Submission to the Standing Committee on National Security, Defence and Veterans Affairs 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
May 22, 2026

Part 1. Overview

1. A series of important amendments to Canada's proposed cybersecurity legislation were made in the House of Commons SECU study earlier this year. However, as important as the recent amendments have been, this committee is now left with the irony that the most significant constitutional vulnerability in the legislation has continued to be left wide open: the imbalance between the bill's privacy-impacted powers, and the contrasting absence of independent judicial oversight. As a result, this brief sets out targeted recommendations that would help establish a much stronger constitutional foundation for legislation that has the potential to guide the protection of Canada's networks for decades to come.

2. In January 2026, the House of Commons SECU committee voted to amend Bill C-8 to incorporate independent judicial authorization of orders issued by the Governor in Council or the Minister under the proposed sections 15.1 or 15.2 of the *Telecommunications Act*, and in respect of compelled secrecy orders. The amendments were nevertheless ruled out of scope after the study's conclusion.

3. The constitutional problem of the absence of independent judicial authorization had been a significant concern raised prior to Bill C-8 being tabled. However, the legislation was not referred to committee until after Second Reading in the House of Commons.

4. It is difficult to envisage how amending legislation to incorporate accompanying constitutional safeguards could be considered out of scope of the principle of proposed legislation. Given their importance, such matters should not be disposed of on procedural grounds. Nevertheless, in the Senate, Bill C-8 has again been referred to committee after the conclusion of Second Reading.

5. As a result, Bill C-8 remains highly vulnerable on constitutional grounds. Independent judicial oversight is the most important protection s. 8 of the *Charter* affords. Not only is the absence of independent oversight from this legislation a core risk for its ability to be implemented in the years ahead without constitutional court litigation, the bill will also destabilize Canada's existing national security framework. Canada's laws were overhauled in 2017. The constitutionality of Canada's new oversight system has not been constitutionally reviewed, and has since been further complicated by ongoing concerns raised by courts and review bodies regarding either issues of illegality in the activities of Canada's national security agencies, repeated issues concerning lack of candour by agencies or agency representatives, and/or chronic problems reviewing the lawfulness of agency activity.[1]

6. Despite the precarity of the current equilibrium, Bill C-8 would only destabilize the existing circumstances further by creating a new warrantless information collection and sharing pathway between telecommunication providers, the Minister of Industry, and Canada's national security bodies, while failing integrate either of the existing independent authorization systems under Canada's existing framework (the Federal Court of Canada and the Intelligence Commissioner of Canada).

[1] See paragraphs 14-19 below.

7. This brief recommends that this committee find that these constitutional risks are too significant to leave hanging over important, public interest legislation. Addressing the imbalance of the warrantless nature of this collection power should be this committee's priority. The Intelligence Commissioner's previous testimony highlighted that "[t]he glaring absentee in this bill is the Canadian public. The information that is collected is Canadians' personal information." For example, the Privacy Commissioner of Canada emphasized during testimony on Bill C-26 that the legislation could result in the inappropriate sharing of subscriber account information, communication data, website visits, metadata, location data and financial data.[2] The Intelligence Commissioner further 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.

8. Should judicial oversight fail to be added to Bill C-8, this brief also sets out additional recommendations in Parts 2 and 3 of this brief which are only more critical to mitigate some of the worst privacy harms and constitutional risks created by the absence of independent oversight. These amendments are not put forward as a cure. They are amendments, however, which could move the bill somewhat towards a stronger constitutional footing than the uneven balance struck at present. These amendments would also assist in providing the public greater confidence over the security over the privacy of their personal information, given the government's unwillingness to protect individual privacy rights through independent judicial oversight.

9. Given the above, this brief expands upon the above priority, and sets out a total of five recommendations to address the constitutional and cybersecurity risks that remain in Bill C-8:

   i. Recommendation 1: Independent judicial oversight is integral to the constitutionality of Bill C-8.

   ii. Recommendation 2: Clarifying subsection 15.2(4) to ensure that it also excludes the interception of metadata.

   iii. Recommendation 3: Section 15.2 should further be amended to clarify that it cannot be used to require telecommunication providers to adopt intercept capabilities.

   iv. Recommendation 4: Where personal or de-identified information is obtained from telecommunications providers, it should only be used by government agencies for cybersecurity and information assurance activities.

