national defence or national security."[10] In contrast, in Bill C-8 there are no limits to the circumstances in which non-disclosure orders could be imposed. Given the important and adverse free expression consequences of excluding the public from access to orders, the legislation should specify what grounds justify secrecy surrounding the issuance of a non-disclosure order.

Privacy Impacts and Section 8 of the *Charter*

17. The telecommunication operators at issue in Bill C-8 are conveyors of the most private information known to our legal system. Bill C-8's powers are not balanced to reflect this reality.

18. Section 15.4 of Bill C-8 would give the Minister of Industry an unprecedented, warrantless power to collect telecommunications data, and to share this information widely across the federal government–including with Canadian Security and Intelligence Service (CSIS) and the Communications Security Establishment (CSE). As a matter of law, the proposed power is presumptively contrary to section 8 of the *Charter*, because it would authorize the collection of information that is subject to a reasonable expectation of privacy without prior independent judicial authorization.[11]

19. Although the legislation stipulates that the powers do not authorize the interception of private communications (section 15.2(2.2)), telecommunication providers host volumes of sensitive personal information that could be collected in circumstances that do not meet the technical definition of an intercept of a private communication. As the Privacy Commissioner of Canada emphasized during testimony on Bill C-26,[12] the legislation could result in the inappropriate sharing of subscriber account information, communication data, website visits, metadata, location data and financial data. There is no reasonable dispute that these information sources carry significant privacy interests.[13]

20. The collection and use of information by security and intelligence agencies about Canadians or persons in Canada is a core matter of public and constitutional concern.

21. Only a few years ago, Canada's national security laws underwent a massive overhaul in the *National Security Act, 2017*.[14] In this comprehensive law reform package, Parliament attempted to strike a controversial equilibrium concerning the need for carefully calibrated protections and constraints surrounding the collection of information in Canada. Protections and limitations vary significantly between security and intelligence bodies. The "mandates of Canada's different security and intelligence agencies…matter enormously in deciding the lawfulness of a given investigative activity."[15] The CSE, for example, is prohibited from directing its activities at Canadians or people in Canada, and there are a series of mechanisms that seek to balance the constitutionally-protected interests engaged by the CSE's mandate and powers. In contrast, CSIS is mandated to collect threat-related information and

[10] *Canada Evidence Act*, R.S.C., 1985, c. C-5.
[11] *Hunter et al. v Southam Inc.*, [1984] 2 S.C.R. 145.
[12] SECU proceedings on Bill C-26, Testimony of the Privacy Commissioner of Canada Phillipe Dufresne, February 15, 2024.
[13] See, e.g., *R. v. Jones*, 2017 SCC 60; *R. v. Spencer*, 2014 SCC 43; *R. v. Bykovets*, 2024 SCC 6.
[14] *National Security Act, 2017*, S.C. 2019, c. 13.
[15] Craig Forcese and Leah West, *National Security Law* (Canada: Irwin Law, 2020) at p 387.

intelligence from within Canada. However, CSIS is obligated to obtain federal court approval to obtain data that carries a reasonable expectation of privacy from telecommunications providers in Canada.[16]

22. Since the law passed in 2019, public debate and scrutiny continues to be warranted. Among many examples of its kind, a Federal Court ruling publicly released in early 2024 expressed serious concerns regarding revelations of inappropriate information sharing of Canadians' personal information in circumstances involving both the CSE and CSIS.[17] The Court was critical of CSIS' lack of candor with the court on repeated occasions, stating that the "failing goes to the heart of CSIS's relationship with the Court."[18] The Federal Court noted that this is not the first type of ruling of its kind in recent years.[19] The National Security Intelligence Review Agency (NSIRA) has also reported chronic problems in reviewing the lawfulness of the CSE's activities.[20]

23. Despite the precarity of the current equilibrium in Canadian national security law, Bill C-8 would only destabilize the existing circumstances further by creating a new information collection and sharing portal between telecommunication providers, the Minister of Industry, and Canada's national security bodies. The information sharing channel opened in Bill C-8 would appear to do indirectly what CSIS and the CSE are not authorized to do directly,[21] and fails to clearly establish a role for the Federal Court in authorizing any collection of information from telecommunication providers that is subject to a reasonable expectation of privacy.

