UNIVERSITY OF TORONTO

munk school
OF GLOBAL AFFAIRS & PUBLIC POLICY

# Submission to the Standing Committee on Public Safety and National Security: Study of Bill C-26, *An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts*

Submission by
Kate Robertson and Lina Li
Citizen Lab, Munk School of Global Affairs & Public Policy
University of Toronto

# Part 1. Introduction and Summary

1. Citizen Lab researchers routinely produce reports concerning technical analyses of information and communications technologies (ICTs), the human rights and policy implications surrounding government surveillance that occurs using ICTs, as well as the cybersecurity threats and digital espionage targeting civil society. Citizen Lab research has also examined the openness and transparency of government and organizations, including telecommunications providers, with respect to the collection, use, or disclosure of personal information and other activities that can infringe upon human rights.

2. This month, the Citizen Lab published *Finding You: The Network Effect of Telecommunications Vulnerabilities for Location Disclosure* ("*Finding You*"), authored by Gary Miller and Christopher Parsons.[1] The report provides a high-level overview of geolocation-related threats sourced from 3G, 4G, and 5G network operators. Evidence of the proliferation of these threats shows how the signalling protocols used by telecommunications providers to facilitate roaming also allow networks to retrieve extraordinarily detailed information about users. These protocols are being constantly targeted and exploited by surveillance actors, "with the effect of exposing our phones to numerous methods of location disclosure."[2] Risks and secrecy surrounding mobile geolocation surveillance are heightened by layers of commercial agreements and sub-agreements between network operators, network intermediaries, and third-party service providers. Ultimately, vulnerabilities in the signalling protocols have "enabled the development of commercial surveillance products that provide their operators with anonymity, multiple access points and attack vectors, a ubiquitous and globally-accessible network with an unlimited list of targets, and virtually no financial or legal risks."[3]

3. *Finding You* highlights the importance of developing a cybersecurity strategy that mandates the adoption of network-wide security standards, including a requirement that network operators adopt the full array of security features that are available in 5G standards and equipment. The report's findings also underscore the importance of public transparency and accountability in the regulation of telecommunications providers. As the authors note, "[d]ecades of poor accountability and transparency have contributed to the current environment where extensive geolocation surveillance attacks are not reported."[4]

4. In short, it is long overdue for regulators to step in at national and international levels to secure our network services. However, Canada's approach to the regulation of telecommunications and cybersecurity also needs to be transparent, accountable, and compliant with applicable human rights standards. One year ago, Citizen Lab published *Cybersecurity Will Not Thrive in Darkness: A Critical*

---

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

[2] *Finding You*, at p. 1.

[3] *Finding You*, at p. 2.

[4] *Finding You*, at p. 32.

*Analysis of Proposed Amendments in Bill C-26 to the Telecommunications Act* ("*Cybersecurity Will Not Thrive in Darkness*").[5] The report was authored by Dr. Christopher Parsons.[6] Dr. Parsons critically examined the proposed draft legislation under Bill C-26, including identified deficiencies. In doing so, Dr. Parsons provided necessary historical and international context surrounding the federal government's proposed telecommunications sector reform. Canada is not the first of its allies to introduce new government powers as a result of heightened concern and awareness surrounding real and pressing risks to critical infrastructure. However, Dr. Parsons identified that although the draft legislation may advance important goals, its current iteration contained thematic deficiencies that risked undermining its effectiveness. This report is set out in **Appendix B**, and is the focus of this brief.

5. The main submissions in this brief are set out in two parts:

   a. **Part 2: Bill C-26 and the *Canadian Charter of Rights and Freedoms* ("*Charter*")**: Part 2 of this Brief discusses the nexus between Bill C-26 and the *Charter*. It focuses, in particular, on how Bill C-26 may impact equality rights (Section 15), freedom of expression (Section 2(b)), and privacy (Section 8). The *Charter* implications of the proposed legislation should be a central consideration for this Committee, and throughout the Parliamentary process ahead.

   b. **Part 3: Recommendations for amendment to Bill C-26**: *Cybersecurity Will Not Thrive in Darkness* provides substantive analysis and recommendations to address a series of thematic deficiencies identified in Bill C-26. We agree that these recommendations are appropriate in the spirit of addressing overarching deficiencies, including secrecy and transparency issues, and the need to incorporate guardrails for the new government powers that the Bill creates. As a result, Part 3 provides a summary of Dr. Parsons' recommendation, as well as comments and supplementary recommendations flowing from the *Charter* analysis in Part 2.

# Part 2. Bill C-26 and the *Charter*: Towards a Human Security Approach to Cybersecurity

6. In analyzing the proposed amendments to Canada's *Telecommunications Act* in Bill C-26, Dr. Parsons identified the following thematic deficiencies in the proposed legislation:

   - The breadth of what the government might order a telecommunication provider to do is not sufficiently bounded.
   - Excessive secrecy and confidentiality provisions in the bill threaten to establish a class of secret law and regulation.

[5] Christopher Parsons, "Cybersecurity Will Not Thrive in Darkness: A Critical Analysis of Proposed Amendments in Bill C-26 to the Telecommunications Act," Citizen Lab Research Report No. 158, University of Toronto, Oct. 2022.

[6] This report was also published at the time that Dr. Parsons was a senior researcher at the Citizen Lab. As such, the report's conclusions and recommendations also do not necessarily reflect those of Dr. Parsons' current employer.

- 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 contour of the legislation cannot be assessed.
- There is no recognition of privacy or other *Charter*-protected rights in Bill C-26 as a counterbalance to the proposed security requirements, nor are appropriate accountability or transparency requirements imposed on the government.[7]

7. These thematic deficiencies relate to the effectiveness of the government's cybersecurity strategy as well as to potential risks to *Charter*-protected rights. Like the Canadian Radio-television and Telecommunications Commission ("CRTC"), the federal government must act in a manner that is consistent with the *Charter* when regulating in respect of telecommunication services and cybersecurity.

8. Following the publication of Dr. Parsons' report in October 2022 (including his recommendation that the federal government table a *Charter* statement in relation to Bill C-26), the federal government tabled its *Charter* Statement in the House of Commons on December 14, 2022. The "non-exhaustive" statement identifies areas where *Charter*-protected rights are engaged by Bill C-26. The statement, however, does not fully address relevant *Charter*-related issues linked to Bill C-26. In the following paragraphs (9-27) we raise additional *Charter* issues to, first, inform the appropriateness of amendments recommended by Dr. Parsons and, second, to underscore the importance of bringing a human rights and human security approach to cybersecurity and the regulation of telecommunications services.

**Equality Rights and Section 15 of the *Charter***

9. This section identifies examples of equality-related issues that could foreseeably arise during the government's implementation of Bill C-26. We raise the potential for adverse impacts in the implementation of orders and regulations under Bill C-26 in order to provide guidance to this Committee about the importance of ensuring that the transparency and accountability mechanisms surrounding Bill C-26 are fit-for-purpose to guard against foreseeable risks. As noted in paragraph 6, accountability and transparency gaps are a thematic deficiency in Bill C-26, which are the subject of recommendations throughout Part 3 of this brief.

10. In 2019, the federal government passed the *Accessible Canada Act* (S.C. 2019, c. 10). The *Act* recognizes the importance of the economic, social and civic participation of all persons in Canada, and to allow all individuals to fully exercise their rights and responsibilities in a barrier-free Canada. The *Act* notes equality and non-discrimination rights protected under the *Canadian Charter of Rights and Freedoms*, and the *Canadian Human Rights Act*, which are implicated by laws and public policies affecting the accessibility of telecommunications services.

[7] *Cybersecurity Will Not Thrive in Darkness*, *supra* at p. 4.

11. Access to affordable, high-quality telecommunications services is unevenly available in Canada.[8] Government measures that have the effect of exacerbating the "digital divide" for *Charter*-protected groups may result in discrimination under section 15 of the *Charter*. If Orders in Council, Ministerial orders, or regulations issued under Bill C-26 are implemented in a manner such that disadvantaged communities are disproportionately exposed to security vulnerabilities, or disproportionately unable to access network services, it perpetuates the disadvantage experienced by *Charter*-protected groups, thus engaging section 15 of the *Charter*.

12. The following are examples of equality-related issues that are foreseeable when considering the types of orders or regulations that may be imposed under the broad powers proposed in Bill C-26:

    a. Firstly, barriers to affordable telecommunications services place a particularly heavy toll on low-income communities in Canada. There is a close connection between poverty and the historical disadvantage that is experienced by groups protected by s. 15 of the *Charter*.[9] As a result, government orders or regulations that impose material costs on telecommunications services may result in heightened barriers to access, which would disproportionately affect historically disadvantaged communities.

    b. Secondly, government orders or regulations that hinder efforts to redress regional disparities in access to telecommunications services in Canada, such as disparities between Indigenous communities and the rest of Canada when it comes to accessing high-speed internet services,[10] can also disproportionately affect *Charter*-protected groups under s. 15.

    c. Thirdly, persons living with disabilities may also be impacted in unintended but foreseeable ways by orders and regulations issued under Bill C-26. For example, measures that slow the availability of secure network services may slow or impede secure access to assistive technologies enabled by connected homes or communities.[11] As another example, orders or regulations that mandate the deployment of certain cybersecurity measures could bind companies to cybersecurity tools that are not accessible. While physical environments are more

---

[8] Office of the Auditor General of Canada, *Connectivity in Rural and Remote Areas*, Report 2 of the Auditor General of Canada's Reports to the Parliament of *Canada*, 2023, <https://www.oag-bvg.gc.ca/internet/English/parl_oag_202303_02_e_44205.html>.

[9] Government of Canada, "Towards a Poverty Reduction Strategy: A backgrounder on poverty in Canada" October 2016; Government of Canada, National Council of Welfare Reports: "Poverty Profile: Special Edition" (2012) ("In two of Canada's largest cities, more than half of all persons living in poverty were from racialized groups: 58% in Vancouver; and 62% in Toronto").

[10] Office of the Auditor General of Canada, *Connectivity in Rural and Remote Areas*, Report 2 of the Auditor General of Canada's Reports to the Parliament of *Canada*, 2023, <https://www.oag-bvg.gc.ca/internet/English/parl_oag_202303_02_e_44205.html>.

[11] For example, H. Nam Kim, "Digital Privacy of Assistive Technology Users with Visual Disabilities" (2022) Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 66(1), 1105-1109; Karen Renaud and Lizzie Coles-Kemp, "Accessible and Inclusive Cyber Security: A Nuanced and Complex Challenge", SN Computer Science (2022) 3: 346; World Health Organization, "Assistive technology", May 15, 2023, <https://www.who.int/news-room/fact-sheets/detail/assistive-technology>.

traditionally integrated into accessibility and inclusivity frameworks, cybersecurity tools often assume "that users are fully abled (e.g. can see the CAPTCHA), cognitively unimpaired (e.g. can create and retain passwords), have the necessary resources (e.g. time, appropriate technology and internet access in a distraction-free environment), and have the required dexterity to interact with the security system (e.g. can use the mouse and keyboard with ease)."[12]

d. Fourthly, network insecurity and privacy risks also expose certain groups to heightened threats. Civil society, including dissidents, journalists, opposition politicians, lawyers, and family members are routinely exposed to targeted threats, hacks, and digital espionage.[13] If governments and regulators fail to address persistent vulnerabilities in our network services–including the widespread abuse of telecommunications networks described in *Finding You*–certain groups (including communities protected by section 15) may be disproportionately left in harm's way. As an alternative hypothetical, cybersecurity measures mandated through orders or regulations could lead to the unintended creation of new or worsening security flaws. Dr. Parsons provides the example that "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."[14]

13. Ultimately, these tensions highlight the overarching importance of inclusivity in setting security standards, and the corresponding importance of regulating telecommunications in a transparent and accountable way that enables the government's cybersecurity approach to be fully integrated into a healthy democratic system. Without public transparency, accountability, and proportionate limits, the government runs the risk 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."[15]

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

14. The current draft of Bill C-26's excessive secrecy and confidentiality provisions jeopardizes the right to freedom of expression under section 2(b) of the *Charter*. The government's *Charter* statement focuses on the speech of the commercial entities who will be directly regulated under Bill C-26. The *Charter* statement posits that because restrictions on commercial speech do not tend to implicate the core

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

[13] For example, the authors of *Finding You* observed a likely instance of state-sponsored surveillance involving numerous requests sent from networks in Saudi Arabia to geolocate the phones of Saudi users travelling in the United States, with the effect "of revealing the mobility patterns of residents of Saudi Arabia in the United States" (Finding You, at p. 16-19). See also, Bill Marczak, John Scott-Railton, Siddharth Prakash Rao, Siena Anstis, and Ron Deibert, "Running in Circles: Uncovering the Clients of Cyberespionage Firm Circles," Citizen Lab Research Report No. 133, University of Toronto, December 2020; and see generally, Citizen Lab, "Targeted Threats Archives", <https://citizenlab.ca/tag/targeted-threats/>.

[14] *Cybersecurity Will Not Thrive in Darkness*, *supra* at p. 14.

[15] *Cybersecurity Will Not Thrive in Darkness*, *supra* at p. 40.

values of section 2(b), restrictions can be more easily justified.[16] However, this analysis fails to account for how individuals' *Charter* rights may be impeded under the current drafting of the legislation. The excessive secrecy and confidentiality provisions in the bill also restrict the public's and media's expressive freedom in Canada.

15. The principles of open courts and open government are derivative components of section 2(b) of the *Charter* (the freedom of expression). The open court principle requires that court proceedings, including judicial reviews in federal court, presumptively be open and accessible to the public and to the media. Access to information about government actions can also arise as a derivative right to section 2(b), if a denial of access to government information effectively precludes meaningful public discussion on a matter of public interest. Where restrictions on access substantially impede meaningful discussion and criticism about matters of public interest, the government must reasonably justify its infringement of the freedom of expression.[17]

16. Telecommunications and cybersecurity law and policy is undoubtedly a matter of public interest. There is a close nexus between human rights and public policy concerning the regulation of telecommunication services. Canada's telecommunications policy is intimately linked with the "social and economic fabric" of Canada and its regions.[18] Equitable access to telecommunication services is sometimes described as a mechanism for "digital self-determination", which speaks to the need to protect the potential for human flourishing in the digital era.[19]

17. The recent Citizen Lab report, *Finding You*, highlights several ways in which excessive secrecy surrounding telecommunications oversight has itself endangered the public. The authors note historical deficiencies in oversight and accountability of network security, which have led to geolocation-related threats associated with contemporary networks. Excessive secrecy has contributed to the persistence of the "low-hanging geolocation threat" identified in *Finding You*:

> Decades of poor accountability and transparency have contributed to the current environment where extensive geolocation surveillance attacks are not reported. This status quo has effectively created a thriving geolocation surveillance market while also ensuring that some telecommunications providers have benefitted from turning a blind eye to the availability of their network interconnections to the surveillance industry.[20]

---

[16] Department of Justice Canada, "*Charter* Statement: Bill C-26: An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts", December 14, 2022.

[17] *Ontario (Public Safety and Security) v. Criminal Lawyers' Association*, 2010 SCC 23; *ARPA Canada and Patricia Maloney v R.*, 2017 ONSC 3285. This inquiry involves a balancing of any countervailing considerations (such as a privilege) that might militate against disclosure.

[18] *Telecommunications Act*, S.C. 1993, c. 38, at s. 7(a).

[19] See Nydia Remolina and Mark James Findlay, "The Paths to Digital Self-Determination - A Foundational Theoretical Framework", (April 22, 2021) SMU Centre for AI & Data Governance Research Paper No. 03/2021.

[20] *Finding You*, *supra* at p. 32.

18. The geolocation surveillance threats discussed in *Finding You* disproportionately jeopardize human rights defenders and other individuals who face heightened risks of targeted security threats (e.g., corporate executives, military personnel, politicians and their staff, senior bureaucrats, etc). Industry has historically charged large amounts of money to receive information about well-known industry threats, with the effect of impeding non-industry groups such as security researchers and civil society from obtaining and disseminating information about the nature of the threats faced by at-risk individuals, or from advocating for the remedies that would benefit the security and privacy of civil society. The authors note that, in many instances, individuals cannot determine whether their own telecommunication provider has "deployed and configured security firewalls to ensure that signaling messages associated with geolocation attacks, identity attacks, or other malicious activity are not directed towards their phones."[21]

19. Citizen Lab's research highlights the substantial public interest in enabling the media, security researchers, civil society, and the public (including individuals facing heightened security risks) to access information about telecommunications policies and regulations, and the nature of the security risks that persist in whole or in part. As security researchers have noted, "the most promising route to full accessibility [in cybersecurity] lies in collaboration between vendors, advocacy groups, and the government."[22] This collaboration is facilitated by "discourse involving cyber security professionals, human-centred security academics, disability charities and other stakeholders."[23] Civil society and the broader business community can press "regulators, policy makers, and politicians to actively compel telecommunications providers to adopt appropriate security postures to mitigate the pernicious and silent threats associated with geolocation surveillance,"[24] and other similar security risks.

