Cybersecurity Will Not Thrive in Darkness

A Critical Analysis of Proposed Amendments in Bill C-26 to the *Telecommunications Act*

By Christopher Parsons

OCTOBER 18, 2022
RESEARCH REPORT #158

munk school
OF GLOBAL AFFAIRS & PUBLIC POLICY

UNIVERSITY OF TORONTO

THECITIZENLAB

Copyright

Electronic version first published by the Citizen Lab in 2022. This work can be accessed through https://citizenlab.ca/2022/10/a-critical-analysis-of-proposed-amendments-in-bill-c-26-to-the-telecommunications-act.

Document Version: 1.0

About the Citizen Lab, Munk School of Global Affairs & Public Policy, University of Toronto

The Citizen Lab is an interdisciplinary laboratory based at the Munk School of Global Affairs & 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.

We use a "mixed methods" approach to research that combines methods 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.

About the Author

Christopher Parsons is currently a Senior Research Associate at the Citizen Lab, in the Munk School of Global Affairs & Public Policy with the University of Toronto. He received his Bachelor's and Master's degrees from the University of Guelph and his PhD from the University of Victoria.

Acknowledgements

I would like to extend my gratitude to the people that have shared their thoughts, expertise, and time with me throughout the process of writing this report. The experts inside and outside of government who have shared their thinking about how Bill C-26 would function in practice as well as its impetus have been invaluable to better understanding the legislation.

I want to specifically thank the individuals who reviewed drafts of this report but who cannot be identified for professional reasons. All remaining errors are my own.

Additionally, I would like to thank Mari Zhou for her assistance in designing and formatting the report. Copyedits were performed by Joyce Parsons of Stone Pillars Editing and Consulting.

This report was undertaken under the supervision of Prof. Ronald Deibert.

Corrections and Questions

Please send all questions and corrections to: chris@citizenlab.ca

Suggested Citation

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.

Contents

Contents

Table of Acronyms

3GPP	3rd Generation Partnership Project
CALEA	Communications Assistance for Law Enforcement Act
CCCS	Canadian Centre for Cyber Security
CIRA	Canadian Internet Registration Authority
CRTC	Canadian Radio-television and Telecommunications Commission
CSE	Communications Security Establishment
CSTAC	Canadian Security Telecommunications Advisory Committee
ETSI	European Telecommunications Standards Institute
eSRP	Evolved Security Review Program
GSMA	Global System for Mobile Communications
HBS	Host Based Sensor
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IT	Information Technology
NCSC	National Cyber Security Centre
NSICOP	National Security and Intelligence Committee of Parliamentarians
SGES	Solicitor General's Enforcement Standards
TSP	Telecommunications Service Provider

Table of Recommendations

Executive Summary

On June 14, 2022, the Government of Canada introduced "Bill C-26: An Act respecting cyber security, amending the *Telecommunications Act* and making consequential amendments to other Acts." If passed into law, it will significantly reform the *Telecommunications Act* as well as impose new requirements on federally regulated critical infrastructure providers. This report, "Cybersecurity Will Not Thrive in Darkness: A Critical Analysis of Proposed Amendments in Bill C-26 to the *Telecommunications Act*," offers 30 recommendations to the draft legislation in an effort to correct its secrecy and accountability deficiencies, while suggesting amendments that would impose some restrictions on the range of powers that the government would be able to wield. These amendments must be seriously taken up because of the sweeping nature of the legislation.

As drafted at time of writing, Bill C-26 would empower the Minister of Industry to compel telecommunications providers to do or refrain from doing anything in the service of securing Canadian telecommunications networks against the threats of interference, manipulation, or disruption. The legislation would authorize the Minister to compel providers to disclose confidential information and then enable the Minister to circulate it widely within the federal government; this information could potentially include either identifiable or de-identified personal information. Moreover, the Minister could share non-confidential information internationally even when doing so could result in regulatory processes or private right of actions against an individual or organization. Should the Minister or other party to whom the Minister shares information unintentionally lose control of the information, there would be no liability attached to the government for the accident.

Where orders or regulations are issued, they would not need to be published in the *Canadian Gazette* and gags could be attached to the recipients of such orders. There may even be situations where the government could issue an order or regulation, with the aforementioned publication ban and gag, that runs counter to a decision by the Canadian Radio-television and Telecommunications Commission (CRTC) and that overrides aspects of that decision. And in any cases where a telecommunications provider seeks judicial review, it might never see the evidence used to justify an order or regulation. However, if a telecommunications provider is found to have deliberately ignored or failed to adhere to an order, then either the individuals who directed the action or the telecommunications provider could suffer administrative monetary penalties.

This report, in summary, identifies and analyzes a series of deficiencies in Bill C-26 as it is presently drafted:

- The breadth of what the government might order a telecommunications provider to do is not sufficiently bounded.
- The excessive secrecy and confidentiality provisions imposed on telecommunications providers threaten to establish a class of secret law and regulations.
- Significant potential exists for excessive information sharing within the federal government as well as with international partners.
- Costs associated with compliance with reforms may endanger the viability of smaller providers.
- Vague drafting language means that the full contours of the legislation cannot be assessed.
- No recognition of privacy or other *Charter*-protected rights exists as a counterbalance to proposed security requirements nor are appropriate accountability or transparency requirements imposed on the government.

Even if it is presumed that the government does need the ability to encourage or compel telecommunications providers to modify their technical or business operations to enhance the security of their services and facilities, it is readily apparent that more transparency and accountability should be required of the government. All of the recommendations in this report are meant to address some of the existent problems in the legislation.

Should these recommendations or ones derived from them not be taken up, then the government will be creating legislation of the worst kind insofar as it will require the public—and telecommunications providers—to simply trust that the government knows what it is doing, is reaching the right decisions, and that no need exists for a broader public discussion concerning the kinds of protections that should be put in place to protect the cybersecurity of Canada's telecommunications networks. Cybersecurity cannot thrive on secretive and shadowy government edicts. The government must amend its legislation to ensure its activities comport with Canada's democratic values and the norms of transparency and accountability.

Introduction

The past two years have demonstrated that critical infrastructure providers are constantly under threat and that threat actors are willing, and interested, in targeting infrastructure in North America.[1] At the same time, Western governments have broadly raised concerns that China-based vendors could be compelled by the Chinese government to modify their products, with the effect of compromising the integrity of critical infrastructure in Western countries.[2] In short, threats to critical infrastructure are real and pressing, and Western governments have generally sought to identify how they can buttress infrastructure against both perceived and real weaknesses.

On May 19, 2022, the Minister of Public Safety and the Minister of Innovation, Science, and Economic Development held a press conference where they announced that Canadian telecommunications providers would be required to remove Huawei and ZTE equipment from their infrastructures.[3] The government also introduced a policy statement that made clear what it specifically planned to require of telecommunications providers.[4] Legislation capable of giving force to the policy statement was tabled on June 14, 2022. The legislation, "Bill C-26: An Act respecting cyber security, amending the *Telecommunications Act* and making consequential amendments to other Acts," would significantly reform the *Telecommunications Act* as well as impose new requirements on other critical infrastructure providers.[5]

Broadly, the proposed reforms would provide the government with new authorities to compel telecommunications providers and critical infrastructure providers to modify

---

1 See: Canadian Centre for Cyber Security. (2020). "National cyber threat assessment 2020," Government of Canada. Available at: https://cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2020; Canadian Centre for Cyber Security. (2022). "Cyber threat bulletin: Cyber threat activity related to the Russian invasion of Ukraine," Government of Canada. Available at: https://cyber.gc.ca/en/guidance/cyber-threat-bulletin-cyber-threat-activity-related-russian-invasion-ukraine; Cybersecurity & Infrastructure Security Agency. "Shield's Up," Government of the United States of America. Available at: https://www.cisa.gov/shields-up; and White House. (2021). "Executive Order 14028: Improving the Nation's Cybersecurity," The White House. Available at: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

2 See: 'Security Stances Adopted by Canada's Allies' as part of "The Policy and Political Implications of 'Securing Canada's Telecommunications Systems'," available at: https://christopher-parsons.com/2022/06/08/the-policy-and-political-implications-of-securing-canadas-telecommunications-systems/.

3 CPAC. (2022). "Ottawa announces move to ban Huawei and ZTE equipment from Canada's 5G networks," *YouTube*. Available at: https://www.youtube.com/watch?v=6odAKonqzIc.

4 Innovation, Science and Economic Development Canada (ISED). (2022). "Policy Statement – Securing Canada's Telecommunications System," Government of Canada. Available at: https://www.canada.ca/en/innovation-science-economic-development/news/2022/05/policy-statement--securing-canadas-telecommunications-system.html.

5 Parliament of Canada. (2022). "Bill C-26: An Act respecting cyber security, amending the *Telecommunications Act* and making consequential amendments to other Acts," Parliament of Canada. Available at: https://www.parl.ca/DocumentViewer/en/44-1/bill/C-26/first-reading.

their technical and organizational practices so as to enhance the security of these organizations' operations in accordance with government demands. The legislation follows in the footsteps of Canadian allies that have recognized the threats posed to critical infrastructure providers and have sought to ameliorate dangers by enabling government agencies to compel changes to providers' practices through legislation as well as executive orders.[6]

This report critically assesses the proposed reforms to Canada's *Telecommunications Act*. In doing so, it identifies the following series of deficiencies in the legislation as it is presently drafted:

- The breadth of what the government might order a telecommunications provider to do is not sufficiently bounded.
- The excessive secrecy and confidentiality provisions imposed on telecommunications providers threaten to establish a class of secret law and regulations.
- Significant potential exists for excessive information sharing within the federal government as well as with international partners.
- Costs associated with compliance with reforms may endanger the viability of smaller providers.
- Vague drafting language means that the full contours of the legislation cannot be assessed.
- No recognition of privacy or other *Charter*-protected rights exists as a counterbalance to proposed security requirements nor are appropriate accountability or transparency requirements imposed on the government.

In many cases, these deficiencies can be addressed through legislative amendments, and this report offers suggestions on how to do so throughout its analysis of the draft legislation. However, left unstated in either the "Securing Canada's Telecommunications System" policy statement or in comments accompanying Bill C-26 is the empirical need to secure Canada's telecommunications systems using the proposed legislative mechanisms. Unlike peer or allied countries, the Canadian government has not publicly marshalled evidence that indicates that Canada's critical telecommunications networks are insecure, nor has it issued a general strategic document that delineates how Bill C-26 fits within a broader effort to secure Canadian critical infrastructure. As the report

6 As examples, see: White House. (2021). "Executive Order 14028: Improving the Nation's Cybersecurity," The White House. Available at: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/; or Department of Home Affairs. (2022). "Security Legislation Amendment (Critical Infrastructure Protection) Act 2022," Government of Australia. Available at: https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/slacip-bill-2022.

ultimately concludes, in addition to specific legislative amendments, the Government of Canada should clearly and publicly explain the risks it is concerned about and the extent to which the introduced legislation looks backward to address existent or historical issues versus the extent to which is it forward-looking and meant to either address future challenges or enable activities with closely allied nations.