24. The concern that the government agencies like the CSE will use and repurpose information it receives through Bill C-8 into its other intelligence activities is not speculative. As noted in the *Joint Civil Society Senate Submission on Bill C-26*,[22] testimony of the Director General of Strategy Policy at the CSE

[16] *Canadian Security Intelligence Service Act*, R.S.C., 1985, c. C-23, s. 21 (and related amendments following the recent passage of Bill C-70, *An Act respecting countering foreign interference*).
[17] *Canadian Security Intelligence Service Act (CA) (Re)*, 2023 FC 1341.
[18] *Ibid* at para. 7.
[19] Citing *Canadian Security Intelligence Services Act (CA) (Re)*, 2020 FC 616 at paras 83-85, 91-100 and 167 (another decision where CSIS failed to disclosure an issue concerning information that had been potentially illegally collected). The Court concluded: "The evidence indicates that the issue of potential illegality was widely known within the circle of those organizations and institutions that play a role in the oversight or management of CSIS operations….Despite this widespread knowledge and the potential relevance the issue of illegality had in the context of warrant applications, the matter was never brought to this Court's attention. This is inexcusable, particularly where there was a heightened awareness of the import of the duty of candour and ongoing engagement between the Court, the Service and the Department of Justice in the aftermath of the *Associated Data* decision and the Segal Report. It appears only the Court was left in the dark" (at para. 168).
[20] Christopher Parsons, "Don't give more powers to CSE until it submits to effective review", *Policy Options*, November 29, 2022, citing NSIRA's 2020 and 2021 annual reports which call attention to the CSE's continued resistance to providing NSIRA with information that NSIRA considers to be necessary for NSIRA to review the lawfulness of the CSE's activities. See also, National Security and Intelligence Review Agency, Annual Report 2022, tabled in Parliament on October 30, 2023.
[21] As noted, CSIS is obliged to obtain Federal Court authorization to obtain information that is subject to a reasonable expectation of privacy from telecommunication providers: *Canadian Security Intelligence Service Act*, R.S.C., 1985, c. C-23, s. 21 (and related amendments following the recent passage of Bill C-70). For its part, when acting in accordance with its cybersecurity and information assurance mandate, the CSE is not authorized to intentionally seek data concerning Canadians or persons in Canada, or to direct its information-acquisition activities towards Canadians or persons in Canada: *Communication Security Establishment Act*, S.C. 2019, c. 13, s. 76, s. 23 (see also *ibid* at s. 22 (1) and (2).
[22] *Joint Civil Society Senate Submission on Bill C-26*, at p. 17-18.

confirmed the agency's interest to use information collected through new powers under Bill C-8 for purposes beyond its cybersecurity and information assurance mandate.[23]

25. In its *Charter* statement on Bill C-8, the Department of Justice asserts that privacy interests are diminished in "regulatory and administrative contexts." However, the privacy interests of the individuals who use telecommunication and critical infrastructure services are not in any way diminished. Human communication is not a "regulatory" matter.

26. In *substance*, Bill C-8 is reforming Canada's national security laws and powers, and will impact the privacy interests of people across Canada—people who are not "regulated" companies.

27. To impose more appropriate guardrails, I recommend the following amendments, which build on the recommendations of Dr. Parsons from *Cybersecurity Will Not Thrive in Darkness*:

- **Recommendation 3: Prior Judicial Approval Must be Required for the Government to Obtain Personal or De-Identified Information from a Telecommunications Provider.** The legislation should be amended such that before the government can compel a telecommunications provider to disclose personal or de-identified information,[24] it must first obtain judicial authorization from the Federal Court. This amendment is critical to address constitutional deficits in the current draft of Bill C-8. As noted above, telecommunication providers host information that is among the highest level of privacy protection that our legal system affords. Judicial oversight is vital to the protection of this information under section 8 of the *Charter*.

- **Recommendation 4: Information Obtained from Telecommunications Providers Should Only be Used by Government Agencies for Cybersecurity and Information Assurance Activities.** Information should not be used for the purposes of signal intelligence and foreign intelligence activities, cross-department assistance unrelated to cyber-security, or active or defensive cyber operations.