**Privacy Impacts and Section 8 of the *Charter***

20. Bill C-26 proposes several new information collection and sharing powers, and may include the collection or sharing of personal information. Many of these powers are insufficiently bounded or defined. The potential privacy risks posed by the powers are heightened by the absence of key accountability and oversight mechanisms. The breadth of the unsupervised information collection and sharing powers heightens the risk that the legislation, if passed as drafted, could unreasonably interfere with section 8 of the *Charter* in at least three four ways.

21. First, the federal government's *Charter* statement posits that Bill C-26 does not interfere with section 8, in part, as a result of the fact that the "the information being gathered and shared in this context relates to the technical operations of TSPs, which are commercial entities", as opposed to "personal

[21] *Finding You*, *supra* at p. 32.

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

[23] *Ibid*.

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

biographical information that attracts a heightened privacy interest".[25] However, Bill C-26 does not explicitly draw this distinction between technical information or other forms of personal information when defining collection or information sharing powers in the bill.

22. Instead, Bill C-26 provides authority to compel a broad array of information-holders to disclose a broad array of information. While the *Charter* statement for Bill C-26 emphasizes the regulatory nature of the scheme in Bill C-26, unlike other statutory inspection powers that have been subject to *Charter* challenges historically, there is no reason to interpret the statutory powers in Bill C-26 as applying only to information in which there is a low expectation of privacy. Rather, section 15.4 would provide authority to compel "any person" to provide "any information" under "any conditions that the Minister may specify," so long as the Minister believes it is relevant to its order making powers. The persons and entities subject to this provision in many circumstances play an integral role in the lives of people in Canada, and may well be information-holders in respect of highly sensitive or personal information.

23. Second, while some aspects of Bill C-26 are regulatory in nature, Bill C-26 also creates criminal offences punishable by imprisonment for non-compliance with specified orders or regulations. Statutory powers authorize collecting and sharing information for the purposes of "verifying compliance or preventing non-compliance" with those orders or regulations. The legislation therefore creates risks that information will be compelled or shared during investigations pertaining to the criminal offences created by Bill C-26, or other offences. Furthermore, the breadth of the order making powers under Bill C-26 mean that the collection of information for the purposes of making such *orders* may cause serious consequences that are separate and apart from any regulatory or criminal prosecution.

24. Third, section 8 also protects privacy by requiring adequate accountability and review mechanisms to accompany information collection powers, even in administrative or regulatory contexts. The Supreme Court states that "[w]hile less exacting review may be sufficient in a regulatory context, *the availability and adequacy of review is nonetheless relevant to reasonableness under s. 8*."[26] Canadian constitutional law has long recognized that without clearly defined safeguards (often including prior judicial oversight), legislation that authorizes intrusions on reasonably held expectations of privacy is inconsistent with s. 8 of the *Charter*. In some circumstances involving searches that are not subject to warrant requirements, the Court still expects that additional safeguards will be established to ensure the requisite level of transparency and accountability, and to help ensure that such powers are not abused. For example, requiring notice to the persons whose information is affected allows the affected individuals to identify and challenge invasions of their privacy, as well as seek a meaningful remedy.[27] Appellate courts have recognized a range of accountability measures when assessing the reasonableness of search and seizure powers, such as: notice requirements (including after-the-fact notice); reporting obligations (to independent institutions or Parliament); the availability of clear mechanisms for review of the exercise

---

[25] Department of Justice Canada, "*Charter* Statement: Bill C-26: An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts", December 14, 2022.

[26] *Goodwin v. British Columbia (Superintendent of Motor Vehicles)*, 2015 SCC 46 at para 71.

[27] See *R. v. Tse*, 2012 SCC 16 at paras. 83-85; *Wakeling v. United States of America*, 2014 SCC 72 at para. 70; *T.L. v. British Columbia (Attorney General)*, 2023 BCCA 167 at paras. 171-173 and 237.

of collection powers; clear rules limiting collection powers to what is necessary, reasonable, and proportionate; and record-keeping requirements.[28]

25. Part 3 of this brief will identify several mechanisms that are necessary to improve accountability surrounding the proposed powers in Bill C-26. For example, the draft legislation proposes broad information sharing powers with no notice requirements. This would mean that individuals and organizations whose information has been collected would have no way of knowing of the fact that information has been shared, thus thwarting review and challenge. Individuals who have private information held by, and collected from, third-party organizations would also not be aware that their information has been collected in the first place, let alone shared with other government entities.

26. Fourth, the extensive confidentiality provisions in Bill C-26 may actually further undermine accountability mechanisms surrounding the bill's proposed information collection powers in ways that would be difficult to reasonably justify under s. 8. Section 15.4 of the proposed *Telecommunications Act* authorizes the Minister to require "any person" to provide "any information" under "<u>any conditions</u> that the Minister may specify." These conditions would foreseeably include conditions to extend confidentiality obligations to the Minister's use of collection powers. The secrecy provisions in Bill C-26, and the authority to extend those secrecy obligations through further "conditions", could effectively chill or silence individuals or entities from notifying other persons that their personal information has been collected, or from challenging the exercise of government power. Furthermore, excessive secrecy surrounding existing orders or regulations would further undermine accountability, as courts or oversight bodies wouldn't be able to assess whether collection or sharing of information was reasonably necessary and proportionate in furtherance of those secret orders or regulations. In short, it is unclear how the proposed confidentiality and secrecy provisions align with the need for accountability measures to ensure there is not an inappropriate intrusion into s. 8 *Charter* rights.

27. The *Charter* statement notes various information sharing agreements that are contained in the legislation. However, there are broad information sharing powers in Bill C-26 that are not subject to any information sharing agreements, or limitations on how the information may be used once shared. Furthermore, the majority of the Supreme Court has previously noted (in the context of other information disclosure powers accompanying supervised warrant provisions in the *Criminal Code*), that information sharing agreements are not "a panacea", given that there is "*always* a risk that a foreign law enforcement agency may misuse the information disclosed."[29]

---

[28] *R. v. Tse*, 2012 SCC 16; *Wakeling v. United States of America*, 2014 SCC 72; *Goodwin v. British Columbia (Superintendent of Motor Vehicles)*, 2015 SCC 46; *T.L. v. British Columbia (Attorney General)*, 2023 BCCA 167 at paras. 213-273.

[29] *Wakeling v. United States of America*, 2014 SCC 72 at para 75.

# Part 3. Towards More Secure, Transparent, Accountable Governments and Telecommunications Networks in Bill C-26

28. This Part 3 summarizes recommendations identified in *Cybersecurity Will Not Thrive in Darkness*, as well as supplementary comments and recommendations flowing from the *Charter* analysis set out in Part 2. The report, including its specific textual recommendations, is enclosed as **Appendix B**. Where recommendations are identified in this brief for the first time, they are numbered with letters (i.e., Recommendation 1A) to maintain the original numbering of the report.

## I. Limiting powers to order modifications to organizations' technical or business activities

29. To include appropriate safeguards surrounding compulsion powers under Bill C-26, *Cybersecurity Will Not Thrive in Darkness* makes the following recommendations:

    a. **Recommendation 1: Orders in Council and Ministerial Orders Must be Necessary, Proportionate, and Reasonable**. Currently, the legislation allows the government to issue an order when necessary to secure the Canadian telecommunications system. However, necessity is an insufficient curb on the government's power; Bill C-26 should impose more conditions regarding the specific circumstances under which the government can exercise its power.

    b. **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.

    c. **Recommendation 3: Government Should Undertake Impact Assessments Prior to Issuing Orders.** Government assessments of its orders should identify 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.

    d. **Recommendation 4: Forbearance or Cost/Cost-Minus Clauses Should Be Inserted**. The government may issue a direction that could severely alter how a telecommunications provider is able to offer a service to customers. 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.

e. **Recommendation 5: The Standards That Can Be Imposed Must Be Defined**. Without a clear definition of what a "standard" in the draft legislation entails, it becomes difficult to assess what kinds of standards the government is seeking to implement and whether it is adopting them safely. The legislation should be amended such that it is clear what kinds of standards are within and outside of the scope of the legislation. The evidence and analysis in *Finding You* underscore that urgent action is needed to establish mandatory security and privacy standards for telecommunications providers to require security postures that address the vulnerabilities in signalling protocols that enable mobile geolocation surveillance threats.

It should also 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.

## II. Secrecy and Absence of Transparency or Accountability Provisions

30. As noted above, Bill C-26 has "extensive and overly onerous secrecy and confidentiality requirements."[30] Laws that impose meaningful limits on the freedom of expression must be balanced and reasonably justified. While some confidentiality will be appropriate to ensure that unresolved security vulnerabilities are effectively brought into control, certain powers in Bill C-26 go further than what is required to accomplish cybersecurity and national security objectives. Furthermore, certain powers proposed are unaccompanied by reasonably available measures to protect the public's interest in access to information concerning an important area of government action. In light of identified deficits concerning excessive secrecy or the absence of accountability provisions, we reiterate the following recommendations from *Cybersecurity Will Not Thrive in Darkness*:

a. **Recommendation 6: Orders Should Appear in *The Canadian Gazette*.** In Bill C-26, orders are required to be published in the *Canadian Gazette*, but the Minister has the authority to "direct otherwise in the order." As such, "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."[31] The potential effect could unjustifiably restrict meaningful public debate on a matter of public importance and, as a consequence, the freedom of expression. The legislation should be amended such that orders must be published within 180 days of issuing them or within 90 days of an order being implemented, based on whichever

[30] *Cybersecurity Will Not Thrive in Darkness*, *supra*, at p. 18.
[31] *Ibid*.

condition is met first. The legislation should also expressly define circumstances that justify secrecy.

b. **Recommendation 7: The Minister Should Be Compelled To Table Reports Pertaining to Orders and Regulations.** To better safeguard the public interest, privacy, and the freedom of expression, the legislation should further 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

c. **Recommendation 8: Non-Disclosure Orders Should Be Time Limited.** Bill C-26 also proposes gag provisions with respect to Orders in Council or Ministerial Orders, which are not limited either temporally (i.e., how long is secrecy necessary?) or substantively (i.e., what circumstances justify secrecy?). As noted at paragraph 15, non-disclosure orders affect not only the recipient of the gag order but, also, the public's right to information that informs democratic debate. The legislation should be amended to include time constraints surrounding non-disclosure orders.

d. **Recommendation 8A: The Circumstances Purporting to Justify Confidentiality in a Non-Disclosure Order Should Be Defined In The Legislation.**

e. **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.

f. **Recommendation 10: An 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.

g. **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*, as well as on regulations pertaining to the *Telecommunications Act* and that are modified pursuant to s. 18 of the *Statutory Instruments Act*.

## III. Deficient Judicial Review Process

31. Bill C-26 contemplates that telecommunication providers may initiate judicial review proceedings in respect of orders or regulations issued under the proposed legislation. In pages 22-24 of his report, Dr. Parson identified problems that would arise if Bill C-26 is passed without amending section 15.9. As drafted, section 15.9 would permit a series of mandatory limits on open court principles, which would prevent judges from exercising judicial discretion in balancing the need for secrecy or confidentiality with the public's interest in disclosure. As noted at paragraph 15 in this submission, the *Charter* protects open court principles that apply in the context of judicial review, including *Charter* protections for the freedom of expression.

32. *Cybersecurity Will Not Thrive in Darkness* recommends (**Recommendation 12**) **that Bill C-26 should explicitly enable appointment of *amicus curiae* or a special advocate during judicial review.** The legislation should be amended such that, at the Court's pleasure, *amicus curiae* or a special advocate 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 in when evidence is sufficiently sensitive to bar a telecommunications provider's counsel from hearing it.

33. We also recommend:

    a. **Recommendation 12A: Section 15.9 Should Be Amended To Ensure The Judge Retains Authority To Balance The Public Interest In Disclosure Against The Interest In Confidentiality**: In general, mandatory limits on open courts (which prevent the judge from balancing the public interests at stake), are generally viewed as excessive infringements on section 2(b) rights.[32] For example, even in analogous provisions of the *Canada Evidence Act* (permitting secrecy in judicial proceedings for matters injurious to international relations, national defence or national security or endanger the safety of any person), the judge retains the authority to determine that "the public interest in disclosure outweighs in importance the public interest in non-disclosure". The same safety valve should be incorporated into section 15.9 of Bill C-26, in order to ensure that any limits to openness minimally impair freedom of expression.

    b. **Recommendation 12B: Where Summaries Are Provided Of Evidence And Information Received By The Court, Pursuant To Section 15.9(1)(C), These Summaries Must Also Be Available To The "Applicant and the Public"**. As noted at paragraph 15, the open court principle protects the public's and the media's interest in the openness of court proceedings. Practically speaking, the public's right of access to judicial summaries of this nature is typically accomplished by marking such summaries as an exhibit to the proceedings. The public's right of access to exhibits is a corollary of the open court principle.

[32] See Kent Roach and David Schneiderman, "Freedom of Expression in Canada", (2013) 61 S.C.L.R. (2d) at p. 488 ("Although the courts have generally been inclined to strike down mandatory bans on access to the courts, they also have been more deferential to bans that give judges discretion to restrict access to the courts and freedom of expression").

c. **Recommendation 12C: The Triggering Threshold Justifying Limits On The Openness Of The Proceedings Should Not Be Higher Than That Which Is Already Contained Under Analogous Provisions Of The *Canada Evidence Act*.**[33] In that regard, we recommend mirroring the language from the *Canada Evidence Act* through the following amendment:

> Section 15.9(1)(a) "…if, in the judge's opinion, the disclosure of the evidence or other information ~~could~~ would be injurious to international relations, national defence or national security or endanger the safety of any person".

## IV. Extensive Information Sharing Within and Beyond Canadian Agencies

34. Bill C-26 proposes to create broad information sharing powers within and beyond Canadian government agencies, without accompanying those powers with necessary limits, oversight, or accountability mechanisms. As noted at paragraph 24, the absence of reasonable procedural safeguards to review government powers that infringe upon privacy interests can render legislation invalid under section 8 of the *Charter*. To impose more appropriate guardrails on the proposed powers to share information within and beyond Canadian agencies, Recommendations 13-20 of *Cybersecurity Will Not Thrive in Darkness* are the following:

a. **Recommendation 13 and 14: Relief Should Be Available If Government Mishandles Confidential, Personal, or De-Identified Information.** The legislation should be amended to enable individuals and telecommunications providers to seek relief should the government or a party to whom the government has disclosed confidential, personal, or de-identified information loses control of that information, where that loss of control has material consequences for the individual, or for a telecommunication provider's business or technical operations.

b. **Recommendation 15: Government Should Notify Telecommunications Providers How It Will Use Collected Information, and Which Domestic Agencies Information Will Receive The Information.**

c. **Recommendation 16: Information Obtained from Telecommunications Providers Should Only be Used by Government Agencies for Cybersecurity and Information Assurance Activities.** Information should not be used for the purposes of signal intelligence and foreign intelligence activities, cross-department assistance unrelated to cyber-security, or active or defensive cyber operations. These restrictions should apply to all agencies.

d. **Recommendations 17 and 18: Data Retention Periods Should Be Attached to Telecommunications Providers' Data and to Foreign Disclosures of Information.** The legislation should be amended to highlight that confidential information 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. Similarly, an amendment should also require that the government attach data

[33] See *Canada Evidence Act*, R.S.C., 1985, c. C-5., at s. 38 to 38.15.

retention and deletion clauses in agreements or memoranda of understanding that are entered into with foreign agencies. Retention periods should be communicated to the affected telecommunications providers.

e. **Recommendation 19: Telecommunications Providers Should Be Explicitly Informed Which Foreign Parties Receive Their Information.** 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.

f. **Recommendation 20: Legislation Should Delimit the Conditions Wherein a Private Organization's Information Can Be Disclosed.** As drafted, section 15.7(1) appears to set an excessively low threshold for disclosing information, and could enable significant sharing of private, if not confidential, information, to address unspecified threats that are not set out in the legislation. Proposed textual amendments are found on page 30 of *Cybersecurity Cannot Thrive in the Darkness* (**Appendix A** to this brief).

## V. Costs Associated with Security Compliance

35. As noted above, imposing substantial costs of compliance on telecommunications providers may have the potential to impact upon the accessibility of telecommunication services, the digital divide, and *Charter*-protected rights or interests. To address concerns surrounding the costs associated with security compliance, *Cybersecurity Will Not Thrive in Darkness* makes the following recommendations:

a. **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.

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

c. **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.