1. Background

Canadian government agencies have worried about the security properties of Canada's telecommunications networks for decades. Documents that have been released under access to information requests showcase that even in 2012, as an example, the Communications Security Establishment (CSE) was preparing presentations on supply chain threats to Canadian telecommunications networks. The CSE recognized that:

> [t]here is no way to prevent the introduction of foreign technology in Canada. We must find the appropriate balance between IT security requirements, the threat-risk environment, and the need to efficiently process information and provide services to Canadians while allowing industry to remain competitive.[7]

To try and strike the right balance, the Canadian government barred Huawei from bidding on the government's telecommunications and email network in 2012.[8] Moreover, foreign equipment, such as that sold by Huawei, has been assessed by EWA-Canada under the Common Criteria program. The government has also historically assessed Huawei equipment through the Communications Security Establishment's Security Review Program[9] and announced the contours of an evolved program in June 2022.[10]

The government has not cast threats to Canada's telecommunications infrastructure as solely originating from potentially maliciously configured Huawei or ZTE telecommunications equipment. In its 2020 threat assessment, the Cyber Centre recognized that critical infrastructure providers were of interest to threat actors and that, as a result,

---

7 Communications Security Establishment Canada. (2012). "Supply Chain Threats to Canada," available at: https://christopherparsonscom.files.wordpress.com/2022/07/a-2012-00397.pdf, p. 6.

8 Steven Chase. (2012). "Ottawa set to ban Chinese firm from telecommunications bid," *The Globe & Mail*. Available at: https://www.theglobeandmail.com/news/politics/ottawa-set-to-ban-chinese-firm-from-telecommunications-bid/article4600199/.

9 Canadian Centre for Cyber Security. (2019). "CSE's security review program for 3G/4G/LTE in Canadian telecommunications networks," Government of Canada. Available at: https://cyber.gc.ca/en/news-events/cses-security-review-program-3g4glte-canadian-telecommunications-networks.

10 The Government of Canada announced an 'evolved' Security Review Program (eSRP) in June 2022, with details available at: Canada Centre for Cyber Security. (2022). "CSE's evolved Security Review Program," Government of Canada. Available at: https://cyber.gc.ca/en/news-events/cses-evolved-security-review-program.

The evolved program "will engage all key suppliers present in the Canadian market to establish new partnerships focused on building confidence in the products and services deployed in Canadian telecommunications infrastructure" as well as continue "annual architecture reviews to identify security gaps and work collaboratively with TSPs to improve the overall security in the telecommunications sector." The eSRP will also "expand assessments to consider the deployment of products from key suppliers, with a focus on the most important and sensitive areas of the telecommunications infrastructure. The deployment assessment identifies risks and provides recommended mitigations to ensure a resilient network/service"; it also focuses on cyber resilience, issue telecommunications security recommendations, and it commits to "continue to work with international partners to promote global standards that raise the common baseline for cyber security and increase confidence in global telecommunications systems."

the Centre expected to conduct outreach with these providers.[11] In the CSE's 2021-2022 annual report, it reported that the Cyber Centre had received some information from critical infrastructure providers, such as the energy and gas sectors, in order to better understand the threat landscape.[12]

Broadly, the CSE, in tandem with Shared Services Canada and Treasury Board Secretariat, is responsible for key aspects of defending federal government systems. Under the CSE's authorizing legislation, it may also provide advice, guidance, or services to help protect electronic information and information infrastructures that are designated as "being of importance" by the Government of Canada.[13] As discussed in a 2022 report that was published by the National Security and Intelligence Committee of Parliamentarians (NSICOP), a non-telecommunications organization was the first to receive assistance from CSE under the *CSE Act* to stop a cyber operation that targeted the organization. As noted by CSE officials, in the NSICOP report:

> this type of deployment was not what was envisioned when the statute was drafted; rather, the authority was meant to enable longer-term, more proactive collaboration with non-federal organizations, **particularly telecommunications companies**.[14]

The same report describes how the CSE's defensive sensor systems, comprising host, network, and cloud sensors, can be used to mitigate threats to organizations that have adopted them.[15] Historical documents included amongst the Snowden revelations suggested that the CSE intended for their sensors to be located on at least some domestic telecommunications networks.[16]

---

11 Canadian Centre for Cyber Security. (2020). "National cyber threat assessment 2020," Government of Canada. Available at: https://cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2020.

12 Communications Security Establishment. (2022). "Communications Security Establishment Annual Report 2021-2022," Government of Canada. Available at: https://www.cse-cst.gc.ca/en/accountability/transparency/reports/communications-security-establishment-annual-report-2021-2022.

13 *CSE Act*, s. 17(a)(ii).

14 National Security and Intelligence Committee of Parliamentarians. (2022). "Special Report on the Government of Canada's Framework and Activities to Defend its Systems and Networks from Cyber Attack," Government of Canada. Available at: https://www.nsicop-cpsnr.ca/reports/rp-2022-02-14/2022-cyber-attack-framework-report-en.pdf, p. 81, emphasis not in original.

15 For a discussion of these sensors, see either the NSICOP's 2022 "Special Report on the Government of Canada's Framework and Activities to Defend its Systems and Networks from Cyber Attack," Government of Canada. Available at: https://www.nsicop-cpsnr.ca/reports/rp-2022-02-14/2022-cyber-attack-framework-report-en.pdf or the analysis of that same report, entitled "Unpacking NSICOP's Special Report on the Government of Canada's Framework and Activities to Defend its Systems and Networks from Cyber Attack," available at: https://christopher-parsons.com/2022/03/30/unpacking-nsicops-special-report-on-the-government-of-canadas-framework-and-activities-to-defend-its-systems-and-networks-from-cyber-attack/.

16 Christopher Parsons. "CASCADE: Joint Cyber Sensor Architecture," *Technology, Thoughts, and Trinkets*. Available at: https://christopher-parsons.com/resources/cse-summaries/#cse-cascade-joint.

Of note, some of Canada's allies, including the United Kingdom's National Cyber Security Centre (NCSC), are using some of the CSE's sensors. See: Richard E. Head. (2020). "Introducing Host Based Capability (HBC)," Government of the United Kingdom. Available at: https://www.ncsc.gov.uk/blog-post/introducing-host-based-capability-hbc. As Head states:

Other government agencies, apart from the CSE, have also recognized risks and threats that are posed to, or that transit, the Canadian telecommunications infrastructure. The CRTC, as an example, issued "Compliance and Enforcement and Telecom Decision 2022-170." This decision details the risks that online bots pose.[17] The Commission found that "regulatory action is necessary to ensure that Canadian carriers that block botnets do so in a way that provides a baseline level of protection to Canadians." Action is needed because, per the CRTC, "botnet traffic constitutes a significant issue for cyber security, both in terms of volume and severity of harm." In forthcoming months, a report should be issued by the CRTC that identifies the party (or parties), including potentially the Canadian Centre for Cyber Security (CCCS) or the Canadian Internet Registration Authority (CIRA), that could serve as the central authority of a blocking framework. The threats posed by automated bots were also raised by the Standing Committee on Public Safety and National Security's 2022 report, "The Rise of Ideologically Motivated Violent Extremism in Canada." Specifically, that report calls for the government to "invest in the development of Canada's cyber infrastructure, specifically to better identify and remove automated bots used to amplify extremist content accessible to Canadians online" (Recommendation 33).[18] Taken together, the CSE might be assigned a role to assist, or provide guidance to, telecommunications service providers so as to ameliorate the threats posed by automated bots.

Finally, law enforcement agencies may rely on electronic interception authorities to combat criminals who either target or use Canadian telecommunications. This activity may entail serving a warrant on telecommunications providers to identify, and see law enforcement agencies subsequently charge, individuals engaged in criminal offences. These offences may be associated with compromising critical telecommunications services and systems or undertaking actions that rely on telecommunications services or

---

> "Fortunately, our friends at the Canadian Centre for Cyber Security have allowed us to utilise the world class Host Based Sensor (HBS) technology that they developed to defend the Government of Canada. This has enabled us to get up and running much more quickly.
>
> The NCSC now actively collaborates with our Canadian counterpart in a range of areas, including co-development of the underlying [Host Based Capability] technology itself, but also on analytics and the best use of the data to defend our respective governments from cyber attack.
>
> …
>
> We'd like to take this opportunity to thank the Canadian Centre for Cyber Security for all their help and support in enabling us to get to this point. The NCSC would not have been able to take on this challenge alone."

17 Canadian Radio-television and Telecommunications Commission. (2022). "Compliance and Enforcement and Telecom Decision CRTC 2022-170," Government of Canada. Available at: https://crtc.gc.ca/eng/archive/2022/2022-170.htm.

18 Standing Committee on Public Safety and National Security. (2022). "The Rise of Ideologically Motivated Violent Extremism In Canada," Parliament of Canada. Available at: https://www.ourcommons.ca/DocumentViewer/en/44-1/SECU/report-6/.

systems to carry out other cyber-enabled criminal activities. The Royal Canadian Mounted Police (RCMP), as an example, collects electronic telecommunications data to target, implant, and maintain malware (referred to as 'On-Device Investigative Tools') on criminal suspects' devices.[19] However, while the Solicitor General's Enforcement Standards (SGES) require telecommunications providers offering mobile wireless services to possess lawful interception capability, which is used in association with RCMP malware, the same is not true of wireline telecommunications providers.[20] The result is that at least some providers may not possess the wireline interception capabilities that law enforcement and security services require to carry out their criminal or national security investigations, including those pertaining to threats to critical infrastructure.

19 Standing Committee on Access to Information, Privacy and Ethics. (2022). "Device Investigation Tools Used by The Royal Canadian Mounted Police (RCMP)," Parliament of Canada. Available at: https://www.ourcommons.ca/Committees/en/ETHI/StudyActivity?studyActivityId=11794265. For documents detailing the technical operation of On-Device Investigative Tools (ODITs), or the associated warrants or policies, see 'RCMP On-Device Investigative Tools' at: https://christopher-parsons.com/resources/miscellaneous/.

20 See: "Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications," available at: https://christopherparsonscom.files.wordpress.com/2022/07/a-2020-00246-sges.pdf and, also, Christopher Parsons and Tamir Israel. (2015). "Canada's Quiet History Of Weakening Communications Encryption," *Citizen Lab*. available at: https://citizenlab.ca/2015/08/canadas-quiet-history-of-weakening-communications-encryption/.