- **Recommendation 5: The Collection And Sharing Of Personal Information Should Be Limited By Both Necessity And Proportionality Requirements.** Several witnesses testified about the importance of including both necessity and proportionality as guardrails under Bill C-26. In response, an official from the Department of Industry testified about areas where proportionality may already be present in existing law governing administrative decision-making or constitutional law.[25] However, those are distinct matters at law, which do

[23] SECU proceedings on Bill C-26, Testimony of Mr. Stephen Bolton (Director General, Strategic Policy, Communications Security Establishment), April 8, 2024.
[24] As noted in previous Citizen Lab research, "[e]ven when personal information has been de-identified or aggregated, it can be possible to re-identify individuals by way of drawing inferences or correlations from the data or by overlaying it with known personal information": Amanda Cutinha and Christopher Parsons. "Minding Your Business: A Critical Analysis of the Collection of De-identified Mobility Data and Its Use Under the Socially Beneficial and Legitimate Interest Exemptions in Canadian Privacy Law," Citizen Lab Research Report No. 161, University of Toronto, November 22, 2022.
[25] SECU proceedings on Bill C-26, Testimony of Andre Arbour, Director General, Strategy and Innovation Policy Sector, Department of Industry, March 18, 2024.

not foreclose the need for requiring proportionality as a limiter of a significant statutory power. Under the *Communications Security Establishment Act*, the minister cannot issue a cybersecurity authorization unless the minister "concludes that there are reasonable grounds to believe that any activity that would be authorized by it is **reasonable *and proportionate***, having regard to the nature of the objective to be achieved and the nature of the activities."[26]

Furthermore, the SECU committee did not table or vote on an amendment that would specifically apply necessity and proportionality standards for the collection and sharing of personal information.[27] The Privacy Commissioner of Canada has emphasized the importance of requiring both necessity and proportionality to ensure powers are minimally-intrusive on privacy interests.[28] Requiring necessity and proportionality in the context of information sharing would protect persons who depend on telecommunication services in Canada, and who would be indirectly impacted by Bill C-8's framework. To that end, I recommend the following textual amendments:

- Section 15.4: The information collection power under s. 15.4 should incorporate necessity and proportionality requirements.
- Section 15.6(1): "Despite section 15.5, to the extent that is necessary **and proportionate** for any purpose…"
- Section 15.5(4)(c): The same amendment ("necessary **and proportionate**") should be added to section 15.5(4)(c).

- **Recommendations 6: Data Retention Periods Should Be Attached to Telecommunications Providers' Data and to Foreign Disclosures of Information.** The legislation should be amended to highlight that confidential information may 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. Similarly, an amendment should also require that the government attach data retention and deletion clauses in agreements or memoranda of understanding that are entered into with foreign agencies. Retention periods should be communicated to the affected telecommunications providers.

- **Recommendation 7: Consent should only be obtained from the person to whom the information relates.** Section 15.5(4)(b) allows for the disclosure of confidential information with the consent of the person who designated the information as confidential. An amendment was made during the SECU Committee study of Bill C-26 to add personal and de-identified information to the scope of "confidential information." This is a positive change, and should be

[26] *Communication Security Establishment Act*, S.C. 2019, c. 13, s. 34(1).
[27] The SECU did consider a related amendment that would have included language under the new sections 15.1(1.1) and 15.2(2.1) to ensure that Orders in Council and Ministerial Orders are proportionate to the gravity of the threat of interference, manipulation, disruption or degradation: SECU proceedings on Bill C-26, March 18, 2024.
[28] SECU proceedings on Bill C-26, Testimony of the Privacy Commissioner of Canada Phillipe Dufresne, February 15, 2024.

further accompanied by clarification of the consent provision attached to confidential information. Particularly given the provision of alternative disclosure mechanisms under section 15.5(4)(a) and (c), it is a constitutional problem to allow telecommunication operators to "consent" on behalf of users to the sharing of highly sensitive information with other government agencies, including those under the purview of the Minister of Public Safety and Emergency Preparedness (e.g., Royal Canadian Mounted Police and Canadian Security Intelligence Service) and the Minister of National Defence (e.g., Canadian Armed Forces and Communications Security Establishment). As the Supreme Court has reiterated, consent to waive the constitutional right to privacy cannot be given by a third party,[29] including by telecommunication providers in respect of their user's private data.[30]

This amendment should be affected by either excluding personal or de-identified information from section 15.5(4)(b), or by amending the provision as follows:

> "...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**."