## VI. Vague Drafting Language

36. The last set of recommendations pertain to ambiguities in Bill C-26. Notably, Bill C-26 does not specify the kinds of security threats that might be addressed by orders or regulations; fails to define key concepts like "interference", manipulation", and "disruption"; provides the Minister with unnecessarily open-ended powers; and lacks clear guidelines as to how personally identifiable information that is obtained from telecommunications providers is to be treated. As a result, *Cybersecurity Will Not Thrive in Darkness* makes the following recommendations:

    a. **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") compare 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 reformed *Telecommunications Act* would expand, contract, or address the same classes of acts as considered in the *CSE Act*.

    b. **Recommendations 25: Explicit Definitions for "Interference," "Manipulation," and "Disruption" Should Be Included in the Legislation or Else Publicly Promulgated.**

    c. **Recommendation 26 and 27: Ministerial Flexibility Should Be Delimited (i.e., remove open-ended language around powers such as "among other things").** In the event that a corresponding amendment is needed for Ministerial powers constrained to emergency circumstances, those powers should be subject to judicial review in Federal Court, including assessment for necessity, reasonableness, and proportionality. Decisions emergent from review should be published by the Federal Court.

    d. **Recommendation 28: The Legislation Should Make Clear that Personal Information and De-Identified Information is Classified as Confidential Information.** As noted above, the federal government's *Charter* statement appears to conclude that it is not the intent of Bill C-26 to authorize the collection and sharing personal information. If that is the case, the legislation should expressly say so. Alternatively, personal and de-identified information should be treated as confidential.

    e. **Recommendation 28A: Individuals Should Be Explicitly Informed If Their Information Has Been Collected Or Shared.** If the federal government does not expressly state that personal and de-identified information should not be included in collection and sharing powers, it should ensure that notice obligations are extended to individuals whose information is impacted by the collection and sharing powers under Bill C-26.

    f. **Recommendation 29: Prior Judicial Approval Should be Required for the Government to Obtain Personal or De-Identified Information from a Telecommunications Provider.** The information is further 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.

g. **Recommendation 30: The Government Cannot Disclose Personal or De-Identified Information to Foreign Organizations.**

# Part 4. Concluding Remarks

37. We urge this Committee to take seriously the recommendations that were identified in *Cybersecurity Will Not Thrive in Darkness*. We note that most of these recommendations have been either reiterated or expanded upon by the Joint Submission to this committee submitted by civil society organizations and individuals.[34] In detailing these recommendations for this Committee's study, we also urge the Committee to consider the additional *Charter* interests that are engaged by Bill C-26, including equality, non-discrimination, freedom of expression, and privacy, as described in Part 2 of this Brief. We echo Dr. Parsons' view that "cybersecurity efforts through Bill C-26 should seek to build trust between the government and non-government entities, including the general public," and that independent bodies (including the Privacy Commissioner of Canada, National Security and Intelligence Committee of Parliamentarians, or National Security and Intelligence Review Agency) should be integrated into the government's assessments of the necessity, proportionality, and reasonableness of Orders in Council, Ministerial Orders, or regulations.

38. Citizen Lab's recent report, *Finding You* (enclosed as **Appendix C**), documents continuing vulnerabilities at the heart of the world's mobile communications networks. The report's findings underscore that cybersecurity has not thrived in darkness. Historical and continuing deficiencies in oversight, transparency, and accountability of network security have led to serious geolocation-related threats associated with contemporary networks. The report notes that the "failure of effective regulation, accountability, and transparency has been a boon for network-based geolocation surveillance."[35]

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

# Part 5. Organizational Information

40. Kate Robertson is a lawyer and senior research associate at the Citizen Lab, Munk School of Global Affairs & Public Policy at the University of Toronto. Her research explores the intersection of law, policy, and technology, and focuses on transparency and accountability mechanisms relevant to the relationship between corporations and state agencies regarding personal data and other surveillance activities. I

[34] Canadian Civil Liberties Association, et al, "Joint Submission to the House of Commons Standing Committee on Public Safety and National Security", published October 27, 2023.

[35] *Finding You*, *supra*, at p. 19.

draw on former experience as a law clerk of the Supreme Court of Canada, and subsequently, as a lawyer in Canada's justice system.

41. Lina Li is a BCL/JD student at McGill University's Faculty of Law and a legal intern at the Citizen Lab, Munk School of GLobal Affairs & Public Policy at the University of Toronto. Her areas of interest lie at the intersection of law and technology, focusing on questions of policy, AI governance, and corporate transparency.

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

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

## Appendix A - Table of Recommendations


| | |
|---|---|
| Recommendation 1: Orders in Council and Ministerial Orders Must Be Necessary, Proportionate, and Reasonable | 10 |
| Recommendation 2: Orders Should Include a Reference to Timeliness | 10 |
| Recommendation 3: Government Should Undertake Impact Assessments Prior to Issuing Orders | 10 |
| Recommendation 4: Forbearance or Cost/Cost-Minus Clauses Should Be Inserted | 10 |
| Recommendation 5: The Standards That Can Be Imposed Must Be Defined | 10 |
| Recommendation 6: Orders Should Appear in The *Canadian Gazette* | 11 |
| Recommendation 7: The Minister Should Be Compelled to Table Reports Pertaining to Orders and Regulations | 11 |
| Recommendation 8: Non-Disclosure Orders Should Be Time Limited | 11 |
| Recommendation 8A: The Circumstances Purporting to Justify Confidentiality in a Non-Disclosure Order Should Be Defined In The Legislation | 12 |
| Recommendation 9: The CRTC Should Indicate When Orders Override Parts of CRTC Decisions | 12 |
| Recommendation 10: Annual Report Should Include the Number of Times Government Orders or Regulations Prevail over CRTC Decisions | 12 |
| Recommendation 11: All Regulations Under the *Telecommunications Act* Should Be Accessible to The Standing Joint Committee for the Scrutiny of Regulations | 12 |
| Recommendation 12: Judicial Review Should Explicitly Enable Appointment of *Amicus Curiae* or a special advocate | 12 |
| Recommendation 12A: Section 15.9 Should Be Amended to Ensure the Judge Retains Authority to Balance the Public Interest in Disclosure Against the Interest in Confidentiality | 13 |
| Recommendation 12B: Where Summaries Are Provided Of Evidence And Information Received By The Court, Pursuant To Section 15.9(1)(C), These Summaries Must Also Be Available To The Public | 13 |
| Recommendation 12C: The Triggering Threshold Justifying Limits On The Openness Of The Proceedings Should Not Be Higher Than That Which Is Already Contained Under Analogous Provisions Of The *Canada Evidence Act* | 13 |
| Recommendation 13: Relief Should Be Available If Government Mishandles Confidential Information | 14 |

| | |
|---|---|
| Recommendation 14: Relief Should Be Available If Government Mishandles Personal or De-Identified Information | 14 |
| Recommendation 15: Government Should Explain How It Will Use Information and Reveal the Domestic Agencies To Which Information Is Disclosed | 14 |
| Recommendation 16: Information Obtained from Telecommunications Providers Should Only be Used for Cybersecurity and Information Assurance Activities | 14 |
| Recommendation 17: Data Retention Periods Should Be Attached to Telecommunications Providers' Data | 14 |
| Recommendation 18: Data Retention Periods Should Be Attached to Foreign Disclosures of Information | 14 |
| Recommendation 19: Telecommunications Providers Should Be Informed Which Foreign Parties Receive Their Information | 14 |
| Recommendation 20: Legislation Should Delimit the Conditions Wherein a Private Organization's Information Can Be Disclosed | 14 |
| Recommendation 21: Compensation Should Be Included for Smaller Organizations | 15 |
| Recommendation 22: Proportionality and Equity Assessments Should Be Included in Orders or Regulations | 15 |
| Recommendation 23: Government Should Encourage Cybersecurity Training | 15 |
| Recommendation 24: Clarity Should Exist Across Legislation | 15 |
| Recommendation 25: Explicit Definitions Should Be Included In the Legislation or Else Publicly Promulgated | 16 |
| Recommendation 26: Ministerial Flexibility Should Be Delimited | 16 |
| Recommendation 27: Emergency Situations | 16 |
| Recommendation 28: Personal Information Is Confidential Information | 16 |
| Recommendation 28A: Individuals Should Be Explicitly Informed If Their Information Has Been Collected Or Shared | 16 |
| Recommendation 29: Prior Judicial Approval to Obtain Personal or De-Identified Information | 16 |
| Recommendation 30: No Disclosure of Personal or De-Identified Information to Foreign Organizations | 16 |

## Appendix B - Enclosed Report

Christopher Parsons. "Cybersecurity Will Not Thrive in Darkness: A Critical Analysis of Proposed Amendments in Bill C-26 to the Telecommunications Act," Citizen Lab Research Report No. 158, University of Toronto, October 18, 2022.

## Appendix C - Enclosed Report

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

# 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


Executive Summary 1

Introduction 3

1. Background 6

2. Proposed Reforms to the Telecommunications Act 10

2.1. Compelling or Directing Modifications to Organizations' Technical or Business Activities 10

**Recommendation 1: Orders in Council and Ministerial Orders Must Be Necessary, Proportionate, and Reasonable** 13

**Recommendation 2: Orders Should Include a Reference to Timelines** 14

**Recommendation 3: Government Should Undertake Impact Assessments Prior to Issuing Orders** 15

**Recommendation 4: Forbearance or Cost/Cost-Minus Clauses Should Be Inserted** 15

**Recommendation 5: The Standards That Can Be Imposed Must Be Defined** 17

2.2. Secrecy and Absence of Transparency or Accountability Provisions 17

**Recommendation 6: Orders Should Appear in *The Canadian Gazette*** 18

**Recommendation 7: The Minister Should Be Compelled to Table Reports Pertaining to Orders and Regulations** 19

**Recommendation 8: Gags Should Be Time Limited** 19

**Recommendation 9: The CRTC Should Indicate When Orders Override Parts of CRTC Decisions** 20

**Recommendation 10: Annual Report Should Include the Number of Times Government Orders or Regulations Prevail Over CRTC Decisions** 20

**Recommendation 11: All Regulations Under *the Telecommunications Act* Should Be Accessible to The Standing Joint Committee for the Scrutiny of Regulations** 21

2.3. Deficient Judicial Review Process 21

**Recommendation 12: Judicial Review Should Explicitly Enable Appointment of *Amicus Curiae*** 24

2.4. Extensive Information Sharing Within and Beyond Canadian Agencies 25

**Recommendation 13: Relief Should Be Available If Government Mishandles Confidential Information** 27

**Recommendation 14: Relief Should Be Available If Government Mishandles Personal or De-Identified Information** 27

**Recommendation 15: Government Should Explain How It Will Use Information and Reveal the Domestic Agencies To Which Information Is Disclosed** 28

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

# Contents

Recommendation 17: Data Retention Periods Should Be Attached to Telecommunications Providers' Data 29
Recommendation 18: Data Retention Periods Should Be Attached to Foreign Disclosures of Information 29
Recommendation 19: Telecommunications Providers Should Be Informed Which Foreign Parties Receive Their Information 30
Recommendation 20: Legislation Should Delimit the Conditions Wherein a Private Organization's Information Can Be Disclosed 31
2.5. Costs Associated with Security Compliance 31
Recommendation 21: Compensation Should Be Included for Smaller Organizations 32
Recommendation 22: Proportionality and Equity Assessments Should Be Included in Orders or Regulations 32
Recommendation 23: Government Should Encourage Cybersecurity Training 33
2.6. Vague Drafting Language 33
Recommendation 24: Clarity Should Exist Across Legislation 35
Recommendation 25: Explicit Definitions Should Be Included In the Legislation or Else Publicly Promulgated 35
Recommendation 26: Ministerial Flexibility Should Be Delimited 36
Recommendation 27: Emergency Situations 36
Recommendation 28: Personal Information Is Confidential Information 37
Recommendation 29: Prior Judicial Approval to Obtain Personal or De-Identified Information 38
Recommendation 30: No Disclosure of Personal or De-Identified Information to Foreign Organizations 38

3. Counterbalances to Security 39

4. Conclusion 41

# 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


| | |
|---|---|
| **Recommendation 1**: Orders in Council and Ministerial Orders Must Be Necessary, Proportionate, and Reasonable | p. 13 |
| **Recommendation 2**: Orders Should Include a Reference to Timeliness | p. 14 |
| **Recommendation 3**: Government Should Undertake Impact Assessments Prior to Issuing Orders | p. 15 |
| **Recommendation 4**: Forbearance or Cost/Cost-Minus Clauses Should Be Inserted | p. 15 |
| **Recommendation 5**: The Standards That Can Be Imposed Must Be Defined | p. 17 |
| **Recommendation 6**: Orders Should Appear in *The Canadian Gazette* | p. 18 |
| **Recommendation 7**: The Minister Should Be Compelled to Table Reports Pertaining to Orders and Regulations | p. 19 |

| | |
|---|---|
| **Recommendation 8**: Gags Should Be Time Limited | p. 19 |
| **Recommendation 9**: The CRTC Should Indicate When Orders Override Parts of CRTC Decisions | p. 20 |
| **Recommendation 10**: Annual Report Should Include the Number of Times Government Orders or Regulations Prevail over CRTC Decisions | p. 20 |
| **Recommendation 11**: All Regulations Under the *Telecommunications Act* Should Be Accessible to The Standing Joint Committee for the Scrutiny of Regulations | p. 21 |
| **Recommendation 12**: Judicial Review Should Explicitly Enable Appointment of Amicus Curiae | p.24 |
| **Recommendation 13**: Relief Should Be Available If Government Mishandles Confidential Information | p. 27 |
| **Recommendation 14**: Relief Should Be Available If Government Mishandles Personal or De-Identified Information | p. 27 |
| **Recommendation 15**: Government Should Explain How It Will Use Information and Reveal the Domestic Agencies To Which Information Is Disclosed | p. 28 |
| **Recommendation 16**: Information Obtained from Telecommunications Providers Should Only be Used for Cybersecurity and Information Assurance Activities | p. 29 |
| **Recommendation 17**: Data Retention Periods Should Be Attached to Telecommunications Providers' Data | p. 29 |
| **Recommendation 18**: Data Retention Periods Should Be Attached to Foreign Disclosures Of Information | p. 29 |
| **Recommendation 19**: Telecommunications Providers Should Be Informed Which Foreign Parties Receive Their Information | p. 30 |
| **Recommendation 20**: Legislation Should Delimit the Conditions Wherein a Private Organization's Information Can Be Disclosed | p. 31 |
| **Recommendation 21**: Compensation Should Be Included for Smaller Organizations | p. 32 |
| **Recommendation 22**: Proportionality and Equity Assessments Should Be Included in Orders or Regulations | p. 32 |
| **Recommendation 23**: Government Should Encourage Cybersecurity Training | p. 33 |
| **Recommendation 24**: Clarity Should Exist Across Legislation | p. 35 |
| **Recommendation 25**: Explicit Definitions Should Be Included In the Legislation or Else Publicly Promulgated | p. 35 |
| **Recommendation 26**: Ministerial Flexibility Should Be Delimited | p. 36 |
| **Recommendation 27**: Emergency Situations | p. 36 |
| **Recommendation 28**: Personal Information Is Confidential Information | p. 37 |
| **Recommendation 29**: Prior Judicial Approval to Obtain Personal or De-Identified Information | p. 38 |
| **Recommendation 30**: No Disclosure of Personal or De-Identified Information to Foreign Organizations | p. 38 |

# 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 amend- ments 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 recom- mendations 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 infrastruc- ture 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<br>15.5 (1) A person who provides any of the following information under section 15.4 may designate it as confidential: | Confidential information — designation<br>15.5 (1) A person who provides any of the following information under section 15.4 may designate it as confidential:<br>…<br>(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 legis- lation 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.

# Finding You

## The Network Effect of Telecommunications Vulnerabilities for Location Disclosure

By Gary Miller and Christopher Parsons

OCTOBER 26, 2023
RESEARCH REPORT #171

munk school
OF GLOBAL AFFAIRS & PUBLIC POLICY
UNIVERSITY OF TORONTO
THECITIZENLAB

# Copyright



Electronic version first published by the Citizen Lab in 2023. This work can be accessed through https://citizenlab.ca/2023/10/finding-you-telecommunications-vulnerabilities-for-location-disclosure/.

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 Authors

**Gary Miller** contributed to this report while a Researcher at the Citizen Lab. He is currently the Founder of the Mobile Intelligence Alliance, a US-based non-profit mobile security research organization, a former mobile network security executive, and regarded as an expert in mobile network espionage. He received his BA in Economics from the University of Washington and is a contributor in mobile espionage investigative journalism research with major global news outlets.

**Christopher Parsons** contributed to this report while he was a Senior Research Associate at the Citizen Lab, in the Munk School of Global Affairs & Public Policy at 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. He is currently an A/Manager, Technology Policy at the Information and Privacy Commissioner of Ontario.

## Acknowledgements

We would like to thank civil society organizations, investigative journalists, and mobile network security experts who graciously agreed to contribute their insights and share forensic artifacts in the course of developing this report.

We want to specifically thank Siena Anstis, Kate Robertson, Jakub Dalek, Celine Bauwens, Levi Meletti, and Mohamed Ahmed for their thoughts and expertise, edits, and peer review of this report.

Additionally, we would like to thank Mari Zhou for her design and publishing assistance and Snigdha Basu for her communications support. This report was undertaken under the supervision of Professor Ronald Deibert.