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

v. Recommendation 5: Section 15.2(2.1) should be clarified to confirm protection for encryption and technical safeguards in telecommunication networks generally, not just the specific encryption that is attached to private communications.

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

10. 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.

11. 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.[3]

12. 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,[4] 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.[5]

13. 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.

14. In 2017, Canada's national security laws underwent a massive overhaul in the *National Security Act, 2017*.[6] 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."[7] 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

[3] *Hunter et al. v Southam Inc.*, [1984] 2 S.C.R. 145.
[4] SECU proceedings on Bill C-26, Testimony of the Privacy Commissioner of Canada Phillipe Dufresne, February 15, 2024.
[5] See, e.g., *R. v. Jones*, 2017 SCC 60; *R. v. Spencer*, 2014 SCC 43; *R. v. Bykovets*, 2024 SCC 6.
[6] *National Security Act, 2017*, S.C. 2019, c. 13.
[7] 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.[8]

15. 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.[9] 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."[10] The Federal Court noted that this is not the first type of ruling of its kind in recent years.[11] Just last fall, further reporting revealed that CSIS had again failed to disclose an intrusive new technology to NSIRA and to the Federal Court.[12]

16. The National Security Intelligence Review Agency (NSIRA) has also reported chronic problems in reviewing the lawfulness of the CSE's activities.[13] In its most recent annual report, it described the problems are persisting:

> …overbroad, unsubstantiated or excessive demands for redactions in access to information consultations are occurring in every file, inconsistent disclosures in response to requests for information are routine, institutional resistance to NSIRA's access rights occurs, and outdated departmental information systems at times impede NSIRA's ability to conduct its work. NSIRA raises these issues with senior departmental officials and escalates to the Minister when necessary, with mixed results. While responsiveness performance varies across departments, it is fair to say that the status quo is one where process challenges regularly challenge NSIRA's ability to deliver on its mandate. NSIRA is looking at ways to provide better real-time public awareness of its responsiveness challenges so that relevant departments can be held accountable.[14]

---

[8] *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*).
[9] *Canadian Security Intelligence Service Act (CA) (Re)*, 2023 FC 1341.
[10] *Ibid* at para. 7.
[11] 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).
[12] Christopher Nardi, "CSIS failed to disclose use of new 'intrusive' technology to minister and court: watchdog", *National Post*, October 14, 2025.
[13] 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.
[14] National Security and Intelligence Review Agency, Annual Report 2024, tabled in Parliament on December 4, 2025.

17. 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,[15] 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.

18. 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*,[16] testimony of the Director General of Strategy Policy at the CSE 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.[17]

19. 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.

20. 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.

21. To impose more appropriate guardrails, I recommend the following four amendments. These amendments build on the recommendations of Dr. Christopher Parsons from *Cybersecurity Will Not Thrive in Darkness*,[18] and further integrate recommendations made by the Canadian Civil Liberties Association in its brief submitted during SECU's study of Bill C-8.[19] The proposed amendments are as follows.

    i. **Recommendation 1: Prior Judicial Approval Must be Required for the Government to Obtain Personal or De-Identified Information from a Telecommunications Provider.** The

[15] 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).

[16] *Joint Civil Society Senate Submission on Bill C-26*, at p. 17-18.

[17] SECU proceedings on Bill C-26, Testimony of Mr. Stephen Bolton (Director General, Strategic Policy, Communications Security Establishment), April 8, 2024.

[18] 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. 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.

[19] Canadian Civil Liberties Association, Submission to the House of Commons Standing Committee on Public Safety and National Security, Study: Bill C-8, An Act Respecting Cyber Security, Amending Telecommunications Act, and Making Consequential Amendments to Other Acts, December 15, 2025.

legislation should be amended such that before the government can compel a telecommunications provider to disclose personal or de-identified information, it must first obtain judicial authorization from the Federal Court.

ii. **Recommendation 2: Clarify subsection 15.2(4) to ensure that it also excludes the interception of metadata.** As noted by the CCLA, the clause currently does not impose any restrictions on the interception of metadata despite its heightened sensitivity. As a result, under the existing provision, telecommunication providers "can be compelled to intercept and retain significant amounts of their customer's Internet activities for cybersecurity purposes, …which can be as revealing of our online activities and personal lives than the private communications being exempted from interception."[20] This data is protected under the *Charter*. As a result, the following clarification is necessary:

> 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 sections 183**, 492.1 and 492.2** of the Criminal Code.

iii. **Recommendation 3: Section 15.2 should be amended to clarify that it cannot be used to adopt intercept capabilities.** The government has publicly stated that the intent of the legislation is not to create a new "surveillance mandate."[21]

Proposed legislation (Bill C-22, the *Lawful Access Act*) is already before Parliament which incorporates proposed powers to compel telecommunication service providers to install intercept capabilities. That legislation is being studied and examined, and Parliamentarians will undoubtedly be carefully considering what limits and safeguards must correspond with government powers of that magnitude. The power to impose technical intercept capabilities could result in the position of backdoors and other intrusive surveillance systems. Those limits and safeguards are not present in Bill C-8. As a result, this committee should ensure that Bill C-8 does not indirectly become a mechanism for imposing new intercept capabilities in telecommunication networks. This recommendation is all the more important, given the government's unwillingness to incorporate independent judicial oversight in the legislation.

As a result, I agree with the Canadian Civil Liberties Association that the following amendment is critical. As the CCLA writes:

> 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

[20] Canadian Civil Liberties Association, Submission to the House of Commons Standing Committee on Public Safety and National Security, Study: Bill C-8, An Act Respecting Cyber Security, Amending Telecommunications Act, and Making Consequential Amendments to Other Acts, December 15, 2025, at p. 3.
[21] SECU proceedings on Bill C-26, Testimony of Member of Parliament Jennifer O'Connell, April 8, 2024.

> 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.[22]

To guard against the risk that Bill C-8's considerable powers will be interpreted in an overbroad manner, the following amendment is required:

> **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.**

iv. **Recommendation 4: Personal and De-Identified 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.

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

22. In SECU's study of Bill C-8, all parties and members of the committee agreed that an amendment to the legislation was required in order to protect encryption technology. The Minister of Industry Mélanie Joly testified:

> We have heard the comments related to the issue of encryption. We are prepared to examine amendments on these issues so that there are no problems with regard to **the protection of the telecommunications system and its infrastructure, the path to encryption and the protection of privacy.**[23]

23. Afterwards, several versions of a corresponding amendment were considered by the committee. The government tabled s. 15.2(2.1), to stipulate that the "Minister must not order the decoding of an encrypted private communication". The government's proposed amendment passed with the support of the member from the Bloc Québécois, who stated that this version of the amendment was more clear than the alternative because it expressly referenced encryption technology, and because it would implement Minister Joly's commitment.[24]

---

[22] Canadian Civil Liberties Association, Submission to the House of Commons Standing Committee on Public Safety and National Security, Study: Bill C-8, An Act Respecting Cyber Security, Amending Telecommunications Act, and Making Consequential Amendments to Other Acts, December 15, 2025, at p. 9.
[23] SECU proceedings on Bill C-8, Testimony, January 27, 2026.
[24] SECU proceedings on Bill C-8, Member of Parliament Claude DeBellefeuille, February 5, 2026.

24. It is a laudable goal to explicitly reference encryption technology in this interpretive provision. Unfortunately, however, the specific wording that was ultimately adopted in s. 15.2(2.1) has had an adverse effect of incidentally **excluding** encryption technology in Canada's telecommunication networks that does not specifically attach to private communications.

25. When telecommunication networks are not properly secured with strong encryption and other technical safeguards, far more data is exposed than only the content of communications. For example, in 2017, CBC reporting showed how hackers would have only needed a Canadian MP's cell phone number in order to intercept his location data and movements, as well as voicemails, text messages, and phone calls.[25] In a joint statement in 2024 by the Canadian Cyber Security Centre, alongside cyber authorities amongst Five Eye countries, the authorities urged telecommunications providers to "Ensure that **traffic** is end-to-end encrypted to the maximum extent possible."[26] Other critical safeguards apply to **authentication** in telecommunication networks.[27]