2. Proposed Reforms to the Telecommunications Act

This section of the report discusses different parts of the draft legislation. This discussion entails outlining what is possible or required under the legislation and, subsequently, assessing the potential implications of the current drafted language. Where possible, the report provides specific recommendations that are meant to improve the current draft.

2.1. Compelling or Directing Modifications to Organizations' Technical or Business Activities

Under s. 15.1, the government, through an Order in Council, can compel a telecommunications provider to either prohibit the use of certain services or products (s. 15.1(1)(a)) or direct the removal of certain products or services (s. 15.1(1)(b)) in order to secure telecommunications systems from interference, manipulation, disruption, or other (undefined) threats (s. 15.1(1)). Under s. 15.2(1), the Minister of Industry may issue an order that would prohibit (15.2(1)(a)) or suspend (s. 15.2(1)(b)) a telecommunications provider from providing any service to a specified person, including to a telecommunications service provider. Notably, the Minister may "by order, direct a telecommunications service provider **to do anything or refrain from doing anything**... that is, in the Minister's opinion, necessary to secure the Canadian telecommunications system, including against the threat of interference, manipulation, or disruption" (s. 15.2(2), emphasis not in original).

Ministerial Orders would be extensive and include the following, "among other things" (s. 15.2(2)):

Legislative Language in Section 15.2(2)	Plain Language
a) prohibit a telecommunications service provider from using any specified product or service in, or in relation to, its telecommunications network or telecommunications facilities, or any part of those networks or facilities;	A telecommunications service provider can't use X.
(b) direct a telecommunications service provider to remove any specified product from its telecommunications networks or telecommunications facilities, or any part of those networks or facilities;	A telecommunications service provider must remove X.

Legislative Language in Section 15.2(2)	Plain Language
(c) impose conditions on a telecommunications service provider's use of any product or service, or any product or service provided by a specified person, including a telecommunications service provider;	If a telecommunications service provider uses X, they must adopt Y conditions.
(d) impose conditions on a telecommunications service provider's provision of services to a specified person, including a telecommunications service provider;	If a telecommunications service provider provides X type of service, it must adopt Y conditions.
(e) prohibit a telecommunications service provider from entering into a service agreement for any product or service used in, or in relation to, its telecommunications network or telecommunications facilities, or any part of those networks or facilities;	A telecommunications service provider can't get into a deal or agreement with X company for Y product or service.
(f) require that a telecommunications service provider terminate a service agreement referred to in paragraph (e);	A telecommunications service provider must terminate service agreement Y that was designed in s. 15.2(2)(e).
(g) prohibit a telecommunications service provider from upgrading any specified product or service;	A telecommunications service provider can't upgrade X product or service.
(h) require that a telecommunications service provider's telecommunications networks or telecommunications facilities as well as its procurement plans for those networks or facilities, be subject to specified review processes;	A telecommunications service provider's networks, facilities, and procurement plans are all subject to a review process.
(i) require that a telecommunications service provider develop a security plan in relation to its telecommunications services, telecommunications networks or telecommunications facilities;	A telecommunications service provider must develop a security plan.
(j) require that assessments be conducted to identify any vulnerability in a telecommunications service provider's telecommunications services, telecommunications networks or telecommunications facilities or its security plan referred to in paragraph (i);	A telecommunications service provider must identify vulnerabilities, including those that are emergent from the security plans (denoted in s. 15.2(2)(i)) in relation to its networks, facilities, or services.
(k) require that a telecommunications service provider take steps to mitigate any vulnerability in its telecommunications services, telecommunications networks or telecommunications facilities or its security plan referred to in paragraph (i); or	A telecommunications service provider must take steps to mitigate vulnerabilities that were identified in its security plan (as noted atin s. 15.2(2)(i)) or in relation to its networks, facilities, or services.

Legislative Language in Section 15.2(2)	Plain Language
(l) require that a telecommunications service provider implement specified standards in relation to its telecommunications services, telecommunications networks or telecommunications facilities.	A telecommunications service provider is required to implement standards regarding services, networks, or facilities.

Any person may be compelled to provide the Minister or persons designated by the Minister with information that the Minister "believes on reasonable grounds is relevant for the purpose of making, amending or revoking an order under 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" (s. 15.4). The Governor in Council, under s. 15.8, may make regulations pertaining to "any provisions that may be contained in an order made under section 15.2" (s. 15.8(1)(a)) and prescribe "persons and entities for the purposes of 15.6(j)" (s. 15.8(1)(b)). Section 15.6(j) outlines the range of parties that may collect or disclose information from one another, which is taken up in more depth in part 2.4.

Analysis

As drafted, the legislation provides a subset of the cybersecurity threats that might prompt the issuance of either an Order in Council or Ministerial Order. This fact is made apparent by the use of "including" in s. 15.1(1)[21] and s. 15.2(1),[22] as well as under s. 15.2(2). Per s. 15.2(2), a Ministerial Order may be issued to "direct a telecommunications provider to do anything or refrain from anything" so as to "secure the Canadian telecommunications system, **including** against the threat of interference, manipulation or disruption."[23] The result is that the legislation may be relied on, in the future, to address other kinds of activities in excess of interference, manipulation, or disruption to secure the Canadian telecommunications system.

From the outset, the legislation restricts the government to issuing an Order in Council or Ministerial Order only when doing so is necessary to secure the Canadian telecommunications system. Necessity on its own, however, is an insufficient curb on the government's power. Thus, the first recommendation is that the legislation be amended to make explicit that such orders must be necessary, proportionate, and reasonable.

21 "If, in the opinion of the Governor in Council, it is necessary to do so to secure the Canadian telecommunications system, **including** against the threat of interference, manipulation or disruption, the Governor in Council may, by order,..." Emphasis not in original.

22 "If, in the Minister's opinion, it is necessary to do so to secure the Canadian telecommunications system, **including** against the threat of interference, manipulation or disruption, the Minister may, by order and after consultation with the Minister of Public Safety and Emergency Preparedness…" Emphasis not in original.

23 Emphasis not in original.

Recommendation 1: Orders in Council and Ministerial Orders Must Be Necessary, Proportionate, and Reasonable

The legislation should be amended to impose further conditions surrounding the specific circumstances under which the government can exercise its powers.

Original Text	Proposed Amendment
15.1 (1) If, in the opinion of the Governor in Council, it is necessary to do so to secure the Canadian telecommunications system, including against the threat of interference, manipulation or disruption, the Governor in Council may, by order,	15.1 (1) If, in the opinion of the Governor in Council, it is necessary, proportionate, and reasonable to do so to secure the Canadian telecommunications system, ~~including~~ against the threat of interference, manipulation or disruption, the Governor in Council may, by order,
15.2(2) The Minister may, by order, direct a telecommunications service provider to do anything or refrain from doing anything — other than a thing specified in subsection (1) or 15.1(1) — that is specified in the order and that is, in the Minister's opinion, necessary to secure the Canadian telecommunications system, including against the threat of interference, manipulation or disruption. In the order, the Minister may, among other things,	15.2(2) The Minister may, by order, direct a telecommunications service provider to undertaken actions which are necessary, proportionate, and reasonable ~~do anything or refrain from doing anything~~ — other than a thing specified in subsection (1) or 15.1(1) — to fulfil directions that are ~~is~~ specified in the order and that is, in the Minister's opinion, necessary to secure the Canadian telecommunications system, ~~including~~ against the threat of interference, manipulation or disruption. In the order, the Minister may, ~~among other things,~~

Second, the legislation lacks a provision that private organizations will be provided with a reasonable period of time in which to modify their practices (see: s. 15.1(1)(a)-(b) and s. 15.2(1)(a)-(b); see also s. 15.2(2)(a)-(l)).[24] While an order can be made only when doing so is necessary, there isn't a correlated requirement that it is actually possible for a provider to implement the order within the assigned time frame. Put somewhat differently, while the government might correctly identify a threat that necessitates a change in how a telecommunications provider operates, the speed at which the government expects a change to be implemented may be unreasonable given the complexity of a provider's network or services.

24 Section 9 of the *Critical Cyber Systems Protection Act* does set out timeframes for establishing a cybersecurity program. It, also, includes the ability to provide extensions to times set out in the Act at the discretion of the appropriate regulator (s. 11 and s. 14(3)) .

The result is that the government may issue orders that potentially reflect unawareness about or care for the challenges that are involved in implementing prohibitions or directions or that demonstrate little concern for the financial burdens that such activities could impose on private organizations and, by extension, their users, subscribers, or customers. While telecommunications providers can seek redress by appealing to the federal court for judicial review of Orders in Council or Ministerial Orders, organizations might not need to appeal to this complaints-driven process if the government was required when preparing an order to make clear that changes in telecommunications providers' networks or services must be performed in a reasonable period of time. While it is possible that such time frames might normally be developed using organizations such as the Canadian Security Telecommunications Advisory Committee (CSTAC) the legislation should be more explicit.[25] Reasonableness in implementation speeds should be clarified in legislation as opposed to being established through coordinating bodies, such as CSTAC, and especially where such bodies do not include all of the telecommunications providers that may receive orders.

Recommendation 2: Orders Should Include a Reference to Timelines

The draft legislation should be amended to include a requirement that telecommunications providers must implement cybersecurity demands or orders within a reasonable period of time in situations where compliance with a demand or order would require significant or material changes to the recipients' business or technical operations.

Third, some of the specific activities that private organizations might be directed to perform in s. 15(2)(a)-(l) may generate downstream security challenges. Under s. 15.2(2)(g), as an example, telecommunications service providers might be prohibited from upgrading a specified product or service. Such a prohibition might be issued because the government judges the upgrade as likely part of a supply chain attack, where the newer version of a product or service contains malicious code or because a government agency, such as the Communications Security Establishment, requires additional time to analyse the update to assess whether it includes any serious vulnerabilities that have either been incidentally or deliberately added to the codebase. However, in the process of prohibiting an upgrade, known-good security patches, hardware upgrades, or service offerings in the same update package might also be blocked. Moreover, this prohibition may have escalating cybersecurity consequences where a private organization is barred from *ever* updating a product or service from a specific vendor or *ever* doing so in a timely fashion; this type of circumstance could turn into a challenge for business operations

25 For more information, see: Government of Canada. (2020). "Canadian Security Telecommunications Advisory Committee (CSTAC)," Government of Canada. Available at: https://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/h_sf10727.html.

if there are no other vendors with equivalent replacement products or services. More concretely, if a prohibition was placed on using a vendor who sold niche equipment to telecommunications providers in rural or less-populated parts of Canada where without this equipment telecommunications service could not be efficiently offered, compliance with the order might lead to Canadian customers losing access to their current quality of telecommunications services.