## Corrections and Questions

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

## Suggested Citation

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

# Information Boxes


| | |
|---|---|
| **Information Box 1**: The IMSI Network Identifier Explained | **p.5** |
| **Information Box 2**: Cross Protocol Signaling Attacks | **p.11** |
| **Information Box 3**: The Future of Global Title Leasing | **p.25** |
| **Information Box 4**: Equivalent Signaling Message Types Used to Query Mobile Device Location | **p.28** |

# Contents


Introduction 1

1. Roaming, SIMs, and Services 101 3

1.1. From SIM to Services - Creating the Path to Network Surveillance 4

2. Geolocation Attacks Against Telecommunications Networks 7

2.1 Active Attacks 7

2.1.1 How Actors Access Networks For Geolocation Tracking 8

2.1.2. Vulnerabilities Tied to Home Location Register Lookup and Network Identification 10

2.1.3. Domestic Threats—Innocent Until Proven Guilty 11

2.2 Passive Attacks 13

2.2.1. Signaling Probes and Network Monitoring Tools 13

2.2.2. Packet Capture Examples of Location Monitoring 14

3. Case Studies and Statistics 16

3.1 Case Study - Saudi Arabia Tracking Travelers in the United States 16

3.2. Current Statistics – Geolocation Tracking vs Other Threat Types 19

4. Incentives Enabling Geolocation Attacks 21

4.1. Economic Enablers 22

4.2 Industry Enablers 22

4.3. Government Enablers 26

5. Geolocation Tracking in 5G Networks and Unimplemented Defensive Measures 28

5.1. Subscriber Identity Privacy Enhancements 28

5.2. International Signaling and Interconnect Security Enhancements 29

6. Conclusion 31

# Introduction

The information collected by, and stored within, mobile networks can represent one of the most current and comprehensive dossiers of our life. Our mobile phones are connected to these networks and reveal our behaviours, demographic details, social communities, shopping habits, sleeping patterns, and where we live and work, as well as provide a view into our travel history. This information, in aggregate, is jeopardized, however, by technical vulnerabilities in mobile communications networks. Such vulnerabilities can be used to expose intimate information to many diverse actors and are tightly linked to how mobile phones roam across mobile operators' networks when we travel. Specifically, these vulnerabilities are most often tied to the signaling messages that are sent between telecommunications networks which expose the phones to different modes of location disclosure.

Telecommunications networks have been designed to rely on private, though open, signaling connections. These connections enable domestic and international roaming, where a mobile phone can seamlessly pass from one company's network to another. The signaling protocols used for this purpose also allow networks to retrieve information about the user, such as whether a number is active, which services are available to them, to which country network they are registered, and where they are located. These connections and associated signaling protocols, however, are constantly being targeted and exploited by surveillance actors with the effect of exposing our phones to numerous methods of location disclosure.

Most unlawful network-based location disclosure is made possible because of how mobile telecommunications networks interoperate. Foreign intelligence and security services, as well as private intelligence firms, often attempt to obtain location information, as do domestic state actors such as law enforcement. Notably, the methods available to law enforcement and intelligence services are similar to those used by the unlawful actors and enable them to obtain individuals' geolocation information with high degrees of secrecy. Over the course of this report we will generally refer to all of these actors as 'surveillance actors' to refer to their interest in undertaking mobile geolocation surveillance.

Despite the ubiquity of global 4G network penetration and the rapidly expanding 5G network footprint there are many mobile devices, and their owners, who rely on older 3G networks. This is particularly the case in the regions of Eastern Europe, the Middle East, and Sub-Saharan Africa where 3G subscriber penetration is 55% according to the GSMA[1], an organization that provides information, services, and guidelines to members of the mobile industry. Further, at the end of 2021 the UK-based mobile market intelligence

1 Kenechi Okeleke, Harry F. Ballon, and James Joiner. (2023). *The Mobile Economy 2023*. https://data.gsmaintelligence.com/research/research/research-2023/the-mobile-economy-2023

firm Mobilesquared estimated that only a quarter of mobile network operators worldwide have deployed a signaling firewall[2] that is designed to impair geolocation surveillance. Telecom insiders understand that the vulnerabilities in the SS7 signaling protocol used in 3G roaming have enabled the development of commercial surveillance products that provide their operators with anonymity, multiple access points and attack vectors, a ubiquitous and globally-accessible network with an unlimited list of targets, and virtually no financial or legal risks.

This report provides a high-level overview of the geolocation-related threats associated with contemporary networks that depend on the protocols used by 3G, 4G, and 5G network operators, followed by evidence of the proliferation of these threats. **Part 1** provides the historical context of unauthorized location disclosures in mobile networks and the importance of the target identifiers used by surveillance actors. **Part 2** explains how mobile networks are made vulnerable by signaling protocols used for international roaming, and how networks are made available to surveillance actors to carry out attacks. An overview of the mobile ecosystem lays the foundation for the technical details of domestic versus international network surveillance, while the vectors of active versus passive surveillance techniques with evidence of attacks shows how location information is presented to the actor. **Part 3** provides details of a case study from a media report that shows evidence of widespread state-sponsored surveillance, followed by threat intelligence data revealing network sources attributed to attacks detected in 2023. These case studies underscore the significance and relevance of undertaking these kinds of surveillance operations.

Deficiencies in oversight and accountability of network security are discussed in **Part 4**. This includes outlining the incentives and enablers that are provided to surveillance actors from industry organizations and government regulatory agencies. **Part 5,** makes clear that the adoption of 5G technologies will not mitigate future surveillance risks unless policymakers quickly move to compel telecommunications providers to adopt the security features that are available in 5G standards and equipment. If policymakers do not move swiftly then surveillance actors may continue to prey upon mobile phone users by tracking their physical location. Such a future paints a bleak picture of user privacy and must be avoided.

2 Mobileum, Mobilesquared. (2021). The State of the Signaling Firewall Landscape November 2021. https://www.mobilesquared.co.uk/wp-content/uploads/2023/04/Mobileum_Security-Research_Nov21-FINAL-VERSION.pdf

# 1. Roaming, SIMs, and Services 101

Mobile users expect their phones to work wherever they travel beyond the borders of their home country. However, it is when individuals are traveling abroad that they are most vulnerable to network-based geolocation tracking.

When an individual travels internationally with a mobile phone, the phone continues to operate outside of its home mobile network (i.e., the domestic carrier with which it is associated). This ongoing operation is accomplished through a series of global interconnections and agreements between network operators around the world. These interconnections and agreements are often unique to each network type (3G, 4G, and 5G) and these networks have historically been bridged by telephony signaling protocols which have been developed since the 1970s to form the Signaling System Number 7 (SS7 network), and subsequently the Long Term Evolution (LTE/4G) network which uses the Diameter signaling protocol.

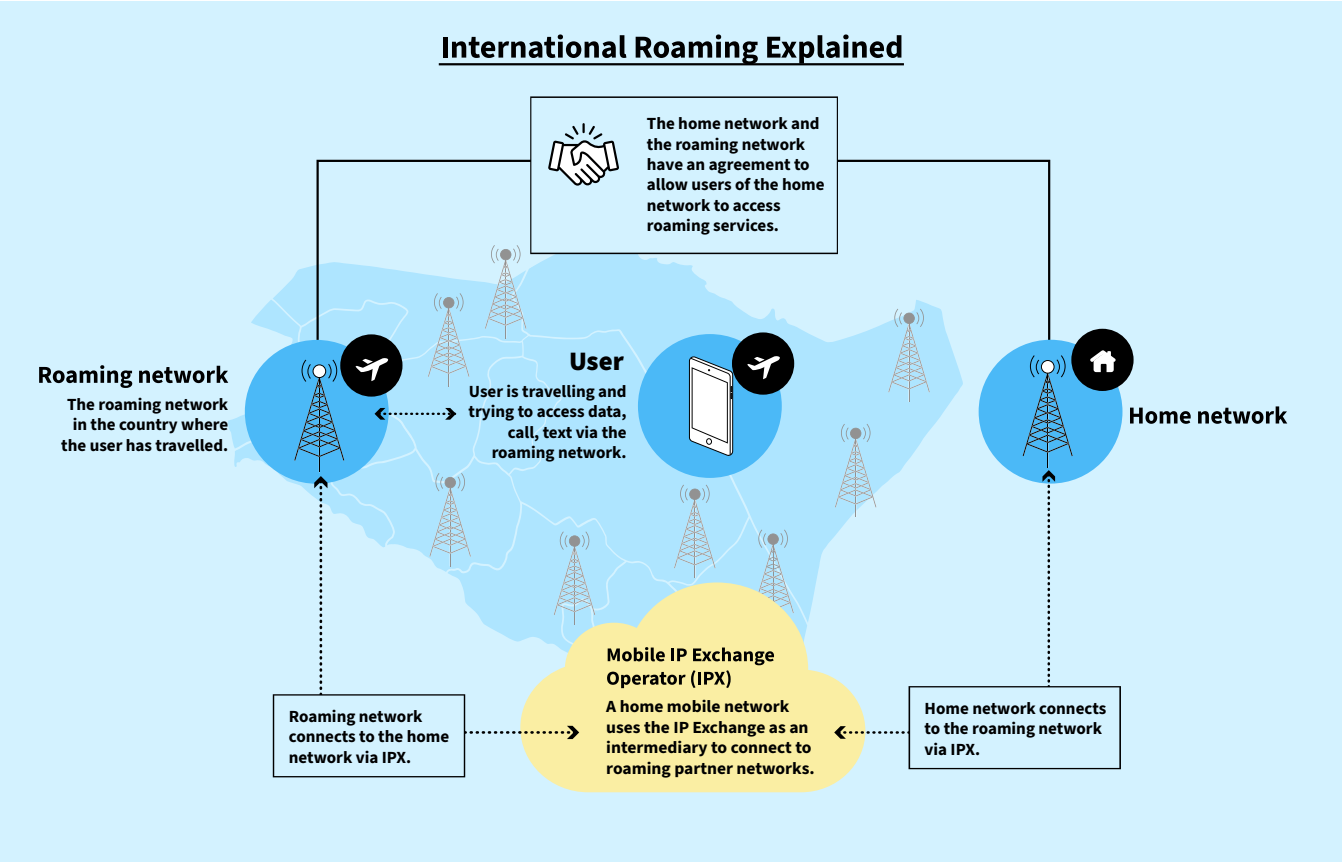



Figure 1: International roaming process flow.

When roaming on different foreign networks, those networks charge differing rates for voice, data, and messaging services in exchange for the services provided to users roaming on their networks. To enable these services, the involved network operators open their networks to one another so they can interoperate. It is this interoperation

that allows individuals to seamlessly make calls, send text messages, or use data while roaming on a foreign network.

Generally speaking, wholesale roaming agreements, such as the information included in the GSMA framework,[3] are used to establish the commercial and operational aspects of sending and receiving signalling messages for service exchange between network roaming partners. Signaling messages are operator-to-operator messages that are used to authenticate and manage user mobility. Functionally, operators use signaling messages to establish and maintain sessions providing services to users. However, while security best practices state that mobile network operators should reject messages sent by non-roaming partners or prevent abusive messages from exposing users to location tracking, these practices are not mandatory or enforced. This voluntary aspect of operator-to-operator signaling message security provides surveillance actors with an entry path into the target network. Further, networks typically connect to at least two network operators per country (and often many more) to minimize roaming costs and maximize network resiliency. While these open connections are a prerequisite for roaming service enablement they have also presented risks to geolocation tracking.

## 1.1. From SIM to Services - Creating the Path to Network Surveillance

Understanding the points of vulnerability that surveillance actors exploit to track user geolocation requires an understanding of how users are globally and uniquely identified on mobile networks. These identifiers play a critical role in the process of routing and delivering the malicious geolocation tracking messages from the surveillance actor's software to the network of the target phone, and returning the information back to the actor.

A starting point for understanding the identity of a user's phone is when the mobile network operator issues the SIM card. While we are accustomed to inserting the ever-smaller cards into mobile devices, these physical cards are rapidly being displaced by a software-based eSIM. Both physical- and software-based SIM cards use a unique identity called the Integrated Circuit Card ID (ICCID). Mobile network operators then use the ICCID to assign a globally unique network identity that is specific to that network operator, known as the International Mobile Subscriber Identity (IMSI), during service activation. This globally unique and network-specific IMSI is the crucial element in the context of delivering services to the phone from any global roaming network. The IMSI is, also, central to the targeting methods that are used in geolocation tracking operations that are sourced from foreign networks.

3 Relevant GSMA international roaming agreements include AA.12, AA.13, and AA.14

After the SIM or eSIM is provisioned to the user account, a phone number—which is referred to by the telecommunications industry as the Mobile Station International Subscriber Directory Number (MSISDN)—is also mapped to the IMSI that is defined by the network operator. This combined information—the MSISDN and the IMSI—is integrated into the network operator's service delivery, authorization, and authentication systems. Key to these systems is the 3G/4G Home Subscriber Service/Home Location Register (HSS/HLR) and 5G Unified Data Manager (UDM), which are collectively master databases containing the rules to authorize services associated with the subscription plan an individual has purchased on a monthly or pay-as-they-go basis.

Having fully assigned and provisioned the SIM, the mobile device can communicate with the operator's network for phone calls, text messages, and application data that can be routed globally. It is, also, at this point that malicious signaling messages can be directed towards the device with the effect of exposing its geolocation.

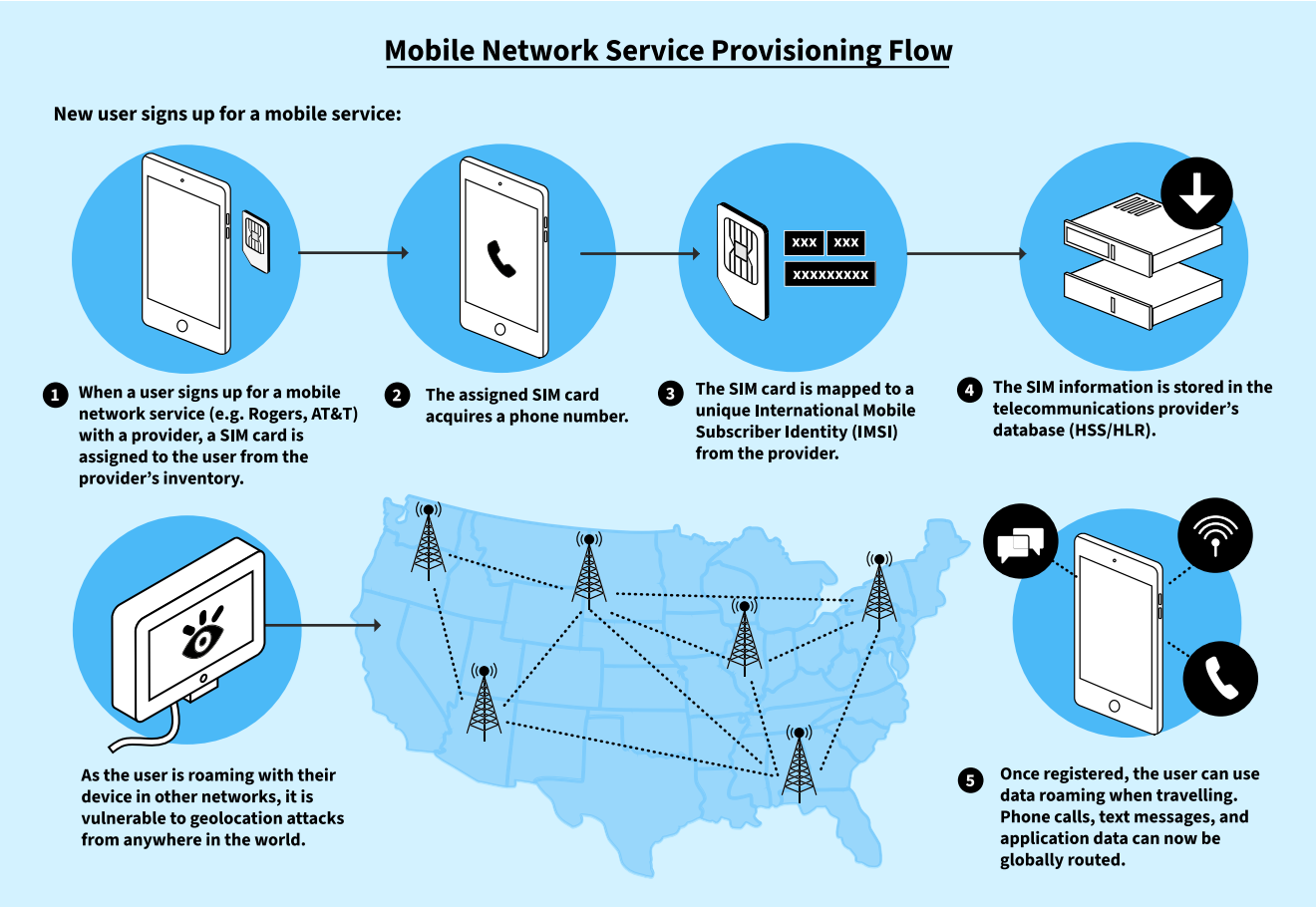



Figure 2: How mobile identities are provisioned to enable surveillance operations.