Part 3. Encryption-breaking powers in Bill C-8 that undermine the security of Canada's networks

28. This Part 3 recommends that an interpretive clause be added to s. 15.2 to confirm that its powers cannot be used to "**compromise the confidentiality, integrity, or availability of a telecommunications facility, telecommunications service, or transmission facility**." As Part 3 outlines, this amendment is intended to address a core cybersecurity danger that the broad powers under s. 15.2 of Bill C-8 might be used to issue orders that weaken the encryption standards in telecommunication networks.[31] Particularly given the federal government has stated that the intent of Bill C-8 is to better protect the security of Canada's networks, this amendment is critical to ensure that the broad powers under s. 15.2 are not implemented in a manner that has the opposite effect of *undermining* network security. This amendment is also recommended in the *Joint Civil Society Senate Submission on Bill C-26* (Recommendation #1).

29. In 2022, the federal government announced a move to block telecom equipment from Huawei and ZTE, citing the "cascading economic and security impacts"[32] that a supply chain breach would endanger. The government cited concerns that Huawei or ZTE might be "compelled to comply with extrajudicial

[29] *R. v. Cole*, [2012] 3 S.C.R. 34.
[30] *R. v. Spencer*, 2014 SCC 43.
[31] Analysis in this Part 3 is developed from: Kate Robertson and Ron Deibert, "Ottawa wants the power to create secret backdoors in our networks to allow for surveillance", *The Globe and Mail*, May 29, 2024.
[32] Innovation, Science and Economic Development Canada, "Policy Statement – Securing Canada's Telecommunications System", May 19, 2022.

directions from foreign governments."[33] And yet, currently Bill C-8 would provide Canadian officials with the same authority that the government has publicly condemned. If a non-amended Bill C-8 passes, all telecom providers in Canada would be compellable through secret orders to install backdoors inside Canada's networks by weakening encryption or network equipment. Specifically, the broad language in subsections 15.2(2)(c), (l), and (m) could be used to order Canadian telecommunications companies to install lawful-access related measures in components of Canada's telecommunication networks. In testimony before the SECU Committee, Eric Smith, Senior Vice-President of the Canadian Telecommunications Association likewise warned that the "very broad" powers under Bill C-26 could be used to weaken encryption.[34]

30. Despite several witnesses warning the government that Bill C-8 would actually facilitate new government powers to compel decryption in telecommunications standards, the government has pushed the bill forward without debate or amendment to fix the problem. The government's push to do so raises concerning questions, particularly given the government has publicly stated that the intent of the legislation is not to create a new "surveillance mandate."[35]

31. Creating powers to drill holes in telecom encryption standards would only entrench or worsen cybersecurity threats into Canada's networks. Today, many network insecurities persist reaching all the way down to the infrastructure layers of communication technology. The Signalling System No. 7 (SS7), developed in 1975 to route phone calls, has become a major source of insecurity for mobile phones.[36] In 2017, CBC reporting showed how hackers would have only needed a Canadian MP's cell phone number in order to intercept his movements, voicemails, text messages, and phone calls.[37] Little has since changed. A 2023 report from the Citizen Lab documents the pervasive vulnerabilities at the heart of the world's mobile networks.[38]

32. Compromising network encryption would be a boon for cybercrime actors. According to a 2020 technical report produced by the International Telecommunication Union (ITU)—acting through the Financial Inclusion Global Initiative (a partnership between the ITU, the World Bank, and the Committee on Payments and Market Instructure)—malicious actors routinely exploit telecom vulnerabilities to perpetrate financial fraud online:

> Telecom vulnerabilities enable criminals to perform various attacks that result in fraud to steal digital money; many of these attacks involve the attacker masquerading as the [digital financial services (DFS)] provider to fraud the end-user or the attacker

[33] *Ibid*.
[34] SECU proceedings on Bill C-26, Testimony of Eric Smith, Senior Vice-President, Canadian Telecommunications Association, March 18, 2024
[35] SECU proceedings on Bill C-26, Testimony of Member of Parliament Jennifer O'Connell, April 8, 2024.
[36] Bill Marczak, John Scott-Railton, Siddharth Prakash Rao, Siena Anstis, and Ron Deibert, "Running in Circles: Uncovering the Clients of Cyberespionage Firm Circles," Citizen Lab Research Report No.133, University of Toronto, December 2020.
[37] Brigitte Bureau, Catherine Cullen, & Kristen Everson, "Hackers only needed a phone number to track this MP's cellphone", *CBC News*, November 24, 2017.
[38] Gary Miller and Christopher Parsons. "Finding You: The Network Effect of Telecommunications Vulnerabilities for Location Disclosure," Citizen Lab Research Report No. 171, University of Toronto, Oct. 2023.