Recommendation 3: Government Should Undertake Impact Assessments Prior to Issuing Orders

The legislation should make clear that the government must undertake assessments of its orders to determine if they could have secondary- or tertiary-impacts that would have the effect of worsening an organization's cybersecurity practices or stance. These assessments should be presented to telecommunications providers along with any demands or orders or regulations that are based upon these assessments. Such assessments should be included in any and all proportionality analyses of government demands or orders.

It is possible that the government may issue an order or regulation that has the effect of severely altering or impairing how a telecommunications provider can offer a service to its existing customers. If, even following judicial review, an order is found to be necessary, proportionate, and reasonable, a provider should be able to seek some financial relief when implementing changes to their technical or business operations would have a material impact on the economic viability of their organization.

Recommendation 4: Forbearance or Cost/Cost-Minus Clauses Should Be Inserted

The legislation should be amended such that telecommunications providers can seek forbearance of certain orders where implementing them would have a material impact on the providers' economic viability. Alternatively, if an order or regulation would have a deleterious effect on a telecommunications provider's economic viability and the government demands that the order be fulfilled regardless, the provider should be compensated on either a cost or cost-minus basis.[26]

Fourth, s. 15.2(2)(l) of the legislation would enable the Minister to "require that a telecommunications service provider implement specified standards in relation to its telecommunications services, telecommunications networks or telecommunications facilities." This power could enable the Minister to compel telecommunications providers to, as an example, enable optional security standards in telecommunications

26 "Cost-minus" refers to a compensation system where the full cost is not remunerated. In this case, it would entail the government providing some, but not all, of the cost-based compensation associated with telecommunications services providers modifying their service offerings to subscribers in their efforts to comply with an Order in Council, Ministerial Order, or regulation.

standards, establish effective multifactor authentication on internal- as well as customer-facing interfaces, or otherwise do anything that has been standardized somewhere. It is possible that standards might even be set for physical security of telecommunications facilities, including requiring certain modes of biometric identity confirmation, security clearances to be held by employees, or anything else that is considered standardized.

A previous Citizen Lab report on telecommunications security argued that the government should be empowered to impose security standards as needed. Specifically, that report stated,

> the government could compel Canadian telecommunications companies to enable security elements in 5G or, alternatively, it could impose market penalties on companies that decline to enable such elements (e.g., held liable for damages or data exfiltrations where networks have not fully enabled 5G security elements). Should these approaches be found still lacking, the government could mandate baseline security standards that were vendor agnostic and that all Canadian carriers (and their vendors) were required to meet as a condition of providing 5G service in Canada.[27]

Without a clear definition of what is envisioned as a standard in the draft legislation, it is challenging to assess whether the government is contemplating international standards or recommendations (e.g., 3GPP, GSMA Recommendations, IEEE, IETF, CALEA or ETSI, etc.), standards that are developed and promulgated by the Canadian government or Canadian organizations, or demands that telecommunications providers adopt standards that 'secure' information by enabling the government to access, assess, or collect providers data traffic for law enforcement or national security purposes. To illustrate this latter point, a Ministerial Order could compel telecommunications providers to adopt potentially problematic encryption standards on the basis that having visibility into some traffic could secure the Canadian telecommunications system by way of better enabling law enforcement or security agencies to identify and act against threats.[28] Alternatively, standards might compel wireline telecommunications providers to adopt lawful interception equipment that comports with international standards, such as the United States' *Communications Assistance for Law Enforcement Act* (CALEA) or those promulgated by the European Telecommunications Standards Institute (ETSI).

To be clear, enabling the government to compel telecommunications providers to adopt certain standards to best secure networks and services is a good thing. As drafted

---

27 Christopher Parsons. (2020). "Huawei & 5G: Clarifying the Canadian Equities and Charting a Strategic Path Forward," *Citizen Lab*. Available at: https://citizenlab.ca/2020/12/huawei-5g-clarifying-the-canadian-equities-and-charting-a-strategic-path-forward/, p. 26.

28 See: Matthew Braga. (2016). "Rogers and Alcatel-Lucent Proposed an Encryption Backdoor for Police," *Motherboard*. Available at: https://www.vice.com/en/article/pgkpvz/rogers-and-alcatel-lucent-proposed-an-encryption-backdoor-for-police; Steven J. Murdoch. (2016). "Insecure by design: protocols for encrypted phone calls," Bentham's Gaze. Available at: https://www.benthamsgaze.org/2016/01/19/insecure-by-design-protocols-for-encrypted-phone-calls/.

presently, however, the legislation does little to clarify the grounds upon which standards might be required[29] nor are there balancing requirements for adopting standards (e.g., assessing whether a given standard might jeopardize individuals' privacy or communications security). The consequence is that what is a potentially positive aspect of the legislation could, in fact, be prospectively used for more nebulous purposes that could compromise the ability of telecommunications service providers to secure their networks or the communications of their subscribers.

Recommendation 5: The Standards That Can Be Imposed Must Be Defined

The legislation should be amended such that it is clear what kinds of standards are within and outside of the scope of the legislation. It should be made explicit that an order or regulation compelling the adoption of particular standards cannot be used to deliberately or incidentally compromise the confidentiality, integrity, or availability of a telecommunications facility, telecommunications service, or transmission facility. 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.

2.2. Secrecy and Absence of Transparency or Accountability Provisions

As currently drafted, Bill C-26 contains numerous secrecy and confidentiality requirements. At a high level, these requirements are meant to ensure that information pertaining to security vulnerabilities, threat actors, or national security information is not made public. Where there are known threats or active threat operations, it may not be in the government's interest to disclose what they know and potentially tip off threat actors of either existent or prospective vulnerabilities. This philosophy pervades the draft legislation.

Both Orders in Council (s. 15.1(2)) or Ministerial Orders issued by the Minister of Industry (s. 15.2(3)) can include provisions that prohibit the disclosure of part or all of the content of the order "by any person." Moreover, these orders "must" be published in the *Canadian Gazette* unless either the Governor in Council (s. 15.1(4)) or Minister (s. 15.2(5)) directs otherwise. In cases where an order is promulgated to telecommunications providers but is inconsistent with "a decision of the [Canadian Radio-television and Telecommunications Commission] made under this Act or another order made, or any authorisation issued, by the Minister under this Act or the *Radiocommunications Act*, the [Ministerial] order... prevails to the extent of the inconsistency" (s. 15.2(6)). If or when the Governor in Council

29 Section 15.2(2) establishes that if the Minister is of the opinion that a standard is necessary to "secure the Canadian telecommunications system", then sufficient grounds have been met to compel the standard's adoption.

makes regulations, similarly, any inconsistencies between those regulations and "a decision of the Commission" or "an order made or an authorisation issued by the Minister under this Act or the *Radiocommunications Act*, the regulation prevails to the extent of the inconsistency" (s. 15.8(2)).

Analysis

The draft legislation has extensive and overly onerous secrecy and confidentiality requirements. Some secrecy or confidentiality arguably does belong in the legislation on the basis that it makes relatively little sense for the government to publicize known vulnerable systems or products; telecommunications providers will need some time to close off existent or potential vulnerabilities. However, at the same time, the draft legislation's confidentiality requirements are too extensive and can enable the government to act without having placed appropriate restrictions on its powers or attaching accountability mechanisms to its order making powers.

First, the *Canadian Gazette* is typically where the Government of Canada will publicize "new statutes, new and proposed regulations, administrative board decisions and public notices."[30] While sections 15.1(4) and 15.2(5) assert that orders "must'' be similarly published, at the same time, the Minister has the authority to "direct otherwise in the order". The result is that the government might issue orders that never appear in the *Canadian Gazette*, and there is no requirement for the order to ever be published in a complete and non-redacted format. This ultimately means that the government could compel modifications in how private organizations' technical or business practices are conducted, even where such modifications are disproportionate to a threat or are counterproductive to protecting Canadian critical infrastructure from threats, and the government would never risk public backlash or critique based on the public reading and analyzing the order(s) in question. Moreover, there is no test that must be met prior to prohibiting an order from being published in the *Gazette* with the effect that the decision is left to the Governor in Council's or Minister's respective whim instead of a demonstrable and pressing need.

Recommendation 6: Orders Should Appear in *The Canadian Gazette*

The legislation should be amended such that orders must be published in the *Canadian Gazette* within 180 days of issuing them or within 90 days of an order being implemented, based on whichever condition is met first.

30 Government of Canada. (2022). "Canada Gazette," Government of Canada. Available at: https://www.gazette.gc.ca/accueil-home-eng.html.

Recommendation 7: The Minister Should Be Compelled to Table Reports Pertaining to Orders and Regulations

The legislation should be amended such that the Minister of Industry is required to annually table a listing of:

- the number of orders and regulations that have been issued
- the kinds of orders or regulations that have been issued
- the number of telecommunications providers that have received the orders
- the number of telecommunications providers that have partially complied with the orders
- the number of telecommunications providers that have completely complied with the orders
- a narrative discussion of the necessity, proportionality, reasonableness, and utility of the order-making power

If the Minister fails to table such reports, the Minister should be required to appear before a parliamentary committee to explain this failure and provide a time frame within which the report will be tabled.

Second, Orders in Council or Ministerial Orders may include gag provisions. These may prevent whistle-blowers from notifying the public of disproportionate or deficient directions or prohibitions from the government. This gag lacks a reasonableness, necessity, or proportionally test that could delimit when a gag can be included in an order. The legislation also does not include language that would lift the gag after a period of time, such as within a specific period of time (e.g., 90, 180, or 365 days) or following the completion of some action (e.g., implementing practices that are responsive to the order in question), or some combination (e.g., 90 days after implementing practices that are responsive to the order or regulation in question). Consequently, it is possible for all orders to include gags that are never lifted with the effect that individuals in Canada or even private organizations will never realize the extent(s) to which the government is issuing orders or regulations.

Recommendation 8: Gags Should Be Time Limited

The legislation should be amended to include a specific period of time after which an order or regulation is received, or following the time of compliance with an order or regulation, that a telecommunications provider can publicize that it received and/or entered into compliance with an order or regulation.

Third, the potential for an Order in Council or Ministerial Order or regulation to override a decision from the Canadian Radio-television and Telecommunications Commission (CRTC), accompanied by the aforementioned secrecy provisions, risks creating a new kind of quasi-shadow law. The CRTC holds relatively open public processes where intervenors can present and challenge evidence and the CRTC's positions in the process of generating a public set of rules for how telecommunications providers can or must operate.

However, the CRTC's decisions are not always factually correct,[31] which could in some situations prospectively compel telecommunications providers to take actions that run counter to what the Government of Canada believes is best to secure Canada's telecommunications infrastructure.