The IMSI of the target phone is a critical information element for conducting surveillance and is frequently seen in the initial procedure of the operation to locate its Cell ID, which

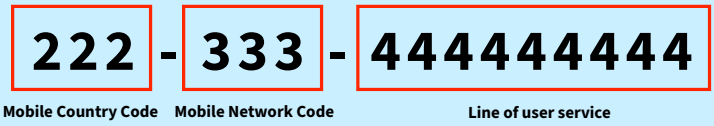
is the unique number used to identify a base station tower of a given network. The Cell ID can then be correlated to a location using one of many Cell ID database services.[4]

**Information Box 1: The IMSI Network Identifier Explained**

Networks use either 3G/4G identities or 5G identities. 3G and 4G networks use the IMSI, which typically include 15 digits, such as the following example:

- 222-333-444444444
- The first 3 digits (222) are the mobile country code (MCC)
- The next 2–3 digits (333) are the mobile network code (MNC).
- The remaining digits (444444444) identify the line of the user service.

**International Mobile Subscriber Identity (IMSI)**




In contrast, 5G networks have defined the Subscription Permanent Identifier (SUPI) instead of IMSIs. The SUPI is equivalent to the IMSI to ensure compatibility with 4G network infrastructure. Such compatibility is particularly important because 4G network infrastructure underpins a majority of current 5G international roaming.

5G adds a security feature called the Subscription Concealed Identifier (SUCI), with an encryption scheme to prevent the open transmission of the user network identity over the radio interface. This has the effect of foiling surveillance actors who have physical proximity to a mobile device and use tools such as IMSI Catchers to intercept radio communications in order to forcibly reveal a device's IMSI number. IMSI Catchers are used by a variety of actors, including law enforcement, security, and foreign intelligence agencies, as well as criminals, to obtain the network identity of users for surveillance purposes.[5]

4 Many commercial and public Cell ID database services are available: https://en.wikipedia.org/wiki/GSM_Cell_ID.

5 For more about IMSI Catchers, see: Christopher Parsons and Tamir Israel. (2016). "Gone Opaque? An Analysis of Hypothetical IMSI Catcher Overuse in Canada." *Citizen Lab and CIPPIC.* Available at: https://citizenlab.ca/wp-content/uploads/2016/09/20160818-Report-Gone_Opaque.pdf.

# 2. Geolocation Attacks Against Telecommunications Networks

This report principally focuses on geolocation threats that result from targeting mobile signaling networks. Surveillance actors can utilize either active or passive surveillance methods to obtain information from mobile signaling networks, with the effect of exposing a user's location. In some cases they may combine multiple methods to accomplish this goal.

The distinction between the two approaches is notable. Active surveillance implies that an actor uses software to engage with a mobile network to elicit a response with the target phone location, whereas passive surveillance uses a collection device to obtain the location of phones directly from the network. When it comes to active attacks, an adversarial network uses software to send crafted signaling messages to vulnerable target mobile networks to query and obtain a current geolocation of the target phone. Such attacks are possible where the targeted networks do not have properly deployed or configured security controls. Further, an actor accessing a network through a lease arrangement can only use active surveillance methods unless they have the ability to install, or otherwise access, passive collection devices located in networks around the world.

There is, however, the possibility that a mobile operator or other actors could be compelled to undertake both active and passive surveillance. In this situation, the network operator may either be legally compelled to facilitate surveillance or, alternately, suffer from a hostile insider who is accessing mobile systems illicitly or illegally. Further, should a third-party gain access to the operator or provider, such as by compromising VPN access into the targeted network systems, they may be able to obtain location information of targeted users in both active and passive modes.

## 2.1 Active Attacks

In cases of active attacks, a domestic or foreign surveillance actor uses software to issue signaling messages which are directed at the target user's mobile phone identity (commonly the IMSI) by manipulating the network signaling data to trigger a response from the target user's home network. Such surveillance measures can be used to facilitate other communications interception, location disclosure, or service interruption. In this section, we discuss how actors may gain access to networks for geolocation tracking as well as some of the vulnerabilities that can subsequently be exploited by surveillance actors that are undertaking active surveillance operations.

### 2.1.1 How Actors Access Networks For Geolocation Tracking

Network-based geolocation tracking most commonly involves three interlinked elements:

1. specialized surveillance software;
2. a signaling address that is used to route malicious messages to the target network(s) so as to extract the targeted device's geolocation data;
3. network connectivity to the global 3G SS7 and 4G Diameter network.

This global SS7 or Diameter network backbone is known as the IP Exchange (IPX). The purpose of the IPX is to facilitate interconnection between mobile operator networks for the transport of signaling messages according to agreed interoperable service definitions and commercial agreements.[6] Further, the IPX architecture states that only service providers that are mobile network operators can connect to the network.[7] Therefore, third-parties who are not part of the mobile network operator community should not be allowed to connect and send mobile signaling messages, where vulnerabilities can expose mobile users to unauthorized geolocation surveillance.

Connections by surveillance actors to the IPX network are generally accomplished through covert commercial arrangements with a mobile operator, intermediary IPX transit, or other third-party service providers, such as SMS messaging providers, private mobile network operators, or sponsored Internet of Things service providers that possess connections to the IPX. While the IPX is designed to enable network roaming between different operators' networks it can also be abused to enable surreptitious geolocation surveillance. The IPX is used by over 750 mobile networks[8] spanning 195 countries around the world.[9] There are a variety of companies with connections to the IPX which may be willing to be explicitly complicit with, or turn a blind eye to, surveillance actors taking advantage of networking vulnerabilities and one-to-many interconnection points to facilitate geolocation tracking.

It is possible for mobile telecommunications companies to 'lease' access to their networks. This has the effect of significantly expanding the number of companies which may offer access to the IPX for malicious purposes. Moreover, a lessee can further sublease access to the IPX with the effect of creating further opportunities for a surveillance actor to use an IPX connection while concealing its identity through a number of leases and subleases.

In more detail, telecommunications operators in a given country apply for, and are allocated, bulk telephone number ranges according to a numbering plan as administered

6 GSMA Document IR.34 - Guidelines for IPX Provider Networks, Section 3 "IPX Network Architecture"

7 GSMA Document IR.34, Section 3.5

8 *About the GSMA - Represents the interests of mobile operators worldwide.* (2023, June 12). About Us. https://www.gsma.com/aboutus

9 *Member States.* (n.d.). United Nations. https://www.un.org/en/about-us/member-states

by their national telecommunications regulatory authority. These ranges are often used for a variety of purposes such as fixed line telephones, mobile numbers, or toll free numbers. Once the operator is allocated numbers, they can assign and use a portion of numbers as addresses, known as Global Title Addresses (GT), to equipment in their networks that are needed to operationalize domestic and international roaming with other network partners. This includes equipment such as the Visitor Location Register (VLR), Home Location Register (HLR), and other core network equipment.

The operators may, also, assign these GTs to third-party lessees. A malicious lessee may:

- configure surveillance software to use the leased GTs to conduct their own surveillance;
- use the GTs in a cloud-hosted solution to provide a commercial surveillance service;
- further partition the GT's for subleasing to other surveillance actors.

Notably, a surveillance actor can potentially lease GTs from either a single telecommunications operator or a range of operators from different jurisdictions. In this latter case, the surveillance actor may rotate attacks between the various subleased GTs either to try and avoid detection or to increase the likelihood of a successful operation if attacks from some of the subleased GTs happen to be blocked by network firewalls.

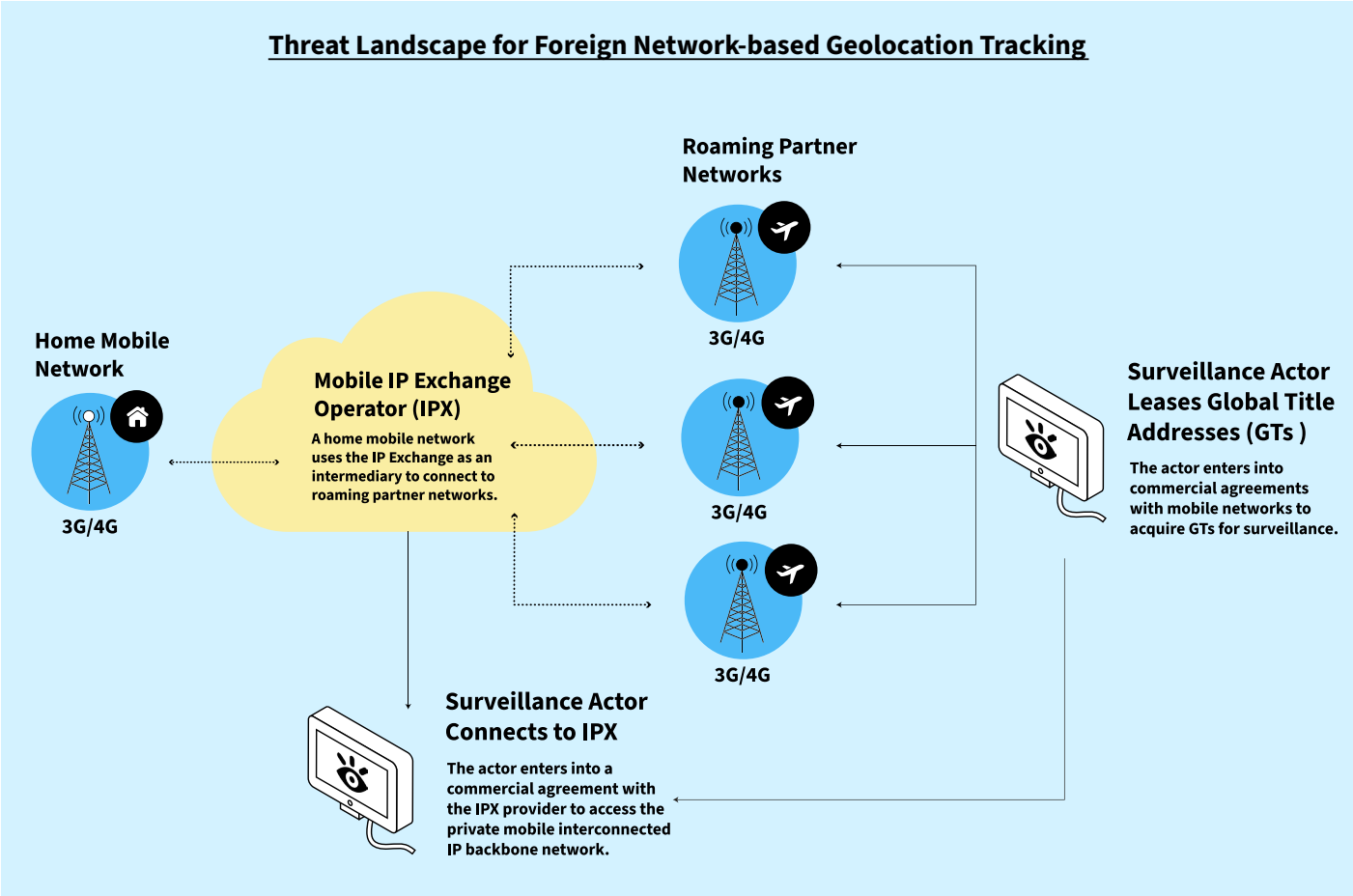



Figure 3: threat landscape for foreign network-based geolocation tracking.

Surveillance actors' operations are made possible due to the hub-and-spoke model that the IPX relies on to facilitate international roaming to other networks. In this model, while the IPX is responsible for routing and delivering messages between the home and roaming networks, it also connects other service providers, such as those delivering SMS messages, and other Value Added Service (VAS) providers that offer mobile number/HLR lookup, IoT mobility services, vehicle tracking, or hosted mobile virtual network operators (MVNO) that have agreements with IPXes. The end result is that a mix of third-parties have global access to mobile network operators' networks despite not having any direct commercial relationship with the foreign networks to which they can connect.

### 2.1.2. Vulnerabilities Tied to Home Location Register Lookup and Network Identification

One of the methods used to reveal network information associated with a mobile phone number entails using a commercial HLR lookup service. These kinds of commercial services enable organizations which are not telecommunications operators to check the status of a mobile phone number using the SS7 network without a mobile operator agreement. In this kind of situation, a surveillance actor would pay a fee to the HLR lookup provider based on the number of mobile number lookups it submitted to the service.

After receiving the phone numbers to lookup, the lookup service would issue a query using the SS7 network and retrieve a response from the network. That response would disclose information about whether the targeted number was valid and actively registered on a mobile network. If it is valid and active, the response will also disclose the network it was attached to and whether it was in a roaming state. Key information in the query will return the target IMSI associated with the MSISDN and the roaming network Visitor Location Register (VLR) address associated with the target phone. With this information in hand the actor can issue geolocation tracking requests with specific knowledge of the country, network, and the VLR used by the target phone.

Alternatively, if the surveillance actor already has access to the SS7 network under a leasing arrangement with a mobile network, they can perform the same HLR lookup, but without relying on an intermediary commercial HLR lookup service.

**Information Box 2: Cross Protocol Signaling Attacks**

3G vulnerabilities are particularly acute due to widespread address leasing arrangements,[10] though 4G networks can also assign and lease node addresses with the same effect. In some cases, actors will use 3G and 4G networks to simultaneously target the same user; these are referred to as "cross-protocol attacks."

The effect is twofold: first, the surveillance actors can directly request and receive geolocation information associated with the IMSI of the targeted device. Second, because the source address must be populated in signaling messages in order to route the message back to the source, it also leaves a fingerprint of the attack. This means that network firewalls operated by telecommunications providers can monitor the network from which the HLR lookup and location tracking messages were sent.

### 2.1.3. Domestic Threats—Innocent Until Proven Guilty

The risk of domestic location disclosure threats can sometimes be more concerning than those originating from foreign sources when third-parties are authorized by mobile operators to connect to their network. These can be particularly concerning in either low rule-of-law countries where domestic law enforcement or security agencies may abuse this access, or where state institutions in even high rule-of-law countries choose to exploit vulnerabilities in global telecommunications networks instead of working to actively secure and defend them.

Signaling firewalls used by telecommunications providers to prevent foreign operators, or surveillance actors, from illicitly querying the geolocation of their subscribers may be less effective against domestic threats. Specifically, if the signaling firewalls are not appropriately configured then attacks originating within the same network may be undetected because the activity—which is originating from within the operator's own network—is assumed to be trusted, and networks may not screen and block location tracking messages from sources within their own networks. The result is that the third-parties which are granted 3G and 4G addresses on home networks may, sometimes, have the ability to silently geolocate users without being noticed or filtered by the telecommunications provider.

In some countries, law enforcement and security agencies are allowed to connect directly to a home country network so that they can send location tracking messages domestically as well as internationally. In these cases, location tracking messages sent from that

10 Crofton Black, Stephanie Kirchgaessner, and Dan Sabbagh. (2020, December 16). Israeli spy firm suspected of accessing global telecoms via Channel Islands. *The Guardian.* https://www.theguardian.com/world/2020/dec/16/israeli-spy-firm-suspected-accessing-global-telecoms-channel-islands

domestic operator network address may be allowed to use networks in that country to track the location of users on other networks in-country or on foreign networks.

An example of the risks associated with state intervention of a telecommunications operator can be demonstrated by recent threat intelligence data showing location tracking attacks from the Vietnam mobile operator Gmobile, owned by GTel Mobile, which in turn is owned by the Vietnam Ministry of Public Security.[11] With a role of investigating national security matters, The Ministry of Public Security has been accused of various human rights violations including censorship and restrictions on internet freedom.[12]

From November 2022 to June 2023, five different SS7 GTs allocated to GTel/Gmobile were seen conducting surveillance operations targeting mobile users in African countries based on threat telemetry outputs from firewalls deployed in multiple mobile networks. Of the surveillance attempts seen from the data, a majority of the malicious signaling messages were associated with location disclosure.[13]

These conclusions emerge from data which is shown in Figure 4 and was derived from the Mobile Surveillance Monitor project, [14] which tracks surveillance activity from threat intelligence data sources. This data revealed that threats were detected and blocked by Cellusys[15] signaling network firewalls deployed at mobile operator networks. The charts show the distribution of various SS7 message operation types that were used by Gmobile in an attempt to track user locations from each of the source GT addresses which were, themselves, detected targeting phones in African mobile networks. As shown in the figure, various message types were used to attempt the location tracking operations. The technique of using different message types for location tracking is commonly used to try and either circumvent a signaling firewall or to enhance the chances of successfully geolocating the targeted devices.

11 Listed under Vietnam Enterprises Under the Ministry of Public Security (MPS): https://www.trade.gov/country-commercial-guides/vietnam-defense-and-security-sector

12 2022 Country Reports on Human Rights Practices: Vietnam (2022). U.S. Department of State. https://www.state.gov/reports/2022-country-reports-on-human-rights-practices/vietnam/

13 Mobile signaling telemetry data was sourced from Cellusys and analyzed by Mobile Surveillance Monitor, a threat intelligence project operated by the author Gary Miller.