masquerading as the end-user to fraud the DFS provider. In all these cases, the attacker uses telecom vulnerabilities to pass authentication and perform actions on compromised accounts.[39]

33. Fraud actors can use a variety of attacks to circumvent two-factor authentication, gain unauthorized access to online bank accounts, or to harvest sensitive data that is then repurposed to generate more sophisticated phishing attacks.[40] The ITU notes that "[e]xploiting these vulnerabilities enables attackers to commit fraud and steal funds from unsuspecting victims, who in most cases are unaware their account is being compromised or hacked."[41] The report states that it is a "misconception" that these attacks are difficult to perpetrate: "today, every hacker with ~$500 … to spare can exploit cellular vulnerabilities."[42]

34. According to recent estimates, only a "quarter of mobile network operators worldwide have deployed a signaling firewall that is designed to impair geolocation surveillance."[43] In a survey conducted by the European Union Agency for Network and Information Security (ENISA), approximately 75% of EU-based operators stated in a survey "that cost is the inhibiting factor in implementation, … and the lack of regulation mandating it."[44] For this reason, the *Finding You* report recommends that legislators and regulators be attentive to whether mobile industry participants in their jurisdictions "are engaged in questionable business practices that endanger individuals' security, privacy, and consumer rights" or whether they are "prioritizing revenues over protecting their subscribers."[45]

35. In the aftermath of the revelations in 2025 of the Salt Typhoon cyberattack, which is now understood to have comprehensively penetrated U.S. telecommunication networks and other networks in countries around the world, United States Senator Ron Wyden sent a responding letter to the Federal Communications Commission and the United States Attorney General, writing that "recently reported hack of U.S. telecommunications companies' wiretapping systems should serve as a major wake-up call to the government."[46] Senator Wyden underscored the need for regulatory action to secure U.S. networks, and emphasized that the U.S. Department of Justice "must stop pushing for policies that

[39] Financial Inclusion Global Initiative, Security, Infrastructure and Trust Working Group, *Technical report on SS7 vulnerabilities and mitigation measures for digital financial services transactions* (International Telecommunications Union, 2020), at p 9.
[40] *Ibid* at p 11 and 14.
[41] *Ibid* at p 9.
[42] *Ibid* at p 13.
[43] *Finding You*, at p 2, citing Mobileum, Mobilesquared, *The State of the Signaling Firewall Landscape*, November 2021. A survey of EU-based network operators by the European Union Agency for Network and Information Security (ENISA) also found that only 28% of operators have implemented signalling firewalls: ENISA, *Signalling Security in Telecom: SS7/Diameter/5G EU level assessment of the current situation*, March 2018.
[44] Financial Inclusion Global Initiative, Security, Infrastructure and Trust Working Group, *Technical report on SS7 vulnerabilities and mitigation measures for digital financial services transactions* (International Telecommunications Union, 2020), at p 17, citing ENISA, *Signalling Security in Telecom: SS7/Diameter/5G EU level assessment of the current situation*, March 2018; Catherine Cullen & Brigitte Bureau, "Cellphone companies may need to step up privacy protections, minister says," *CBC News*, November 23, 2017.
[45] Gary Miller and Christopher Parsons. "Finding You: The Network Effect of Telecommunications Vulnerabilities for Location Disclosure," Citizen Lab Research Report No. 171, University of Toronto, Oct. 2023, at p. 32.
[46] Letter, United States Senator Ron Wyden, October 11, 2024.

harm Americans' privacy and security by championing surveillance backdoors in other communications technologies," given those backdoors "create an irresistible target for hackers and spies."[47] Senator Wyden highlighted the shared responsibility of both telecommunications companies, and the federal laws that mandated surveillance systems, for insecurity in telecommunication systems. Senator Wyden wrote:

> During the Congressional hearings for CALEA, cybersecurity experts warned that these backdoors would be prime targets for hackers and foreign intelligence services. However, these concerns were dismissed by then-FBI Director Louis J. Freeh, who testified to Congress that experts' fears of increased vulnerability were "unfounded and misplaced." Congress, relying on the FBI Director's assurances that the security risks experts warned about could be addressed, passed the law mandating backdoors.
>
> …While the government has released no public information about the most recent hack, if the press reports are accurate, it may have caused enormous harm to U.S. national security.[48]

36. These events in the United States should also serve as a wake-up call to course correct on Canada's own cybersecurity law as proposed in Bill C-8.