While it is perhaps understandable that the government would like the ability to prevent telecommunications providers from undertaking activities it considers harmful to Canadian interests, the Orders in Council or Ministerial Orders or regulations that telecommunications providers receive will not necessarily be made public. This runs the risk of creating a kind of public law—known through CRTC decisions—and shadow law—understood only to parties that have received countermanding government orders or regulations—with the effect of inhibiting individuals in Canada from actually understanding the rules that govern telecommunications providers that operate in Canada.

Recommendation 9: The CRTC Should Indicate When Orders Override Parts of CRTC Decisions

The legislation should be amended to, at a minimum, require that the CRTC post a public notice attached to any of its decisions where there is a contradiction between its decision and an Order in Council or Ministerial Order or regulation that has prevailed over part of a CRTC decision.

Fourth, the potential for the government to issue orders or regulations that override public law decisions that are reached through CRTC processes may jeopardize the process by which decisions are reached by intervenors in CRTC hearings. While the present CRTC deliberative process is subject to external critique, the process nevertheless remains relatively transparent to providers and the public. In introducing the ability to quietly compel telecommunications providers to do a thing, potentially in contravention of CRTC decisions and without public notice, the very value or importance of participating in CRTC decisions associated with cybersecurity are drawn into question: why participate when the government might secretly issue orders that are contrary to the publicly debated procedure and associated decisions?

Recommendation 10: Annual Report Should Include the Number of Times Government Orders or Regulations Prevail Over CRTC Decisions

The legislation should be amended to require the government to annually disclose the number of times it has issued orders or regulations that prevailed in the case of an inconsistency between a given order or regulation and a CRTC decision, as well as denote which CRTC decision(s) were affected.

31 See as an example: CIRA's 'Clarification' where it explains why a recent CRTC decision concerning botnets failed to understand some of the services that CIRA offers to Mozilla. Available at: Canadian Internet Registration Authority (CIRA). “A Botnet Blocking Framework for Canada,” CIRA. Available at: https://www.cira.ca/blog/state-internet/a-botnet-blocking-framework-canada.

Fifth, one of the roles of Parliament is to scrutinize regulations. By imposing gag restrictions on regulations, potentially excluding them from the *Canadian Gazette*, and having amended the Statutory Instruments Act in 2015[32] it is possible that the Standing Joint Committee for the Scrutiny of Regulations will be unable to hold the government accountable for the regulations that are enacted under the drafted reforms to the *Telecommunications Act*. The result is that regulations might be created and promulgated without the Committee being able to assess the "legality and the procedural aspects of regulations, as opposed to the merits of particular regulations or the policy they reflect."[33]

Recommendation 11: All Regulations Under *the Telecommunications Act* Should Be Accessible to The Standing Joint Committee for the Scrutiny of Regulations

The legislation should be amended such that the Standing Joint Committee for the Scrutiny of Regulations is able to obtain, assess, and render a public verdict on any regulations that are promulgated under the proposed draft reforms to the *Telecommunications Act*. The Committee should also be empowered to obtain, assess, and render a public verdict on regulations pertaining to the *Telecommunications Act* and that are modified pursuant to s. 18 of the *Statutory Instruments Act.*

2.3. Deficient Judicial Review Process

In situations where telecommunications providers disagree with orders made under either s. 15.1 (Order in Council) or s. 15.2 (Ministerial Orders), or regulations under s. 15.8(1)(a), they can request a judicial review. Specifically, where a telecommunications provider "believes that a certain governmental authority has exercised its power in an arbitrary, discriminatory, or otherwise unreasonable way, [they] can file a suit in a court

32 The *Statutory Instruments Act* was amended to provide for documents (or other pieces of information) to be incorporated into a regulation without need for consideration by the Scrutiny of Regulations Committee. See: "Bill S-2: Statutes of Canada 2015–An Act to amend the Statutory Instruments Act and to make consequential amendments to the Statutory Instruments Regulations," Parliament of Canada. Available at: https://www.parl.ca/Content/Bills/412/Government/S-2/S-2_4/S-2_4.PDF. S. 18.

33 Standing Joint Committee for the Scrutiny of Regulations. (2022). "About," Parliament of Canada. Available at: https://www.parl.ca/Committees/en/REGS/About.

The Committee judges each regulation against 13 criteria. This involves assessing whether a given regulation: "1. is not authorized by the terms of the enabling legislation or has not complied with any condition set forth in the legislation; 2. is not in conformity with the Canadian Charter of Rights and Freedoms or the Canadian Bill of Rights; 3. purports to have retroactive effect without express authority having been provided for in the enabling legislation; 4. imposes a charge on the public revenues or requires payment to be made to the Crown or to any other authority, or prescribes the amount of any such charge or payment, without express authority having been provided for in the enabling legislation; 5. imposes a fine, imprisonment or other penalty without express authority having been provided for in the enabling legislation; 6. tends directly or indirectly to exclude the jurisdiction of the courts without express authority having been provided for in the enabling legislation; 7. has not complied with the Statutory Instruments Act; 8. appears for any reason to infringe the rule of law; 9. trespasses unduly on rights and liberties; 10. makes the rights and liberties of the person unduly dependent on administrative discretion or is not consistent with the rules of natural justice; 11. makes some unusual or unexpected use of the powers conferred by the enabling legislation; 12. amounts to the exercise of a substantive legislative power properly the subject of direct parliamentary enactment; 13. is defective in its drafting or for any other reason requires elucidation as to its form or purport."

of law and ask for 'judicial review', that is, to ask that the court review the administrative decision. If the court finds in favour of the plaintiff, it can annul the administrative decision."[34] Under the draft legislation, however, the process by which judicial review would proceed could be clouded in secrecy.

To begin, the Minister of Industry may request that some of the government's evidence be heard exclusively by the judge. If the government makes this request and the judge concludes that "the disclosure of the evidence or other information could be injurious to international relations, national defence or national security or endanger the safety of any person", then the judge must grant the request (s. 15.9(1)(a)). The judge must ensure the confidentiality of any such evidence where "its disclosure would be injurious to international relations, national defence or national security or endanger the safety of any person" (s. 15.9(1)(b)).

The applicant for the review must be provided with "a summary of the evidence and other information available to the judge that enables the applicant to be reasonably informed of the Government of Canada's case", but the applicant is not permitted access to information that "in the judge's opinion, would be injurious to international relations, national defence or national security or endanger the safety of any person if disclosed" (s. 15.9(1)(c)). While the applicant and Minister must have an opportunity to be heard (s. 15.9(1)(d)), the judge's ultimate decision can be made based on evidence that was not presented to the applicant (s. 15.9(1)(e)). The decision cannot be based on evidence which was withdrawn or found to be irrelevant (s. 15.9(1)(f)). All evidence presented by the Minister, including that which is withdrawn, must be kept confidential (s. 15.9(1)(g)). Any appeals must incorporate the same secrecy provisions (s. 15.9(2)).

Analysis

There is a possibility that an Order in Council or Ministerial Order or regulation may be based on evidence that has been obtained by a Canadian security or intelligence agency or was provided to the Canadian government by a foreign state or organization. The security and intelligence community zealously guards its sources and methods, as well as those of foreign organizations, for fear that revealing sources and methods might impair ongoing intelligence collection or endanger information sharing with foreign states and organizations. The rationale for the secrecy in s. 15.9 is presumably that absent these safeguards the government will have to carefully assess whether it wants to present evidence that could justify compelling private organizations to modify their technical or business practices, or choose not to compel the modification and instead preserve the secrecy of relevant sources and methods.

34 Centre for Constitutional Studies. (2019). "Judicial Review," Centre for Constitutional Studies. Available at: https://www.constitutionalstudies.ca/2019/07/judicial-review/.

Section 15.9, in other words, is designed, at least in part, to let the government use secret evidence or intelligence to develop orders and regulations without running the risk of such evidence or intelligence being made public or revealed to non-government parties.

However, the draft legislation would have the effect of potentially preventing telecommunications providers from making full-throated arguments for why a government's order was arbitrary, discriminatory, or otherwise unreasonable. Consider the following: the government learns that there is a vulnerability in part of a software update, and the security and intelligence community suspects it could be exploited by motivated adversaries to interfere, manipulate, or disrupt the Canadian telecommunications system. In response, the Minister issues an order to prohibit telecommunications providers from upgrading the products (s. 15.2(2)(g)) and, subsequently, to adopt particular conditions for future software updates (s. 15.2(2)(b))). The order may not, however, explain or justify the proportionality or reasonableness of the directive or describe which specific elements of a patch have raised concerns, and thus cause the telecommunications provider to apply for judicial review.

The telecommunications provider could be opposed to the order on the basis that:

- If updates are *not* applied, then all other vulnerabilities that are ameliorated in the software patch will be known to adversaries, and they can then leverage those to try and exploit the providers' networks or systems.
- It is impracticable or impossible to separate out just the exploitable element(s) of the software update, and on a balance of probabilities, it is more important to secure as much of the network or system as possible, notwithstanding the potentially exploitable vulnerabilities that would also be introduced.

In either of these cases, the provider in question could mount an argument without access to secret evidence. However, unless a government order denotes a specific *part* of an update that is problematic, the provider may be unable to offer suggestions of alternative and more proportionate methods of mitigating the threat in question. As an example, it is possible that a given software update could be implemented *and* threat mitigated, but for a provider to make this argument, they would need to understand the specific, actionable threat vector to develop a mitigation policy

There are other situations where the government might issue a demand, but the providers would be unable to mount a fulsome argument against the government’s directive without access to the government’s secret evidence. For example, the government might issue orders that align with the government’s adversarial or politicized posture toward particular vendors and services that operate out of the People’s Republic of China. While a federal judge might decide that an order barring ZTE and Huawei was legitimate in light of evidence published by the United Kingdom’s The National Cyber Security Centre (NCSC),

how should the same judge assess prospective risks posed by other Chinese vendors where less information is published about them? Similarly, how could a judge assess situations where services that a telecommunication provider relies on has code contributed to it by individuals with Chinese citizenship and who are believed to be acting to comply with China's expansive national security law? Where the government's specific evidence is not presented to providers, they may be unable to robustly argue that the government's arguments are derived less from the evidence presented than from suppositions surrounding such evidence.

Finally, it is possible that the perceived vulnerability, itself, may not be a vulnerability. Put differently, the technical evidence the government bases its order or regulation upon may be deficient. In any situation where revelation of the evidence is framed by the government as harmful to Canada's national defence and thus excluded from a provider's view, a provider might be unable to present why the technical conclusions reached by the government would fail to meet the necessity requirement associated with an order, let alone its proportionality or reasonableness.