14 Tracking Digital Privacy Threats With Intelligence: https://surveillancemonitor.org

15 Cellusys: https://www.cellusys.com

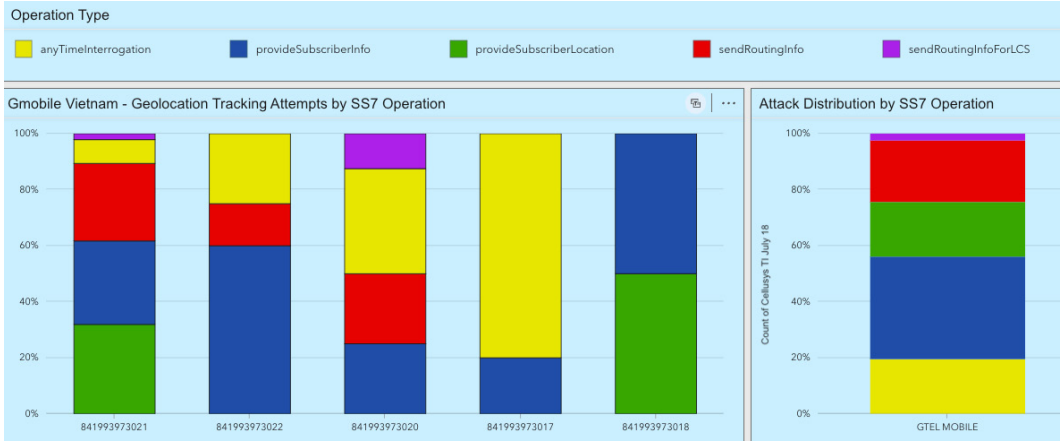



Figure 4: SS7 message types used by Gmobile Vietnam GT's to track user geolocation.

Gmobile was the only Vietnam network seen conducting targeted SS7 surveillance during this period of time. Given its ownership by the Ministry of Public Security the targeting was either undertaken with the Ministry's awareness or permission, or was undertaken in spite of the telecommunications operator being owned by the state.

## 2.2 Passive Attacks

Passive location attacks involve a domestic or foreign mobile network collecting usage or location information associated with a target mobile phone using collection devices installed in the network. The devices collect, and forward, communications and network data to a data warehouse or command and control facility which is operated by the surveillance actor.

### 2.2.1. Signaling Probes and Network Monitoring Tools

Signaling probes and network monitoring tools are typically placed into mobile networks by telecommunications companies for operational purposes, such as network trouble-shooting. These devices are generally placed in strategic network locations to capture network traffic at the user-level as it passes between network equipment. This process involves the probes ingesting raw signaling messages or IP traffic sent within a home network, or between the home and roaming partner networks where the user is currently registered. The network transactions are collected and provided to an upstream platform where they are processed and stored. Once in this platform, the messages can be aggregated to create operational Key Performance Indicators (KPIs) for analytics or saved in a format to trace user activity, such as a packet capture tool or analyzer such as Wireshark.[16] Because the probes intercept user signaling information they can track the general location of a mobile phone, even if the phone is not actively engaged in a voice call or data session.

16 Wireshark is a popular network analyzer tool, and is used to read and interpret captured network traffic.

## 2.2.2. Packet Capture Examples of Location Monitoring

The following figures (5 and 6) show examples of Packet Capture (PCAP) traces acquired from a mobile network. The traces are derived from an anonymous source to demonstrate how surveillance actors can extract location data from mobile signaling networks. The first two types of messages shown are Provide Subscriber Location (PSL) and Provide Subscriber Information (PSI). These are just two examples of the many types seen in location tracking operations. The final example seen in Figure 7 shows how a passive device capturing a user data session on the mobile network could reveal the location of the phone.

```
> Frame 2: 141 bytes on wire (1128 bits), 141 bytes captured (1128 bits)
> Message Transfer Part Level 2
> Message Transfer Part Level 3
> Signalling Connection Control Part
> Transaction Capabilities Application Part
v GSM Mobile Application
  v Component: returnResultLast (2)
    v returnResultLast
        invokeID: -50
      v resultretres
        v opCode: localValue (0)
            localValue: provideSubscriberLocation (83)
        v locationEstimate: a02e251fafad5400005507205a
            1010 .... = Location estimate: Ellipsoid Arc (10)
            0... .... = Sign of latitude: North (0)
            .010 1110 0010 0101 0001 1111 = Degrees of latitude: 3024159 (32.44571 degrees)
            1010 1111 1010 1101 0101 0100 = Degrees of longitude: -5264044 (-112.95414 degrees)
            Inner radius: 0
            .101 0101 = Uncertainty radius: 85
            Offset angle: 7
            Included angle: 32
            .101 1010 = Confidence(%): 90
            [Location OSM URI: https://www.openstreetmap.org/?mlat=32.44571&mlon=-112.95414&zoom=12]
          ageOfLocationEstimate: 0
          utranPositioningData: 404c660b40
        v cellIdOrSai: cellGlobalIdOrServiceAreaIdFixedLength (0)
            cellGlobalIdOrServiceAreaIdFixedLength: 13014072[redacted]
          sai-Present
```

Figure 5: PSL signaling message active location tracking example.

In the PSL message response, the GPS latitude and longitude coordinates of the phone location is disclosed in the message sent back to the source GT, which could be operated by a surveillance actor.

```
> Frame 4: 150 bytes on wire (1200 bits), 150 bytes captured (1200 bits) on interface unknown, id 0
> Message Transfer Part Level 2
> Message Transfer Part Level 3
> Signalling Connection Control Part
v Transaction Capabilities Application Part
  > end
v GSM Mobile Application
  v Component: returnResultLast (2)
    v returnResultLast
        invokeID: 1
      v resultretres
        v opCode: localValue (0)
            localValue: provideSubscriberInfo (70)
        v subscriberInfo
          v locationInformation
              ageOfLocationInformation: 0
            > vlr-number: 91617[redacted]
            v locationNumber: 03174[redacted]
                0... .... = Odd/Even: False
                ..00 0011 = Nature of address indicator: national (significant) number (national use) (3)
                0... .... = Internal Network Number indicator (INN): False
                ..01 .... = Numbering plan indicator: ISDN (telephony) numbering plan (ITU-T Recommendation E.164) (1)
                .... 01.. = Address presentation restricted indicator: presentation restricted (1)
                .... ..11 = Screening indicator: network provided (3)
                Address digits: 647[redacted]
                Country Code: New Zealand (64)
            v cellGlobalIdOrServiceAreaIdOrLAI: cellGlobalIdOrServiceAreaIdFixedLength (0)
                cellGlobalIdOrServiceAreaIdFixedLength: 0302162904d9dc
            v msc-Number: 91617[redacted]
                1... .... = Extension: No Extension
                .001 .... = Nature of number: International Number (0x1)
                .... 0001 = Number plan: ISDN/Telephony Numbering (Rec ITU-T E.164) (0x1)
              > E.164 number (MSISDN): 1647[redacted]
            sai-Present
```

Figure 6: PSI signaling message active location tracking example.

In Figure 6, an international roaming user with a phone number based in Toronto, Canada has been located with a PSI message while using a mobile network in New Zealand. This has the effect of exposing the phone geolocation at the Cell ID level. The location information of the user is encoded in the cellGlobalIdOrServiceAreaIdFixedLength parameter,[17] which is an octet string including the current MCC, MNC, Location Area Code (LAC),[18] and Cell ID. In effect, with the octet string in hand it is possible to geolocate the mobile device.

```
> Frame 1: 295 bytes on wire (2360 bits), 295 bytes captured (2360 bits)
> Ethernet II, Src: Cisco_48:11:27 (78:0c:f0:48:11:27), Dst: HewlettP_26:c1:ba (b8:83:03:26:c1:ba)
> Internet Protocol Version 4, Src: 69.[redacted] Dst: 216.[redacted]
> User Datagram Protocol, Src Port: 2123, Dst Port: 2123
v GPRS Tunneling Protocol V2
  > Flags: 0x48
    Message Type: Create Session Request (32)
    Message Length: 249
    Tunnel Endpoint Identifier: 0x00000000 (0)
    Sequence Number: 0x0030150b (3151115)
    Spare: 0
  > International Mobile Subscriber Identity (IMSI) : 310[redacted]6
  > MSISDN : 1623[redacted]
  > Mobile Equipment Identity (MEI) : 35909[redacted]
  v User Location Info (ULI) : TAI ECGI
      IE Type: User Location Info (ULI) (86)
      IE Length: 13
      0000 .... = CR flag: 0
      .... 0000 = Instance: 0
    > ULI Flags: 0x18, ECGI Present, TAI Present
    v Tracking Area Identity (TAI)
        Mobile Country Code (MCC): United States (311)
        Mobile Network Code (MNC): [redacted]
        Tracking Area Code: 0x01[redacted])
    v E-UTRAN Cell Global Identifier (ECGI)
        Mobile Country Code (MCC): United States (311)
        Mobile Network Code (MNC): [redacted]
        Spare: 0
      v ECI (E-UTRAN Cell Identifier): 13020[redacted]
          .... 0111 1100 0010 1100 1110 .... .... = eNodeB Id: 5086[redacted]
          .... .... .... .... .... .... 0110 1101 = CellId: 10[redacted]
  > Serving Network : MCC 311 United States, MNC 0[redacted]
  > RAT Type : EUTRAN (6)
```

Figure 7: user location and identifiable information revealed in mobile data sessions.

The packet capture shown in Figure 7 indicates that the IMSI, MSISDN, and IMEI of a mobile user has been revealed while attempting to establish a data session, as indicated by the GPRS Tunneling Protocol "Create Session Request" message. The request specifies the User Location Info (ULI), which provides the information necessary to derive the current global location of the user including the country, mobile network operator, base station, and Cell ID of registered user.

17 Defined in the mobile standards document 3GPP TS 23.003.

18 Defined in the mobile standards document 3GPP TS 24.008.

# 3. Case Studies and Statistics

The following case study reveals a tactic used to track the location of targeted users on a mobile network. It shows how a state sponsored surveillance actor can monitor the location of international traveler phones outside of their country.

## 3.1 Case Study - Saudi Arabia Tracking Travelers in the United States

*The Guardian* revealed a particularly notable example of likely state-sponsored geolocation tracking when it exposed activities which were likely conducted by the Kingdom of Saudi Arabia. The outlet reported that the country allegedly tracked the movements of individuals who traveled from Saudi Arabia to the United States and who were subscribers to Saudi telecommunications providers by exploiting the SS7 network.[19]

This surveillance was carried out by sending large volumes of Provide Subscriber Information (PSI) messages targeting the mobile devices that were roaming into the United States. These messages were issued by Saudi Arabia's largest three mobile operators, Saudi Telecom Company (STC), Mobily (Etisalat), and Zain KSA. When a network receives a PSI message, it will respond with the Cell ID (CID) of the targeted device and the CID, in turn, can uniquely identify the base station to which the device is registered at any given point. In effect, the United States network processed the PSI messages which had the effect of exposing the geolocation of the phones in the United States to the surveillance actors in Saudi Arabia. Surveillance actors can link the CID with a CID database to identify the GPS coordinates of the Cell ID. In aggregate, then, any PSI messages allowed into the network acted as a lynchpin to identify individuals' geolocation at the time of the surveillance and the duration of the targeted persons' travels in the United States. This would have had the effect of revealing the mobility patterns of residents of Saudi Arabia in the United States. This operation is described in the figure below.

19 Stephanie Kirchgaessner. (2020). Revealed: Saudis suspected of phone spying campaign in US. *The Guardian.* https://www.theguardian.com/world/2020/mar/29/revealed-saudis-suspected-of-phone-spying-campaign-in-us

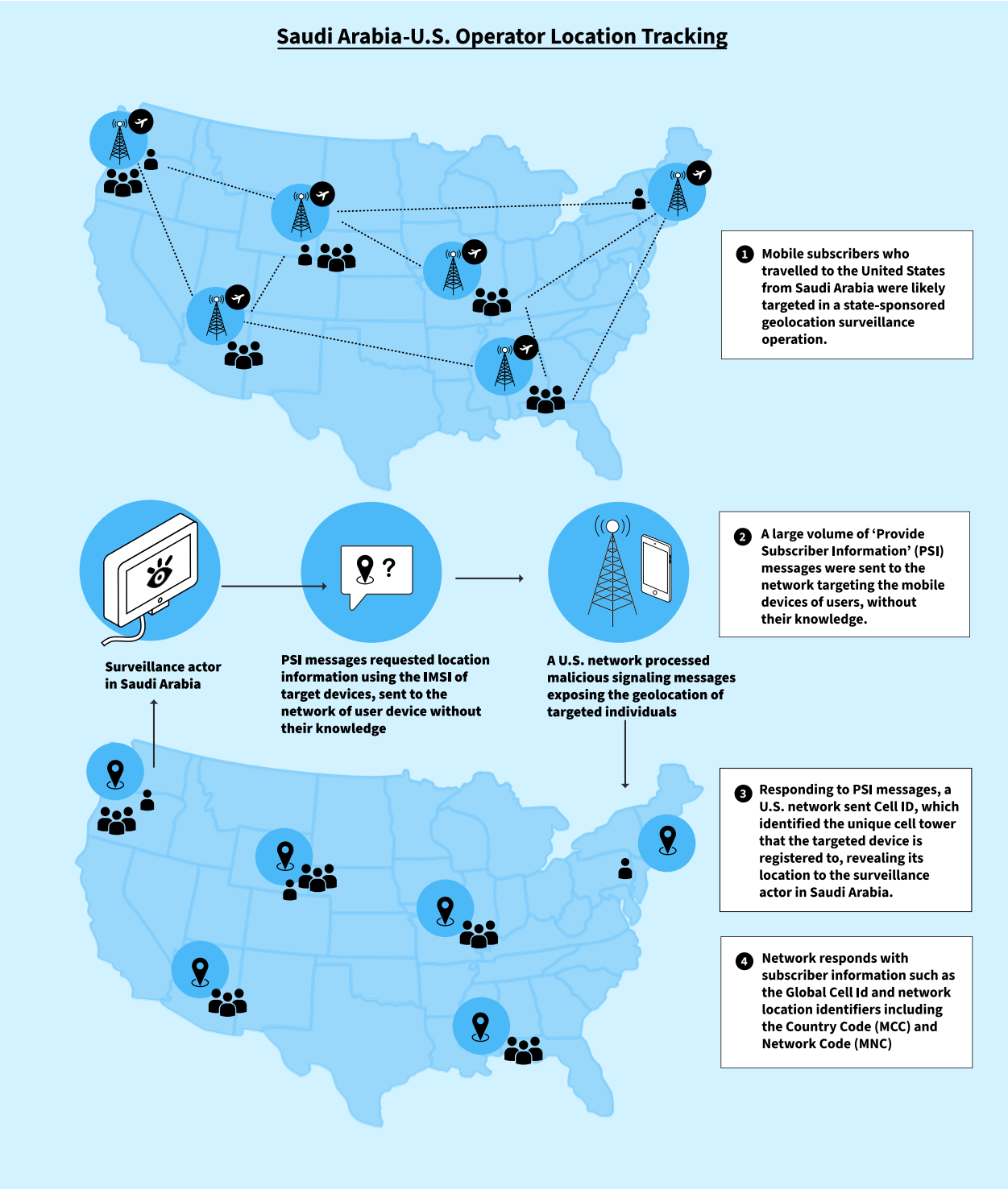



Figure 8: Location tracking of Saudi Arabian travelers in the United States.

The article noted that these messages were sent to each targeted Saudi phone many times per hour and that the anomalous activity could not be explained or justified under expected network operating procedures.

The transactions shown in Table 1 were aggregated over October to December 2019. They reveal the number of PSI messages that were sent from the three Saudi Arabia mobile operators to a specific United States mobile network, targeting IMSIs of Saudi phones

roaming on that network. The total IMSI count is the number of unique phones from the roaming partner seen on the network during the same timeframe.[20]

| Roaming Partner Name | MCC, MNC | PSI Transactions | Total IMSIs |
|---|---|---|---|
| Saudi Telecom Company (STC)-SAUAJ | 420,01 | 4,741,919 | 32,536 |
| Etihad Etisalat Mobily-SAUET | 420,03 | 2,821,709 | 11,362 |
| Zain KSA-SAUZN | 420,04 | 417,412 | 3,658 |
| **Total** | | **7,981,040** | **47,556** |

Table 1: Saudi Arabia location tracking to United States mobile operator — Oct-Dec 2019

Data in Table 2 calculates the total number of tracking messages which were received from Saudi Arabia network operators during a 24-hour period, broken into hourly segments. Based on these single day statistics, each mobile phone was geolocated approximately every 11 minutes.

| Event Date | PSI Transactions | Total IMSIs | Successful IMSIs | Requests Per Phone |
|---|---|---|---|---|
| 29 Nov, 2019 00 hr | 1750 | 265 | 262 | 6.60 |
| 29 Nov, 2019 01 hr | 1469 | 242 | 241 | 6.07 |
| 29 Nov, 2019 02 hr | 1491 | 223 | 221 | 6.69 |
| 29 Nov, 2019 03 hr | 1469 | 214 | 212 | 6.86 |
| 29 Nov, 2019 04 hr | 1199 | 209 | 207 | 5.74 |
| 29 Nov, 2019 05 hr | 1441 | 250 | 247 | 5.76 |
| 29 Nov, 2019 06 hr | 1231 | 222 | 222 | 5.55 |
| 29 Nov, 2019 07 hr | 1249 | 270 | 266 | 4.63 |
| 29 Nov, 2019 08 hr | 1125 | 229 | 229 | 4.91 |
| 29 Nov, 2019 09 hr | 1523 | 306 | 303 | 4.98 |
| 29 Nov, 2019 10 hr | 1260 | 290 | 288 | 4.34 |
| 29 Nov, 2019 11 hr | 1358 | 304 | 304 | 4.47 |
| 29 Nov, 2019 12 hr | 1325 | 298 | 297 | 4.45 |
| 29 Nov, 2019 13 hr | 1677 | 368 | 367 | 4.56 |
| 29 Nov, 2019 14 hr | 1567 | 380 | 378 | 4.12 |
| 29 Nov, 2019 15 hr | 1684 | 406 | 403 | 4.15 |
| 29 Nov, 2019 16 hr | 2191 | 443 | 439 | 4.95 |
| 29 Nov, 2019 17 hr | 2560 | 507 | 504 | 5.05 |
| 29 Nov, 2019 18 hr | 2426 | 484 | 484 | 5.01 |
| 29 Nov, 2019 19 hr | 2368 | 467 | 465 | 5.07 |
| 29 Nov, 2019 20 hr | 2363 | 422 | 417 | 5.60 |
| 29 Nov, 2019 21 hr | 2196 | 407 | 402 | 5.40 |
| 29 Nov, 2019 22 hr | 2397 | 409 | 400 | 5.86 |
| 29 Nov, 2019 23 hr | 2387 | 354 | 348 | 6.74 |

Table 2. Saudi Arabia single day PSI location tracking targeting a United States mobile operator — Nov 29, 2019

20 In Table 1, the total unique IMSIs were observed over a three month timeframe. In Table 2, the total unique IMSIs were observed every hour.