26. As a result, this Part 3 recommends a critical clarification to ensure that new Ministerial powers are not used to compromise the security of Canada's networks:

    i. **Recommendation 5: Section 15.2(2.1) should be clarified to confirm protection for encryption and technical safeguards in telecommunication networks generally, not just the specific encryption that is attached to private communications.** 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."[28] The language set out below incorporate the recommendation of the Canadian Civil Liberties Association[29]:

> Private communication **and Technical Safeguards**
>
> 15 (2.1) Despite subsection (2), the Minister must not order the decoding of an encrypted private communication, as defined in section 183 of the *Criminal Code*, **or to make an order that would have the effect of degrading, removing, defeating or bypassing any other technical safeguard including encryption.**

[25] Brigitte Bureau, Catherine Cullen, & Kristen Everson, "Hackers only needed a phone number to track this MP's cellphone", *CBC News*, November 24, 2017.
[26] U.S. Cybersecurity and Infrastructure Security Agency, Canadian Cyber Security Centre, et al., "Enhanced Visibility and Hardening Guidance for Communications Infrastructure", December 3, 2024.
[27] U.S. Cybersecurity and Infrastructure Security Agency, Canadian Cyber Security Centre, et al., "Enhanced Visibility and Hardening Guidance for Communications Infrastructure", December 3, 2024, at p. 4-5.
[28] 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.
[29] Canadian Civil Liberties Association, Submission to the House of Commons Standing Committee on Public Safety and National Security, Study: Bill C-8, An Act Respecting Cyber Security, Amending Telecommunications Act, and Making Consequential Amendments to Other Acts, December 15, 2025, at p. 8.

27. Particularly given the federal government has stated that the intent of Bill C-8 is to better protect the security of Canada's networks, and that Minister Joly testified that the federal government was willing to implement an amendment to protect the ***path to encryption and telecommunication systems generally***, 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 by the *Canadian Civil Liberties Association* (Recommendation #1).

28. The remainder of this Part 3 outlines the importance of addressing the 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.[30]

29. In 2022, the federal government announced a move to block telecom equipment from Huawei and ZTE, citing the "cascading economic and security impacts"[31] that a supply chain breach would endanger. The government cited concerns that Huawei or ZTE might be "compelled to comply with extrajudicial directions from foreign governments."[32] 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 network encryption or 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.[33]

30. 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.[34] Little has changed since the CBC's 2017 reporting showing the vulnerability of a Canadian MP's mobile phone.[35] A 2023 report from the Citizen Lab documents the pervasive vulnerabilities at the heart of the world's mobile networks.[36]

---

[30] 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.
[31] Innovation, Science and Economic Development Canada, "Policy Statement – Securing Canada's Telecommunications System", May 19, 2022.
[32] *Ibid*.
[33] SECU proceedings on Bill C-26, Testimony of Eric Smith, Senior Vice-President, Canadian Telecommunications Association, March 18, 2024
[34] 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.
[35] Brigitte Bureau, Catherine Cullen, & Kristen Everson, "Hackers only needed a phone number to track this MP's cellphone", *CBC News*, November 24, 2017.
[36] 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.

31. 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 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.[37]

32. 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.[38] 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."[39] 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."[40]

33. According to recent estimates, only a "quarter of mobile network operators worldwide have deployed a signaling firewall that is designed to impair geolocation surveillance."[41] 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."[42] For this reason, Citizen Lab's report, *Finding You: The Network Effect of Telecommunications Vulnerabilities for Location Disclosure,* recommends that regulators be attentive to whether mobile industry participants in their jurisdictions "are engaged in questionable business

---

[37] 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.
[38] *Ibid* at p 11 and 14.
[39] *Ibid* at p 9.
[40] *Ibid* at p 13.
[41] *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.
[42] 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.

practices that endanger individuals' security, privacy, and consumer rights" or whether they are "prioritizing revenues over protecting their subscribers."[43]

34. 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."[44] 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 harm Americans' privacy and security by championing surveillance backdoors in other communications technologies," given those backdoors "create an irresistible target for hackers and spies."[45] 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.[46]

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

Part 4. Concluding Remarks

36. 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.

[43] 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.
[44] Letter, United States Senator Ron Wyden, October 11, 2024.
[45] *Ibid*.
[46] *Ibid*.

37. 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

38. 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.

39. 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.

40. 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