Broadly, then, the issue with secret evidence potentially forming the basis of a decision out of judicial review is that providers may be forced to undertake actions or cease certain activities where the evidence in question does not fully support the government's directive. What might be done to correct this? At a minimum, the legislation should make explicit that where evidence is sufficiently sensitive to bar a telecommunications provider's counsel from hearing it that *amicus curiae* might be appointed to hear and potentially contest the evidence at hand.[35] There needn't be a *requirement* for one to be appointed—it is possible that, in some cases, the evidence is such that it is clear that an order is not arbitrary, discriminatory, or unreasonable—but building *amicus curiae* explicitly into the legislation might reduce the opaqueness of the review process and, as a result, enhance the perception of the reasonableness of government orders and correctness of judicial decisions.

Recommendation 12: Judicial Review Should Explicitly Enable Appointment of *Amicus Curiae*

The legislation should be amended such that, at the Court's pleasure, *amicus curiae* can be appointed to contest and respond to information provided by the government in support of an Order in Council, Ministerial Order, or regulation under s. 15.8.

35 As noted by Justice Mosley, "*amicus curiae* to assist [the Federal Court] in examining the contested information and to respond to the arguments of the Attorney General...The amicus will be given access to the disputed materials on a confidential basis, and will be able to challenge the government's claims that the public disclosure of the information in question will harm national security, national defence or international relations. The amicus can also make representations on behalf of the accused person or interested party in relation to the balancing exercise that has to be carried out by the designated judge." See: The Honourable Richard G. Mosley. (2015). ""A View from the Bunker: The Role of the Federal Court in National Security," Federal Court of Canada. Available at: https://www.fct-cf.gc.ca/Content/assets/pdf/base/Mosley%20J%20lecture%20-%20A%20View%20from%20the%20Bunker%20-%20for%20posting%20(ENG).pdf.

2.4. Extensive Information Sharing Within and Beyond Canadian Agencies

The Minister of Industry has extensive capabilities to compel the disclosure of information from telecommunications providers and subsequently share it widely within the federal government as well as internationally. Any person may be required to provide the Minister of Industry with information 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" (s. 15.4).

Confidential information is defined in s. 15.5(1) and includes (a) trade secrets, (b) confidential financial, commercial, scientific, or technical information, and information that could reasonably be expected to (c)(i) result in material financial loss or gain to any person, (c)(ii) prejudice the competitive position of any person, or (c)(iii) affect contractual or other negotiations of any person. The definition does not make explicit that personal information would necessarily constitute confidential information.

While no person "shall knowingly disclose or knowingly permit to be disclosed" any confidential information, there are exceptions. It may be disclosed when required by law (s. 15.5(3)(a)), when the party who designated it as confidential approves the disclosure (s. 15.5(3)(b)), or when "the disclosure is necessary, in the Minister's opinion, to secure the Canadian telecommunications system, including against the threat of interference, manipulation or disruption" (s. 15.5(3)(c)).

Section 15.6 makes clear how wide a range of parties may, notwithstanding s. 15.5, collect or disclose information for the purposes of "making, amending or revoking … an order under section 15.1 or 15.2 or a regulation under paragraph 15.8(1)(a)" or "to [verify] compliance or [prevent] non-compliance with such an order or regulation." This range of parties includes:

> (a) the Minister;
>
> (b) the Minister of Public Safety and Emergency Preparedness;
>
> (c) the Minister of Foreign Affairs;
>
> (d) the Minister of National Defence;
>
> (e) the Chief of the Defence Staff;
>
> (f) the Chief or an employee of the Communications Security Establishment;
>
> (g) the Director or an employee of the Canadian Security Intelligence Service;
>
> (h) the Chairperson or an employee of the Commission;
>
> (i) a person designated under section 15.4; and
>
> (j) any other prescribed person or entity.

Moreover, per s. 15.7(1) any non-confidential information may also:

> 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**.[36]

If information is shared with a foreign government, there is the possibility of Canadian companies or individuals suffering non-penal consequences. If a telecommunications provider has engaged in conduct that is counter to an order under s. 15.1 or s. 15.2 or a regulation under the Act and where a law of a foreign state addresses conduct that is substantially similar to such an order or regulation (s. 15.7(2)), the foreign state cannot use the information for pursuing criminal investigations. However, the foreign state could potentially initiate regulatory proceedings or private rights of action. For example, should a telecommunications provider have regulatory obligations in a foreign state that parallel the requirements set out in an order under s. 15.2 or s. 15.2, or a regulation under 15.8, the foreign regulator could launch an action. If, say, the United States government had placed a ban on software services from a given vendor or imposed specific reporting requirements paralleling Canada's and a provider was found to have violated these orders, the provider might run afoul of US regulators.[37] Section 15.7(2), then, has the potential of exposing telecommunications providers that operate in Canada to foreign legal proceedings.

Analysis

The power to compel confidential information is needed to enable, enforce, and assess orders under s. 15.1 and s. 15.2, as well as regulations under s. 15.8. However, while the draft legislation would empower the Minister to collect and widely disclose telecommunications providers' information and confidential information, the legislation does not bake in accountability requirements for the government. Each of the recommendations in this section of the report would move toward inscribing governmental accountability into the legislation.

First, the legislation makes clear that when or if the Minister compels information (including confidential information) from a telecommunications provider, it may be

36 Emphasis not in original.

37 While outside the scope of this report, some requirements imposed on telecommunications providers and critical infrastructure providers can be found in: White House. (2021). "Executive Order 14028: Improving the Nation's Cybersecurity," The White House. Available at: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/; or Department of Home Affairs. (2022). "Security Legislation Amendment (Critical Infrastructure Protection) Act 2022," Government of Australia. Available at: https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/slacip-bill-2022.

circulated widely across the Government of Canada. Domestically, s. 15.6(j) will mean that any party may theoretically receive the information in question.[38] This may have the effect of granting the government far deeper insight into the configuration, operation, and management of telecommunications providers' systems while simultaneously heightening risks that confidential information, as well as personal or de-identified information, may be inappropriately circulated or disclosed, simply by merit of the sheer number of parties or individuals who may become aware of the information. No particular penalty is applied to the Canadian government should the party who receives the confidential information, or personal or de-identified information, unknowingly or accidentally permit its disclosure.

Recommendation 13: Relief Should Be Available If Government Mishandles Confidential Information

The legislation should be amended to enable telecommunications providers to seek relief should the government or a party to whom the government has disclosed confidential information unintentionally loses control of that information, where that loss of control has material consequences for a telecommunication provider's business or technical operations.

Recommendation 14: Relief Should Be Available If Government Mishandles Personal or De-Identified Information

The legislation should be amended to enable individuals to seek relief should the government or a party to whom the government has disclosed their personal or de-identified information unintentionally loses control of that information and where that loss of control materially affects the individual.

Second, there is no requirement to inform the telecommunications provider whether or why its confidential information is being shared within federal agencies and with Canadian institutions. Section 15.4 does not require the Minister to explain why information is being collected or to whom it might be circulated.[39] This may place telecommunications providers in situations where they neither appreciate what, specifically, is required by the Minister nor who will be reviewing or making use of the provided information.

38 "**15.6** Despite section 15.5, to the extent that 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 … (j) any other prescribed person or entity."

39 "**15.4** The Minister may require any person 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 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."

Recommendation 15: Government Should Explain How It Will Use Information and Reveal the Domestic Agencies To Which Information Is Disclosed

The government should be required to provide to affected telecommunications providers at least a general summary of how it intends to use any information it obtains from them, including confidential information, as well as a description of the parties to whom the information will or may be disclosed.

Third, the legislation does not tightly restrict how government agencies may use information they receive from telecommunications providers, vis-a-vis powers conveyed to the Minister of Industry under Bill C-26. In the case of the Communications Security Establishment (CSE) as an example, information that it receives could be used to facilitate any aspect of its mandate and not just the cybersecurity and information assurance elements of that mandate. Information from telecommunications providers could be used to inform some elements of the CSE's signals intelligence activities, cybersecurity and information assurance operations, assistance to other designated federal agencies, or even its active or defensive cyber operations. The legislation should make clear how receiving agencies can use information from telecommunications providers and bar these agencies from using the information for activities not in the service of cybersecurity or information assurance.

Recommendation 16: Information Obtained from Telecommunications Providers Should Only be Used for Cybersecurity and Information Assurance Activities

The legislation should be amended to restrict government agencies to exclusively using information obtained from telecommunications providers under Bill C-26 for cybersecurity and information assurance activities. Information should not be permitted to 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. These restrictions should apply to all agencies, including but not limited to those under the purview of the Minister of Public Safety and Emergency Preparedness (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).

Fourth, there is no language in the legislation that would compel Canadian agencies to delete or destroy information or confidential information obtained from telecommunications providers after a given period of time or an event having occurred (e.g., assessing compliance with an order). The result is that government agencies might retain information from telecommunications companies indefinitely with the effect of insufficiently incorporating accountability provisions alongside proposed new government powers.

Recommendation 17: Data Retention Periods Should Be Attached to Telecommunications Providers' Data

The legislation should be amended to make clear that information obtained from telecommunications providers will be retained only for as long as necessary to make, amend, or revoke an order under section 15.1 or 15.2 or a regulation under paragraph 15.8(1)(a), or to verify the compliance or prevent non-compliance with such an order or regulation.

Retention periods should be communicated to telecommunications providers from whom the Minister has collected information.

Fifth, the legislation does not require the government to impose data retention and deletion requirements on foreign states, agencies, or organizations to whom the Canadian government discloses telecommunications service providers' information. Just as the government should be compelled to adopt retention periods, so should any international bodies that receive providers' information.

Recommendation 18: Data Retention Periods Should Be Attached to Foreign Disclosures of Information

The draft legislation should be amended to require that the government attach data retention and deletion clauses in agreements or memoranda of understanding that are entered into with foreign agencies.

Sixth, there is no requirement to inform a telecommunications provider of the range of foreign parties with whom its information has been disclosed. Given that foreign parties can use information to launch investigations and bring non-penal charges against providers, the government should provide some notice when telecommunications providers' information is being, or has been, shared for cybersecurity purposes.

Recommendation 19: Telecommunications Providers Should Be Informed Which Foreign Parties Receive Their Information

The legislation should be amended such that telecommunications providers are explicitly informed of when and, if so, to whom information can be disclosed when the receiving party is a foreign state, agency, organisation, or party.

Original Text	Proposed Amendment
15.7 (1) Any information collected or obtained under this Act, other than information designated as confidential under subsection 15.5(1), may be disclosed by the Minister under an agreement, a memorandum of understanding or an arrangement in writing between the Government of Canada and the government of a province or of a foreign state, an international organization of states or an international organization established by the governments of states, or any institution of any such government or organization, if the Minister believes that the information may be relevant to securing the Canadian telecommunications system or the telecommunications system of a foreign state, including against the threat of interference, manipulation or disruption.	15.7 (1) Any information collected or obtained under this Act, other than information designated as confidential under subsection 15.5(1), will only be ~~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~~ is or will 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.