Typically, PSI signaling messages from foreign networks are blocked by a network firewall. This defensive measure is intended to prevent unauthorized geolocation lookups. However, this did not occur in this case study because the targeted mobile phones were roaming on a United States network by their respective Saudi Arabia home networks. In contrast, had the messages been sent from a foreign network to a subscriber who did not belong to that same network, such as if a British operator had queried the same Saudi Arabian users while they roamed on United States networks, these messages should have been blocked.

The reason for the blanket surveillance outlined in this case study is not entirely clear. Nevertheless, we can conclude that this was likely state-sponsored activity intended to identify the mobility patterns of Saudi Arabia users who were traveling in the United States.

## 3.2. Current Statistics – Geolocation Tracking vs Other Threat Types

The failure of effective regulation, accountability, and transparency has been a boon for network-based geolocation surveillance. The figures below provide some context and offer a current view of the global mobile network landscape.

While some industry experts believe that mobile operators use firewalls to block a majority of geolocation tracking, with the effect of limiting the utility of using traditional SS7 surveillance methods, statistics provided by Mobile Surveillance Monitor indicate that geolocation disclosure is the most prevalent network threat type by a wide margin.

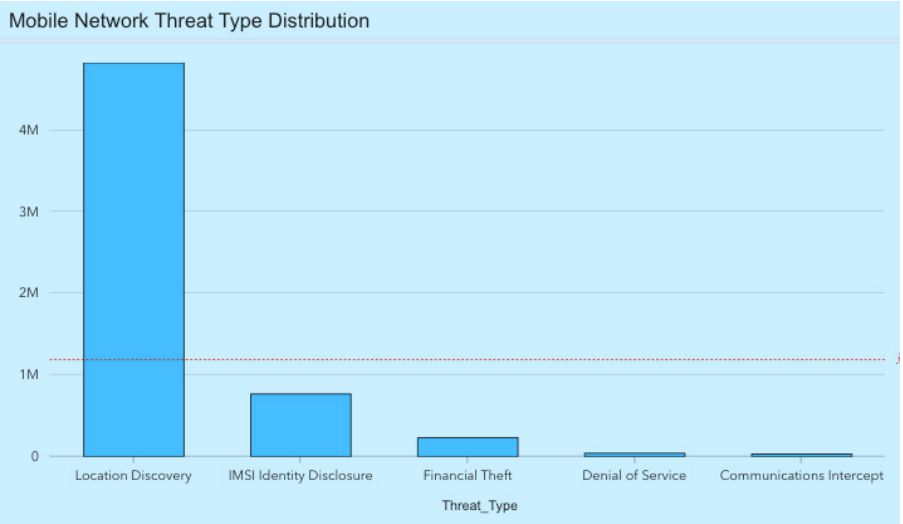



Figure 9: Network attack distribution by threat type.

Mobile Surveillance Monitor has also identified that approximately 171 networks from 100 source countries have sent targeted geolocation tracking messages to mobile operator networks located in Africa during the first half of 2023, indicating continued widespread

attempted SS7 surveillance activity. The top malicious networks from which these messages were sourced in 2023 are shown in Figure 10. The volume disparity between the top two network sources from the rest of the list indicates that GT's from Millicom Chad and Celtel DRC are likely attempting to harvest user location data. The activities by these GTs stand in contrast to other sources, such as Fink Telecom Services, which was exposed for selling targeted commercial phone surveillance services in the report "Ghost in the network" by the investigative journalism firm Lighthouse Reports.[21]

Network Threat Sources - Location Disclosure

| Source Country | Source Network | Sum of Count SUM |
|---|---|---|
| Chad | MILLICOM CHAD | 3,623,713 |
| Congo DRC | CELTEL DRC | 969,960 |
| Zimbabwe | TELECEL ZIMBABWE | 68,498 |
| India | BHARAT SANCHAR NIGAM CELONE | 53,436 |
| Mozambique | MOCAMBIQUE CELULAR MOZAMBIQUE | 35,614 |
| Iceland | NOVA | 16,979 |
| Saudi Arabia | MOBILY ETIHAD ETILSAT | 5,478 |
| Jamaica | DIGICEL JAMAICA | 4,884 |
| Uganda | UGANDA TELECOM | 3,784 |
| Malaysia | CELCOM AXIATA BERHAD | 3,773 |
| Sweden | FINK TELECOM SERVICES | 3,387 |
| Italy | TELECOM ITALIA MOBILE | 3,358 |
| Saudi Arabia | ZAIN | 3,141 |
| Ghana | MILLICOM GHANA | 2,699 |

Figure 10: SS7 network geolocation disclosure threats — ranking by source network.

21 Ghost in the network — Lighthouse Reports. (2023). *Lighthouse Reports.* https://www.lighthousereports.com/investigation/ghost-in-the-network/.
See also: Crofton Black and Omar Benjakob. (2023, May 14). How a secretive Swiss dealer is enabling Israeli spy firms. *Haaretz.com*. https://www.haaretz.com/israel-news/security-aviation/2023-05-14/ty-article-magazine/.highlight/global-surveillance-the-secretive-swiss-dealer-enabling-israeli-spy-firms/00000188-0005-dc7e-a3fe-22cdf2900000

# 4. Incentives Enabling Geolocation Attacks

From an outsider's perspective, securing the perimeters of mobile networks would appear to be a straightforward process. Enterprises routinely place rigid security controls and filters at the edges of their networks using a firewall, so why would the same approach not be applied to mobile networks? And why not follow industry standards and widely accepted network security guidelines for mobile networks? In practice, security in mobile telecommunications is not as clear cut as it should be. A deeper look at some of the drivers in this critical infrastructure space can expose some controls which are more easily enforced than others.

Whereas domestic roaming policies can be mandated by the regulatory agencies of each country, such as the CRTC Telecom Regulatory Policies[22] or the UK Telecommunications Security Act,[23] international roaming is based on independent bidirectional negotiations and addressing information exchanges which are not regularly monitored or updated. At the industry level, technical interoperability and commercial aspects are facilitated by the GSMA Wholesale Agreements and Solutions (WAS) Working Group,[24] and the interoperability and addressing information that is exchanged between operators is maintained in documents called IR.21[25] and exchanged electronically using the Roaming Agreement Exchange (RAEX).[26] The network information in the IR.21 includes assignments of GT addresses or ranges to specific equipment in the operator network, with the purpose of informing each roaming partner for routing, interoperability, and security.

In the mobile telecommunications industry, the lack of strict requirements to maintain an inventory of address assignments to core network equipment has resulted in insufficient diligence by mobile operators around the world in updating their roaming address information. The effect of creating ambivalence about relying on RAEX and the network addresses listed in IR.21 ultimately reduces its reliability as a mobile security resource. The lack of an authorized and validated list of roaming partners with verified network information runs counter to the fundamentals of building a zero trust security posture.[27] If a system of strict compliance were properly maintained by each operator around the world, networks could use it to create better perimeter security controls.

---

22 Canadian Radio-television and Telecommunications Commission. (2021). Review of mobile wireless services. https://crtc.gc.ca/eng/archive/2021/2021-130.htm

23 Telecommunications (Security) Act 2021. (2021). https://www.legislation.gov.uk/ukpga/2021/31/enacted

24 Wholesale Agreements and Solutions Group — Working Groups. (2023, June 15). *Working Groups.* https://www.gsma.com/aboutus/workinggroups/wholesale-agreements-and-solutions-group

25 IR.21 GSM Association Roaming Database, Structure and Updating Procedures

26 RAEX IR.21 Management System – RoamSmart. (2019, June 18). *RoamSmart*. https://roam-smart.com/raex-ir-21-management-system/

27 According to the US National Security Telecommunications Advisory Committee (NSTAC), Zero Trust is described as "a cybersecurity strategy premised on the idea that no user or asset is to be implicitly trusted." https://www.cisa.gov/resources-tools/groups/presidents-national-security-telecommunications-advisory-committee/presidents-nstac-publications

## 4.1. Economic Enablers

As mobile operators deployed analytics to monitor traffic exchanged between their roaming partner networks, it quickly became apparent that the trust model was broken. Millions of unauthorized messages from foreign networks were discovered[28] and this drove the industry to develop requirements for a signaling network firewall. While security guidelines and specifications have been designed and released by the GSMA's Fraud and Security Group (FASG)[29] there are, as of writing, no universal accountability or enforcement mechanisms. It is up to each respective mobile network operator—and perhaps their domestic telecommunications regulators and cybersecurity authorities—to decide whether, and how, they should protect their networks and subscribers.

Attention to unauthorized signaling messages became more acute following the presentation of the Carmen Sandiego Project at Blackhat 2010[30] and the presentation by Tobias Engel in 2014 at the Chaos Communication Congress.[31] The former revealed points of security vulnerability and the latter showed how basic software and SS7 network connectivity could enable limitless surveillance operations.

It was those presentations, and accompanying media attention, that drove vendors to begin developing and selling signaling firewalls. The adoption of these firewalls was often delayed, however, because some mobile network operators had already been leasing their networks to third-party Value Added Service (VAS) providers. This meant they were disincentivized to adopt a security posture which might negatively impact these business relationships and accompanying revenue. It was only after the GSMA finalized SS7 network security guidelines in 2017 that network operators began to deploy firewalls. However, by that time surveillance actors had been leasing GT's and deployed capabilities in mobile networks around the world, with the effect of mitigating some of the protections that signaling firewalls were meant to provide.

## 4.2 Industry Enablers

The mutually beneficial revenues associated with the vibrant GT leasing business has provided mobile networks around the world with significant sources of revenue. As of May 2023, network providers such as the Swedish telecommunications provider Telenabler AB, shown in Figure 11, continued to openly promote SS7 Global Title Leasing as a business offering.

---

28 Many discovered messages provided a phone's location, active calls, and more to the party that initiated the query.

29 Fraud and Security Group — Working Groups. (2023, March 23). *Working Groups.* https://www.gsma.com/aboutus/workinggroups/fraud-security-group

30 The Carmen Sandiego Project. *Blackhat* (2010, July 4). https://media.blackhat.com/bh-us-10/whitepapers/Bailey_DePetrillo/BlackHat-USA-2010-Bailey-DePetrillo-The-Carmen-Sandiego-Project-wp.pdf

31 Schedule 31. Chaos Communication Congress. (n.d.). https://fahrplan.events.ccc.de/congress/2014/Fahrplan/events/6249.html


Since Telenabler belongs to Limitless Mobile Group, a mobile network operator (MNO) in the US, it has an access to dedicated mobile network codes, Global Titles (GT) and number ranges, as well as roaming agreements with +150 mobile operators in +115 countries,

Therefore, Telenabler has the ability to provide Global Titles (GT) to customers requiring GTs for routing.

GTs can be provided for individual nodes, such as an HLR, MSC, VLR, IN or SMSC or a whole network where a customer wishes to maintain all aspects of call control. To ensure speed to market, utilises IP / SIGTRAN for connectivity.

Figure 11: Telenabler Global Title leasing web page.

The point of GT leasing risks is made clear by examining GT's assigned to Telenabler by the Swedish Post and Telecom Authority (PTS) as shown in Figure 12 below. The outlined number range identifies a specific block of 10,000 numbers allocated to Telenabler, where a subset of those numbers were seen as the source of location tracking operations.

PTS e-tjänster

Svenska | English

Search in numbering plans

**Numbering plan** National Numbering Plan - Subscriber Numbers (E.164)
**Operator** Telenabler AB
**NDC** 76
**Status** Assigned
**Service type** Mobile telephony services
**Enter date** From To

Clear Search

The table shows the first **200** lines of 10. Scroll down this page to load additional lines.

Export to Excel Export to Csv Export to Json

| NDC | Number from | Number to | Nrl. | No. | Operator | Status | Service type | Created | Changed date | Decision date | Reference no. | Ported |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 76 | 4700000 | 4709999 | 9 | 10000 | Telenabler AB | Tilldelad | Mobiltelefonitjänster | 2010-07-02 | 2014-03-31 | 2014-03-31 | 14-3325 | Show |
| 76 | 4710000 | 4719999 | 9 | 10000 | Telenabler AB | Tilldelad | Mobiltelefonitjänster | 2010-07-02 | 2014-03-31 | 2014-03-31 | 14-3325 | Show |
| 76 | 4720000 | 4729999 | 9 | 10000 | Telenabler AB | Tilldelad | Mobiltelefonitjänster | 2010-07-02 | 2014-03-31 | 2014-03-31 | 14-3325 | Show |
| 76 | 4730000 | 4739999 | 9 | 10000 | Telenabler AB | Tilldelad | Mobiltelefonitjänster | 2010-07-02 | 2014-03-31 | 2014-03-31 | 14-3325 | Show |
| 76 | 4740000 | 4749999 | 9 | 10000 | Telenabler AB | Tilldelad | Mobiltelefonitjänster | 2010-07-02 | 2014-03-31 | 2014-03-31 | 14-3325 | Show |
| 76 | 4750000 | 4759999 | 9 | 10000 | Telenabler AB | Tilldelad | Mobiltelefonitjänster | 2010-07-02 | 2014-03-31 | 2014-03-31 | 14-3325 | Show |
| 76 | 4760000 | 4769999 | 9 | 10000 | Telenabler AB | Tilldelad | Mobiltelefonitjänster | 2010-07-02 | 2014-03-31 | 2014-03-31 | 14-3325 | Show |

Figure 12: Swedish number range assigned to telenabler seen as the source of location tracking operations.

Four of the telephone numbers assigned to Telenabler were detected attempting geolocation surveillance up until June 29, 2023 as seen in Figure 13 below. Consistent with many surveillance actors, the source numbers used as GT's assigned to Telenabler are seen using multiple SS7 signaling message operation types, as seen in Figure 13. While different types of signaling messages were used, each had the objective of disclosing the geolocation of a target user's phone.

Mobile Network Threat Summary

| Source Network | Source Node | Operation | Sum of Count (SUM) |
|---|---|---|---|
| TELENABLER AB | 467647531812 | anyTimeInterrogation | 10 |
| | | provideSubscriberInfo | 383 |
| | | provideSubscriberLocation | 116 |
| | | sendRoutingInfo | 37 |
| | 46764753182 | anyTimeInterrogation | 15 |
| | | provideSubscriberInfo | 2 |
| | 46764753183 | anyTimeInterrogation | 27 |
| | | provideSubscriberInfo | 33 |
| | | provideSubscriberLocation | 17 |
| | | sendRoutingInfo | 4 |
| | 467647531851 | anyTimeInterrogation | 35 |
| | | sendRoutingInfo | 6 |
| | | | **Total** 685 |

Figure 13: Location surveillance threat events attributed to telenabler leased GTs.

GT leasing rates have been removed from most websites due to the perceived negative implications of making networks available for a cost. However, the fees have traditionally been in the $5,000-$15,000 per month range.[32] Global Title lessors assert that there are a number of benefits associated with their commercial engagements. First, they assert they can offer SS7 network access to third parties without the resources to obtain number ranges. Second, they claim they can offer access to MVNOs and Global SIM service providers with a core network when they may not otherwise be able to obtain them due to local regulatory requirements. And, third, they assert that by leasing GTs they can offer global connectivity to messaging and value added service providers to mobile networks with low barriers to entry. Regardless of the extent to which these benefits are realized they also open the door to malicious operators to make GTs available to surveillance actors to undertake surreptitious geolocation surveillance.