37. As a result, this Part 3 recommends:

- **Recommendation 8: Order-making powers should be amended to ensure that new Ministerial powers are not used to compromise the security of Canada's networks.** An interpretive clause should be added to s. 15.2, to confirm that, <u>for greater certainty, the Minister is not authorized to make an order that would compromise the confidentiality, integrity, or availability of a telecommunications facility, telecommunications service, or transmission facility</u>. The intent of this recommendation is "to prevent the government from ordering or demanding that telecommunications service providers deploy or enable lawful access-related capabilities or powers in the service of 'securing' infrastructure by way of adopting a standard."[49]

- **Recommendation 9: The Governor in Council and Minister of Industry should be required to consider the effect of orders on the privacy and security of communications.** According to new amendments made during SECU hearings, the Governor in Council and Minister of Industry are now required to consider a list of factors before issuing orders under s. 15.1 or under s. 15.2 (factors listed under s. 15.1(2.1) and 15.2(3.1)). I recommend that a clause be added alongside those factors to require consideration of the effect of the order on the privacy and security of communications:

  > **(a)** its operational impact on the affected telecommunications service providers;

[47] *Ibid*.
[48] *Ibid*.
[49] Christopher Parsons, "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, University of Toronto, Oct. 2022, at p. 17.

(b) its financial impact on the affected telecommunications service providers;
(c) its effect on the provision of telecommunications services in Canada;
(d) **its effect on the privacy and security of communications**; and
(e) any other factor that the [Governor in Council/Minister] considers relevant.

Part 4. Concluding Remarks

38. I urge this Committee to take seriously the recommendations that were identified in *Cybersecurity Will Not Thrive in Darkness*, including in particular the priority recommendations that are expanded upon in this brief. In detailing these recommendations for this Committee's study, I also urge the Committee to consider the additional *Charter* interests that are engaged by Bill C-8, including freedom of expression and privacy interests, as described in Part 2 of this Brief.

39. While Canada needs to move forward in combating threats to its telecommunications and critical infrastructure, it should not legislate out of fear, and at the expense of democratic norms and safeguards, public transparency and accountability, or respect for the *Charter* and human rights. Rather, a human security and human rights approach to cybersecurity requires the recognition of the importance of accessible and inclusive cybersecurity, public accountability, and public transparency when regulating telecommunications and cybersecurity.

Part 5. Organizational Information

40. I am a lawyer and senior research associate at the Citizen Lab, Munk School of Global Affairs & Public Policy at the University of Toronto. My research explores the intersection of law, policy, and technology, and focuses on transparency and accountability mechanisms relevant to the relationship between corporations and state agencies regarding personal data and other surveillance activities. I draw on former experience as a law clerk of the Supreme Court of Canada, and subsequently, as a lawyer in Canada's justice system.

41. The views presented in this brief are my own and based on research that I and colleagues have carried out at our place of employment, the Citizen Lab. The Citizen Lab is an interdisciplinary laboratory based at the Munk School of Global Affairs and Public Policy, University of Toronto, focusing on research, development, and high-level strategic policy and legal engagement at the intersection of information and communication technologies, human rights, and global security.

42. We use a "mixed methods" approach to research combining practices from political science, law, computer science, and area studies. Our research includes: investigating digital espionage against civil society, documenting Internet filtering and other technologies and practices that impact freedom of expression online, analyzing privacy, security, and information controls of popular applications, and examining transparency and accountability mechanisms relevant to the relationship between corporations and state agencies regarding personal data and other surveillance activities.

Appendix A - Table of Recommendations

Appendix B - Enclosed Report

Christopher Parsons. "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, University of Toronto, October 18, 2022.

Appendix C - Enclosed Report

Gary Miller and Christopher Parsons. "Finding You: The Network Effect of Telecommunications Vulnerabilities for Location Disclosure," Citizen Lab Research Report No. 171, University of Toronto, October, 2023.