Seventh, s. 15.7(1) makes clear that non-confidential information may be disclosed under a memorandum of understanding where 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."[40] The conjoined use of "believes" and "may be" suggests that the possible threshold that must be met prior to disclosing information is not particularly high and thus could enable significant sharing of private, if not confidential, information.

Further, the use of "including" in the current draft legislation does not tightly delimit what is meant by "securing" a Canadian or foreign telecommunications system. The effect is that while information may be shared to address threats of interference, manipulation,

40 Emphasis not in original.

or disruption, it could be disclosed for other threats that are not explicit in the legislation. Interference, manipulation, and disruption are already very broad categories of possible threats. The government should be required to table amendments to this tripartite list instead of being enabled to just quietly append other kinds of activities without having to publicize additions to the list. Specifically enumerating the threats that justify disclosing private, though not confidential, information will add a check to the government's future uses of private organizations' information.

Recommendation 20: Legislation Should Delimit the Conditions Wherein a Private Organization's Information Can Be Disclosed

The government should restrict the conditions under which the Minister can disclose a private organizations' information.

2.5. Costs Associated with Security Compliance

Bill C-26 provides the Minister of Industry with an extremely broad capability to require telecommunications providers to do or to refrain from doing anything so long as the ordered action would secure the Canadian telecommunications system against threats, including those associated with interference, disruption, or manipulation activities or operations. Providers that protest the orders but are unsuccessful in seeking judicial review will have to comply with the orders, even if they have not received the evidence that is used to justify an order or regulation. Providers will not be entitled to compensation "for any financial losses" associated with following an order under s. 15.1 or s. 15.2 (s. 15.1(5) and s. 15.2(7)).

Analysis

First, the costs associated with complying with orders and regulations may vary significantly based on what the government demands of a telecommunications provider, and smaller providers may be challenged in managing these costs. As an example, consider the costs that may be incurred in developing a comprehensive security plan that also accounts for identifying and managing vulnerabilities, mitigation practices, and standards compliance. The cost of developing such a plan may be higher overall for a larger telecommunications provider (e.g., Bell, Telus, Rogers) than a smaller one (e.g., Execulink or Teksavvy) while, simultaneously, constituting a smaller portion of larger providers' quarterly revenue because they may already have requisite policy, security, and technical staff who can be (re)tasked to developing and maintaining such a policy.

Recommendation 21: Compensation Should Be Included for Smaller Organizations

There should be a mechanism whereby smaller telecommunications providers (e.g., those with fewer than 250,000 or 500,000 subscribers or customers) that have historically been conscientious in their security arrangements can seek at least some temporary relief if they are required to undertake new, modify existing, or cease ongoing business or organizational practices as a result of a government demand or order or regulation. Such relief may be for only a portion of the costs incurred and, thus, constitute a 'cost-minus' expense formula.

Second, in some situations, the costs of complying with an order may compromise certain aspects of a telecommunications provider's business. Consider a case where an order prohibits the use of Vendor A's products or services and where there is not an equivalent competitor that provides similar services at similar cost. If Vendor A's products or services are required to reach a subset of customers (e.g., Vendor A sells specialized equipment that enables rural wireless service), there is a prospect that affected customers will lose telecommunications service due to a lack of a comparable, existent replacement product or service. The same could be said for specialized equipment sold by vendors that, while possessing prospective or actual security vulnerabilities that might be exploited, are essential to providing current grades of service to individuals and organizations in Canada. There is nothing in the legislation, as presently drafted, that clearly takes these equities into consideration nor how severing certain business lines or customer service regions could have detrimental financial impacts on telecommunications providers, to say nothing of the individuals and organizations that could be affected by any security-related severance of services.

Recommendation 22: Proportionality and Equity Assessments Should Be Included in Orders or Regulations

There should be proportionality and equity assessments included in the development of any Order in Council, Ministerial Order, or regulation under the Act. The results of these assessments should be taken into consideration by the government prior to issuing an order or regulation, should be provided to telecommunications providers alongside associated orders or regulations, and should be included in any evidentiary packages that may be used should a telecommunications provider seek a judicial review of any given order or regulation.

Third, telecommunications service providers may be required to undertake a range of activities in order to enhance the security of their networks and services. At least some providers will likely be required to hire staff or retain consultants to fulfill the

requirements that are set down in government demands or orders or regulations. It is already challenging to find and retain staff with dedicated cybersecurity skills, and in the case of small businesses with narrow profit margins and few employees, they may be fiscally challenged in hiring the requisite staff. These difficulties may be magnified in the case of telecommunications providers that principally service rural or remote communities. In effect, it is unclear how easily telecommunications providers will be able to find talent that may be required to comply with government cybersecurity demands, orders, or regulations, let alone afford those professionals' salaries.

Relatedly, depending on how the government staffs its own teams that are responsible for assessing cybersecurity guidance, developing compliance requirements, and so forth, there is an open question of whether the federal government will also need to hire new staff to bring into force its telecommunications and critical infrastructure security programs. Assuming that the government will need to hire more professionals, this may create a situation where the private and public sector are competing for the same class(es) of cybersecurity professionals, making it even more challenging for either public agencies or federally regulated private organizations to secure the staff needed to develop and comply with security-related orders and regulations.

Recommendation 23: Government Should Encourage Cybersecurity Training

The government should commit to enhancing scholarships, grants, or other incentives to encourage individuals in Canada to pursue professional cybersecurity training. Such training could include targeted training that would alleviate hiring challenges that could result from requiring telecommunications providers and other critical infrastructure providers to adopt new proactive and reactive cybersecurity practices associated with cybersecurity-related Orders in Council, Ministerial Orders, or regulations. Such education and training efforts should be designed so as to foster a diverse and inclusive workforce.

2.6. Vague Drafting Language

As noted in previous parts of this report, the draft legislation does not delimit the specific kinds of security threats that might be addressed by Orders in Council, Ministerial Orders, or regulations. This is indicated by language such as “including” in s. 15.1(1), s. 15.2(1), and s. 15.2(2) that has the effect of describing some kinds of threats to the Canadian telecommunications system (i.e., interference, manipulation, or disruption) without enumerating all of the potential threats the legislation could address in the future.

Relatedly, other key terms or concepts such as given in the following list are not explained or defined in the legislation:

- Interference
- Manipulation
- Disruption

The legislation also provides the Minister of Industry with an undefined scope of power insofar as per s. 15.2(2) the "Minister may, by order, direct a telecommunications service provider **to do anything or refrain from doing anything**…".[41] The effect is that there are no particularly clear limits on what might be contained in an order, and thus enable the Minister to be as specific or vague as they desire in their orders, up to and including ordering a telecommunications provider to do, or refrain from doing, something that functionally may not be in the telecommunications providers' power to do or not do.

Finally, the bill does not clearly identify how personally identifiable information that is obtained from telecommunications providers is to be treated. This is evident when examining s. 15.5. Specifically, s. 15.5(1)(b) recognizes that some financial, commercial, scientific, or technical information is classified as confidential. Confidential information can, also include that which could reasonably be expected to (c)(i) result in material financial loss or gain to any person, (c)(ii) prejudice the competitive position of any person, or (c)(iii) affect contractual or other negotiations of any person if it were to be disclosed. It is possible personal information might sometimes, but not always, fall into these categorizations.

Analysis

In the absence of specific definitions, the government, telecommunications companies, and judges who review the application of the legislation may turn to past judicial decisions, dictionaries, other Canadian laws, case law, and decisions made in other jurisdictions to define key terms in the legislation. Nonetheless, each of the essential terms in the legislation can potentially cover an extraordinarily broad swath of activities. As just one example, a Ministerial Order could be issued that imposes a condition on a telecommunications provider's end-to-end encrypted voice telephony system. Specifically, the order might, under s. 15.2(2)(b), impose a condition on the provider to enable lawful access on all its voice services, such that when the provider is served with a valid warrant, it could disclose the contents of the communication in a plaintext/non-encrypted format to government agencies. This would not explicitly order the telecommunications provider to *not* make available an end-to-end encrypted telephony service but would nonetheless serve the same purpose.

Similarly, and as an example, a Ministerial Order could under the "among other things" clause in s. 15.2(2) require that telecommunications providers enter into cybersecurity

41 Emphasis not in original.

arrangements with the Canadian Centre for Cyber Security (CCCS) to better protect against network-based threats. In such a situation, the providers might contact the CCCS/Communications Security Establishment (CSE) and enter into an agreement under s. 27(2) of the *CSE Act* with the effect of enabling the CSE to:

> in the furtherance of the cybersecurity and information assurance aspect of its mandate, access an information infrastructure designated under subsection 21(1) as an information infrastructure of importance to the Government of Canada and acquire any information originating from, directed to, stored on or being transmitted on or through that infrastructure for the purpose of helping to protect it, in the circumstances described in paragraph 184(2)(e) of the *Criminal Code*, from mischief, unauthorized use or disruption.

Significantly, under the *CSE Act*, it is clearer what kinds of threats are to be addressed—mischief, unauthorized use, or disruption per the Criminal Code—whereas the same definitions are not provided under Bill C-26's reforms to the *Telecommunications Act*. Indeed, the government has not explained why under the *CSE Act*'s cybersecurity authorizations are restricted to mischief, unauthorized use, or disruption whereas, in contrast, the proposed *Telecommunications Act* reforms use the language, "including against the threat of interference, manipulation or disruption." The language contained in Bill C-26 is arguably much expansive than that in the *CSE Act*.

Recommendation 24: Clarity Should Exist Across Legislation

The government should clarify how the envisioned threats under the draft legislation ("including against the threat of interference, manipulation or disruption.") compares to the specific acts denoted in s. 27(2) of the *CSE Act* ("mischief, unauthorized use or disruption"), with the goal of explaining whether the *Telecommunications Act* reforms would expand, contract, or address the same classes of acts as considered in the *CSE Act*.

Where the intent is to mirror the actions denoted in s. 27(2), similar language should be adopted, and if the goal is to intentionally diverge from that language, the government should clarify how and why it is doing so to foster public debate over the divergence.

Recommendation 25: Explicit Definitions Should Be Included In the Legislation or Else Publicly Promulgated

The legislation should be amended to provide either explicit definitions for "interference," "manipulation," and "disruption," or make clear that the definitions are found in specific other Acts, or it should require the government to publicly promulgate these definitions and any updates that are subsequently made to the definitions outside of the legislation.