32 Global Title leasing (fixed price per month). (n.d.). Freelancer. https://www.freelancer.com/projects/network-administration/global-title-leasing-fixed-price

**Information Box 3: The Future of Global Title Leasing**

The practice of third-party network leasing by foreign mobile networks remains an unregulated and opaque practice in the mobile industry. Network operators cannot determine which networks and which addresses have been leased to third-parties. Further, they have no ability to check the legitimacy of those third-parties or whether they have additional subleasing arrangements with surveillance actors such as criminal groups or state-sponsored entities. As a result, there is little accountability in the event a foreign network operator knowingly or unknowingly sells network access to a surveillance actor who is targeting mobile users.

The current status quo, however, may be changing. In March 2023, the GSMA released the document entitled "Global Title Leasing Code of Conduct."[33] The document lists a number of issues and concerns related to the commercial practice of GT leasing, which we have detailed in this report, and goes on to state that "GT leasing has evolved through the emergence of commercial relationships that were built up over time without any industry standardization, specifications, or recommendations. As a result, there is no agreed framework governing the relationships between GT Lessors and the networks to which they are interconnected."[34] The document proceeds to state very clearly that, "GSMA strongly advises that GT Leasing should not be used."[35]

While this is only a recommendation, it represents a significant shift in the official position of the GSMA and makes clear that the Association is at least willing to alter its policy positions. However, it remains unclear whether this will affect the third-party network reselling business that directly results in millions of yearly location tracking events seen on the world's mobile networks.

The GSMA Global Title Leasing Code of Conduct, discussed in Information Box 3, assigns legal liability to the GT Lessor in the event of malicious signaling traffic that causes harm to the target operator. By placing legal liability on the GT lessor that enables malicious cyber activities, such as geolocation tracking, it is difficult to conceive that the benefits to the selling operator outweigh the security, operational, and financial risks. However, telecommunications regulation is a state affair and, as such, it can be challenging to develop uniform cross-national industry policies or mandates that restrict such activities. Consequently, each respective operator is required to maintain strict security controls and firewalls to protect their network and subscribers.

Historically speaking, the impact of industry organizations to encourage restrictions on GT leasing have proven insufficient. While industry working groups such as the GSMA FASG have been formed to create guidelines meant to encourage mobile network operators to deploy security controls, they do not provide enforcement, publicly disclose attack statistics, or offer relevant threat intelligence with active operator participation. The GSMA

33 GSM Association Official Document FS.52 Global Title Leasing Code of Conduct

34 GSMA Official Document FS.52, Section 2.4 Issues and Concerns with GT Leasing

35 GSMA Official Document FS.52, Section 3 Global Title Leasing Use Cases

provides the Telecommunication Information Sharing and Analysis Center (T-ISAC) as a threat intelligence information sharing hub with the intention of distributing information regarding cybersecurity attacks. However, the service is only available to GSMA members and access to this information thus requires an annual financial contribution. In 2023, this contribution was between $14,306-$136,460, effectively serving as a payment gate to access information of benefit to the security and privacy of civil society.[36]

Mobile operators can directly engage the offending mobile operator whose networks are seen as the source of malicious signaling messages targeting their subscribers. This process traditionally involves the targeted mobile operator contacting the operator that was the source of the malicious signaling messages and giving them notice that if they do not see any responsible mitigation that the targeted operator will block subsequent traffic sent by the offending source GT address. However, if the targeted network operator blocks signaling messages from the source operator GT the surveillance actor can simply shift to sending these messages using another GT leased from the same operator or others from which they have leasing arrangements. This process could continue, where the attacker cycles through the available leased GT's until they are exhausted. Alternatively, attacks may be spread evenly over multiple networks across the world as a detection avoidance technique. This process ends up being an operationally intensive game of whack-a-mole where the defending operator simply gives up or configures the firewall to block the message types used in the attacks.

## 4.3. Government Enablers

In addition to some network operators being financially motivated to engage in leasing arrangements to surveillance actors, and the industry being largely unable to self-regulate, governments have generally taken a "hands off" approach to mobile network security. This may be linked to a lack of clear authorities conferred on telecommunications regulators, to assuming that mobile operators are best situated to solve security issues in their networks and, in other situations, to some government agencies benefitting from mobile network vulnerabilities and the state of weak operator security protocols.

In the first case, some domestic regulators are starting to take more active roles in demanding mobile network security standards. Critical infrastructure legislation is being passed and cybersecurity agencies are becoming more active in requiring telecommunications operators to provide details of how they secure their systems.[37] It remains to be seen, however, whether the wave of legislation that is being passed will necessarily

36 See: Membership Categories & Contributions — Membership. (2023, March 20). Membership. https://www.gsma.com/membership/membership-categories-contributions/

37 See: UK Telecommunications (Security) Act 2021, UK (DRAFT) Telecommunications Security Code of Practice

lead to effective government action or if, instead, it will just provide a range of powers and tools which governments are either ill-prepared to use or which could lead to insufficiently accountable government interference in telecommunications networks.[38]

In the second case, as states become more assertive in the kinds of security that telecommunications operators must adopt, the telecommunications operators can push back. They might oppose new government activity on the basis that proposed standards and requirements are overly intrusive, generally unneeded, or are simply inappropriate to the contemporary threat environment. In countries such as Canada there have long been voluntary forums wherein mobile operators and the government establish high-level standards that are accompanied by security review processes by government agencies.[39] Such measures may be insufficient given the current state of network insecurity.

In the third case, and perhaps more ominously, intelligence and security agencies that rely on mobile networks for surveillance may balk at the idea of heightening domestic telecommunications networks' security postures. They may also have an upper hand when it comes to determining what kinds of security elements are most appropriate, on the basis that they can effectively veto cybersecurity solutions that would impede their abilities to conduct surveillance domestically and abroad. While intelligence and security agencies may be most likely to understand how to exploit telecommunications networks for geolocation tracking, policymakers should also be mindful of the potential for law enforcement agencies to similarly misuse access to telecommunications networks, particularly in cases where domestic law enforcement agencies have a history of inappropriately exercising their powers absent suitable oversight and judicial authorization.

38 Christopher Parsons. (2022). "Cybersecurity Will Not Thrive in Darkness: A Critical Analysis of Proposed Amendments in Bill C-26 to the Telecommunications Act," *Citizen Lab*. Available at: https://citizenlab.ca/2022/10/a-critical-analysis-of-proposed-amendments-in-bill-c-26-to-the-telecommunications-act/

39 Canadian Security Telecommunications Advisory Committee (CSTAC). (2020, June 30). https://ised-isde.canada.ca/site/spectrum-management-telecommunications/en/learn-more/committees-and-stakeholders/committees-and-councils/canadian-security-telecommunications-advisory-committee-cstac

# 5. Geolocation Tracking in 5G Networks and Unimplemented Defensive Measures

Surveillance actors have an ongoing interest in mobile networks and so they will adapt their methods according to the capabilities of the target network. While mobile telecommunications technologies and standards continuously evolve, many of the underlying principles and functionalities of the network architecture and surveillance methodologies remain the same.

**Information Box 4: Equivalent Signaling Message Types Used to Query Mobile Device Location**

In the case of user location lookups, each of these messages perform a similar action and could be exploited by an adversary; an adversary could even use all of these vectors simultaneously to target a single user if telecommunications operators expose these vectors as a result of how they have configured their networks.

| Network Type | Sending Node | Example Message |
|---|---|---|
| 2G/3G SS7 | HLR | MAP_Provide-Subscriber-Information (PSI) |
| 4G Diameter | HSS | Diameter Insert_Subscriber_Data_ Request (IDR) |
| 5G | UDM | Namf_Location_ ProvideLocationInformation (NPLI) |

Given the historical exposure of users to location tracking by adversaries, and the emergence of new services in 5G such as connected cars, smart homes, smart grids, and healthcare, it is critical that mobile network operators take a holistic and all-encompassing approach to protecting their networks if they are to limit the vulnerabilities which surveillance actors will otherwise exploit and abuse.

## 5.1. Subscriber Identity Privacy Enhancements

New security features which are available in the 5G standards take a significant step towards preventing network-based location surveillance. Whereas 3G and 4G networks use the IMSI as the user network identity, which has been exposed to adversaries and obtained over the years to conduct geolocation tracking attacks, 5G provides privacy enhancements. These enhancements have the ability to obfuscate the network identity

of the user and their device, and they come in the form of the following identifiers:

- **Subscription Permanent Identifier (SUPI) -** The globally unique identifier that is allocated to each 5G subscription
- **Subscription Concealed Identifier (SUCI)** - The encrypted equivalent of the SUPI that includes the Mobile Country Code (MCC) and Mobile Network Code (MNC), and the Mobile Subscription Identity Number (MSIN)
- **Globally Unique Temporary Identifier (5G-GUTI)** - The temporary identifier used in 5G networks to identify a mobile device and its associated subscription information

Implementing security features, however, is highly dependent on telecommunications operators adopting correct network configurations and taking advantage of the available 5G security features. There is a risk that some operators may not adopt these configurations on the premise that doing so increases the costs of deploying 5G infrastructure. Moreover, users have no ability to determine whether available privacy or security measures have been implemented. This customer-harmful business judgment on implementing privacy or security features should be avoided on the basis that, in doing so, businesses may be placing themselves in legal or regulatory jeopardy should individuals seek recompense for a failure to adequately protect their privacy, or regulators should impose fines on companies that have deliberately failed to protect their customers' personal information.

## 5.2. International Signaling and Interconnect Security Enhancements

The ability for foreign networks to target international users with signaling messages to reveal geolocation constitutes the most prevalent known attacks on mobile networks. Despite this being well known within the telecommunication industry the question remains as to whether operators are protecting their customers from these threats.

In fully-compliant, cloud-native 5G deployments,[40] international roaming signaling messages transit foreign networks with a new interface called N32 and use a network function called the Security Edge Protection Proxy (SEPP). This function was introduced into the 5G network architecture to add protection to the historically vulnerable communication between foreign network operators. The SEPP provides much needed encryption, integrity, and authentication at the border edge between roaming networks.

However, to provide privacy protection, networks on both ends of the roaming interface must implement the SEPP function. Getting all roaming partners to implement SEPP may

40 Fully-compliant refers to the 3GPP 5G Standalone (SA) defined in Technical Specification 29.573 (TS 29.573)

be extremely challenging; of the 351 network operators reported to have launched 5G services, only 41 have launched 5G cloud-native architectures according to the Global Mobile Suppliers Association (GSA) as of April 2023.[41] The remaining 310 operators are still using the Non-Standalone Architecture (NSA) for 5G, which lets mobile operators bypass the SEPP feature in 5G roaming while still providing the improved speed and reduced latency benefits of the 5G radio access network.

According to interviews with telecommunications security vendors at the Mobile World Congress (MWC) conference in March 2023,[42] only a handful of operators have deployed SEPP, let alone are actually using it. The effect is that many operators are not integrating the security and privacy benefits of the 5G standards when they are deploying 5G networks.

Many network vulnerabilities are specific to a given mobile network operator's implementation of telecommunications standards. However, given that many operators have shown a willingness to sell access to third-parties, there is a serious concern that surveillance actors will have software code in place to probe and test the integrity of foreign 5G networks. This will let surveillance actors adjust their tactics, techniques, and procedures for various network type vulnerabilities across each target network implementation. Historically, surveillance actors have quickly learned to modify their attacks to disguise traces and circumvent firewalls, and the slow pace of operator security deployments reduce the challenge that such actors will have in finding and exploiting obvious vulnerabilities.

The slow pace of operator security deployments over the most vulnerable attack vectors should be a wake up call to country regulators. To counter attacks quickly, adherence to 5G security guidelines and standards are imperative, in addition to adequate tools for threat detection. Without these measures, the ways in which 5G networks have been deployed may only be marginally better at protecting users from surveillance actors' attacks than the prior 3G and 4G networks, if at all.

41 GSA — 5G Public-Networks April 2023 Summary Report https://gsacom.com/paper/public-networks-april-2023-summary-report/

42 HardenStance Briefing — MWC23: Taking Stock of Telco Security https://www.hardenstance.com/wp-content/uploads/2023/03/HardenStance-Briefing-MWC23-Taking-Stock-of-Telco-Security-FINAL.pdf

# 6. Conclusion

Based on historic, current, and forward-looking assessments of mobile network security, geolocation surveillance should continue to be of significant concern to the public and policymakers. Exploitable vulnerabilities exist in 3G, 4G, and 5G network architectures and are expected to remain, absent forced transparency that exposes bad practices, and accountability measures that compel operators to correct such issues. If anything, the availability of all three network types provides multiple options for surveillance actors. If nation states and organized crime entities can actively monitor the location of mobile phones domestically or in foreign countries, then such vulnerabilities will continue to represent a security risk to the safety of not only at-risk groups, but also corporate staff as well as military and government officials.

The past four years reveal that surveillance originates from networks operating within nations with high internet freedom rankings, small remote island countries, and ostensibly neutral countries. Current vulnerabilities of mobile networks are systematically exploited as a source of intelligence gathering or espionage by surveillance actors, law enforcement, and organized crime groups who exploit vulnerabilities for their own purposes. Threat activity that is emergent from small Caribbean countries, as well as attacks from eastern European and African countries, point to widespread abuse of many telecommunications networks' Global Title leasing arrangements.

In light of the existent threats, what can be done? While this report does not offer comprehensive policy recommendations or technical suggestions, there are a series of interventions that should be prioritized.

First, attacks which often occur during international travel suggest the likelihood of third-parties sharing private user IMSIs. There should be active efforts by law enforcement and security services to prevent trafficking in such information, such as through the dark web.

Second, network and other third-party service providers, such as those who provide IPX and inter-carrier billing settlement, should be required to encrypt the unique details of a phone's IMSI and its accompanying mobile data files. Such activities should be accompanied by a strict and regular schedule of compliance audits. These protection and accountability measures would prevent malicious actors within the networks from illicitly monetizing or otherwise leveraging such retained information. Such audits might be undertaken by data protection authorities, privacy commissioners, telecommunications regulators, or consumer rights regulators.

Third, the prospect of inappropriately allowing third-party access to the private IPX network, or brokering information it obtains when exchanging signaling traffic, raises the likelihood for significant malicious surveillance capability.[43] Specifically, surveillance operators could connect and monitor traffic from international signaling hubs between foreign networks and play a key role in the ability to execute these attacks. Telecommunications, cybersecurity, data privacy, and consumer rights regulators should all assess whether mobile participants in their jurisdictions are engaged in questionable business practices that endanger individuals' security, privacy, and consumer rights. Legislators, too, should be attentive of whether they should provide additional powers to regulators to discipline bad actors or mobile industry participants that are prioritizing revenues over protecting their subscribers.

Fourth, the increasing frequency of geolocation attacks using 4G networks indicates an increased level of sophistication amongst surveillance actors and an evolutionary trend that is elevating espionage risks as the world moves into the 5G era. 5G deployments are already fully launched in many developed nations and geolocation surveillance activity is seen from some of these same countries. This calls into question the security of future roaming partnerships with networks of western countries. While a great deal of attention has been spent on whether or not to include Huawei networking equipment in telecommunications networks, comparatively little has been said about ensuring non-Chinese equipment is well secured and not used to facilitate surveillance activities.[44] Policy makers, telecommunications regulators, cybersecurity agencies, and legislators alike should move to develop a vendor- and platform-neutral set of mandatory security and privacy standards. They should, also, work to actively enforce these standards and attach significant penalties to companies that are found deliberately not adhering to them.

Consumers might rightfully assume that their telecommunications provider has deployed and configured security firewalls to ensure that signaling messages associated with geolocation attacks, identity attacks, or other malicious activity are not directed towards their phones. Unfortunately this is not often the case. Decades of poor accountability and transparency have contributed to the current environment where extensive geolocation surveillance attacks are not reported. This status quo has effectively created a thriving geolocation surveillance market while also ensuring that some telecommunications providers have benefitted from turning a blind eye to the availability of their

43 Jon Brodkin. (2021, October 6). Company that routes SMS for all major US carriers was hacked for five years. *Ars Technica.* https://arstechnica.com/information-technology/2021/10/company-that-routes-sms-for-all-major-us-carriers-was-hacked-for-five-years/

44 For more, see: Christopher Parsons. (2020). "Huawei and 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/.

network interconnections to the surveillance industry. While it is implausible to expect that all telecommunications networks will adopt security and privacy postures to protect against all threats, the low-hanging geolocation threats detailed in this report should be addressed post-haste.

Operators should be required to: adopt and act to attain and demonstrate compliance with cybersecurity guidelines and frameworks such as zero trust; report when they experience attacks; accept accountability for when their networks are abused by surveillance actors; work towards buiding security agreements and accreditations; and undertake penetration tests to identify and remediate vulnerabilities. In cases where operators decline to undertake these activities willingly, then regulators should step in to compel corporations to undertake these kinds of activities.

Today, surveillance actors use geolocation to reveal intimate and personal information. It is used to track human rights defenders, senior business leaders, government officials, and members of militaries. In the future, with the blossoming of smart cities, the internet of things, and the growth of internet-connected systems, the capabilities and potentials for attack will only grow. If organizations should fail to act, then advocates in civil society and the broader business community will have to pressure regulators, policy makers, and politicians to actively compel telecommunications providers to adopt appropriate security postures to mitigate the pernicious and silent threats associated with geolocation surveillance.