While the example of compelling telecommunications providers to enter into agreements with the CSE is, perhaps, a bit of a stretch, it nonetheless serves the purpose of demonstrating what "among other things" could potentially entail under the draft legislation. While flexibility is almost certainly needed to ensure that the government can respond to emerging threats, it has not, at this time, made clear why the existing listing of possible activities under s. 15.2(2)(a)-(l) are insufficient. Should the government believe that some built-in flexibility is required, it might adopt an amendment that would enable it to compel companies to take actions in response to an emergency condition, and thereafter, have the emergency order reviewed for necessity, reasonableness, and proportionality by the Federal Court, with an associated obligation for the court's review to be published.

Recommendation 26: Ministerial Flexibility Should Be Delimited

The legislation should be amended to delimit the Minister's specific capabilities and powers under the legislation.

Original Text	Proposed Amendment
15.2(2) The Minister may, by order, direct a telecommunications service provider to do anything or refrain from doing anything — other than a thing specified in subsection (1) or 15.1(1) — that is specified in the order and that is, in the Minister's opinion, necessary to secure the Canadian telecommunications system, including against the threat of interference, manipulation or disruption. In the order, the Minister may, among other things,	15.2(2) The Minister may, by order, direct a telecommunications service provider to do anything or refrain from doing anything — other than a thing specified in subsection (1) or 15.1(1) — that is specified in the order and that is, in the Minister's opinion, necessary to secure the Canadian telecommunications system, including against the threat of interference, manipulation or disruption. In the order, the Minister may, ~~among other things,~~

Recommendation 27: Emergency Situations

The legislation could be amended such that, if recommendation 26 is adopted, the Minister would retain a degree of flexibility while ensuring that novel kinds of orders will be subject to judicial review that is conducted by the Federal Court. Such reviews should be assessed for necessity, reasonableness, and proportionality, and the decisions emergent from the reviews should be published by the Federal Court.

Finally, the legislation should be amended to, at a minimum, make explicit that personal information and de-identified information should be treated as confidential. Furthermore, amendments should establish that prior judicial approval is required before the government can compel telecommunications providers to disclose such information. Under the present draft of the legislation, there are likely some cases where personal information would be confidential, such as if its disclosure by a telecommunications provider would materially affect an individual's finances, competitive positions, contracts, or negotiations. However, these categories likely encompass a vanishingly small number of situations with the effect that, in most cases, personal information and de-identified information would not fit under these categories.

Alternatively, telecommunications providers themselves might designate their subscribers' personal information or de-identified information as constituting financial, commercial, scientific, or technical information though, again, the information itself may not always clearly align with these categories. As such, the government should make explicit that personal and de-identified information that is obtained from telecommunications providers constitutes confidential information and that the government must seek prior approval from the Federal Court in cases where they are attempting to compel such information from providers for the purposes of making, amending, or revoking an order under s. 15.1 or 15.2 or a regulation under paragraph 15.8(1)(a), or of verifying compliance or preventing non- compliance with such an order or regulation. The government should be precluded from disclosing personal or de-identified personal information to foreign governments or organizations.

Recommendation 28: Personal Information Is Confidential Information

The legislation should be amended to make clear that all personal information and de-identified information that is disclosed by telecommunications providers is classified as confidential information.

Original Text	Proposed Amendment
Confidential information — designation 15.5 (1) A person who provides any of the following information under section 15.4 may designate it as confidential:	Confidential information — designation 15.5 (1) A person who provides any of the following information under section 15.4 may designate it as confidential: … (d) information which is personal or de-identified.

Recommendation 29: Prior Judicial Approval to Obtain Personal or De-Identified Information

The 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 a relevant judicial order from the Federal Court, where the information is to be used exclusively for the purposes of making, amending, or revoking an order under s. 15.1 or 15.2 or a regulation under paragraph 15.8(1)(a), or of verifying compliance or preventing noncompliance with such an order or regulation.

Recommendation 30: No Disclosure of Personal or De-Identified Information to Foreign Organizations

The legislation should be amended to clarify that the government cannot disclose personal or de-identified personal information that it has compelled from telecommunications providers to foreign governments or organizations.

3. Counterbalances to Security

As drafted, Bill C-26 would have the effect of providing the government with insufficiently bounded powers that could compel telecommunications providers to do anything, and within a thick veil of secrecy surrounding what is ordered and how providers respond. Information that the government compels from telecommunications providers might be widely circulated, and some of that information could include identifiable or de-identified personal information. Further, the costs associated with compliance with government orders may materially affect telecommunications providers, up to and including the risk that some companies may be unable to continue providing service to all of their customers.

Perhaps most notably, the proposed *Telecommunications Act* reforms lack any reference to independent bodies that could assist the government in assessing the necessity, proportionality, or reasonableness of an Order in Council, Ministerial Order, or regulation. The government could remedy this by making clear what roles the Office of the Privacy Commissioner of Canada, National Security and Intelligence Committee of Parliamentarians, or National Security and Intelligence Review Agency would have at different stages of the order- or regulation-making process. Similarly, while telecommunications providers can seek judicial review of orders or regulations they must comply with, the individuals or communities that may be affected by these orders have no recourse. What is an individual or community to do, as an example, if a government order has the effect of terminating services that those individuals or communities rely on? And, in the case where an order or regulation overrides some element of a CRTC decision, how will telecommunications providers or members of the public that participate in CRTC decision-making processes know and consider the effects of such orders or regulations when they take part in telecommunications regulatory processes?

In addition to not indicating what individuals or communities might do if a government order has deleterious effects on them, the government has declined to publish a *Charter* statement to accompany the legislation.[42] The result is that the legislation is manifestly focused on security to the exclusion of any other interests, and at no point does the legislation reforming the *Telecommunications Act* address how privacy or equity interests should be safeguarded. While it is important that Canada's federally regulated critical infrastructure, including telecommunications networks, is secure from adversarial meddling, such efforts must be balanced against competing democratic norms of making the government accountable for its activities and legible to the public.

---

42 See: Department of Justice Canada. (2022). "Charter Statements," *Government of Canada*. Available at: https://www.justice.gc.ca/eng/csj-sjc/pl/charter-charte/index.html.

In assessing how to amend Bill C-26, parliamentarians and the Government of Canada should reflect on the role that privacy and other rights-based interests should play in the course of developing or issuing a demand, order, or regulation that could affect how individuals or communities make use of telecommunications systems. While it is possible that existing government policy could require that privacy-oriented or gender-based analyses be integrated into any orders or regulations, along with other equity-based assessments, the legislation as presently drafted does not require that such assessments be made. Many in government might complain that such assessments would have the effect of restricting Canada's ability to respond to cybersecurity threats. However, failing to undertake these assessments may cause the government—and those motivated to defend Canadian interests—to take actions that negatively affect the residents who inhabit Canada. The outcome is that Canada's telecommunications networks might be secured at the cost of disproportionately affecting the very individuals and communities that are most reliant on those networks.

Put differently, cybersecurity efforts should first focus on how actions will enable the flourishing of individuals and communities residing in Canada, as opposed to isolating attention toward the secure operation of critical infrastructure systems. The risk that actions could have unintended and detrimental consequences, such as on historically disenfranchised individuals and communities, is magnified by the current lack of proportionality requirements in the draft legislation. Conjoining necessity and proportionality requirements could have the effect of conditioning orders or regulations that might otherwise have inequitable consequences on residents of Canada.

Bill C-26, as currently drafted, threatens to further impair trust between the government and non-government cybersecurity experts, to say nothing of weakening trust between government and the public. This latter element is particularly important as the existence of legislation that could significantly modify the business and technical attributes of Canadian telecommunications networks might be used by irresponsible actors to further inflame fears that the federal government is using its vast powers to the detriment of Canadian residents' *Charter* rights. Building appropriate safeguards into C-26 may help to ameliorate at least some of these concerns while, simultaneously, demonstrating the government's commitment to protecting *Charter* rights and developing legislation that accords with democratic values and the norms of transparency and accountability.

4. Conclusion

"Bill C-26: An Act respecting cyber security, amending the *Telecommunications Act* and making consequential amendments to other Acts" is intended to provide the Canadian government with powers to force telecommunications providers to do or refrain from doing specific acts in order to secure the Canadian telecommunications system from threats, such as those associated with interference, manipulation, or disruption. The legislation echoes the legislation and executive actions of some of Canada's allies and friends. But, to date, the government has not clearly explained why it needs this legislation in the first place. To what extent do Canada's telecommunications providers (and other critical infrastructure providers) currently meet the cybersecurity expectations of the government of Canada and to what extent are those expectations appropriate or reasonable? Is Bill C-26 meant to address existing or historical challenges or, instead, is it forward-looking and meant to deal with forecast threats? Or is it meant to do both? The government owes it to residents of Canada and Canadian business alike to justify why it is seeking new powers and to explain the underlying rationales driving the introduction of this cybersecurity legislation.

Citizen Lab work has previously argued that the government should have the ability to compel private organizations to adopt standards in order to best secure critical infrastructure. Similarly, the government should be able to discipline, deter, and impose costs on actors that operate in a way that endangers individuals and communities in Canada or that risk compromising the telecommunications systems that are the backbone of the information economy. And, where telecommunications companies are resistant to explaining how they are securing systems, it makes sense for the government to be able to compel that information.

But the powers being sought by the government are insufficiently bounded, are accompanied by overly broad secrecy clauses, and would potentially impair the ability of private companies to dispute demands, orders, or regulations that are issued by the government. Similarly, there is a real risk that the CRTC could draft one set of public law through its decisions while a kind of secret law, promulgated through orders and regulations, actually guides telecommunications providers' cybersecurity behaviours. The government's proposed powers in Bill C-26, then, need to be pared back in some places, essential clauses and terminology need to be defined, and accountability and transparency requirements must be sprinkled liberally in an amended version of the legislation.

If the government declines to meaningfully amend its legislation and make itself both more accountable and transparent to telecommunications providers and the public alike, it will have passed a bad law. Authoritarian governments would be able to point to a non-amended Bill C-26 in the course of justifying their own unaccountable, secretive,

and repressive security legislation. While the current form of Bill C-26 might be successful in combating threats to Canada's telecommunications systems, it will simultaneously undermine the legitimacy of law by preventing individuals in Canada from truly understanding what the law means or how and when it is used.

Some in government may believe that it is imperative to maintain the secrecy of how telecommunications companies are compelled to secure their systems and networks on the basis that such secrecy would be good for cybersecurity. These individuals and groups must adopt a broader view and consider how the secrecy currently laced through Bill C-26 fails to cohere with a healthy democratic system. This report has shown how the government might amend Bill C-26 to better secure Canada’s telecommunications system while, simultaneously, infusing the legislation with accountability and transparency provisions. Security can be and must be aligned with Canada’s democratic principles. It is now up to the government to amend its legislation in accordance with them.