Reactive Sanctions and Foreseeable Technology-Enabled Human Rights Harm: Assessing Canada's *Special Economic Measures Act* through the Geedge Networks Case

by

Yihao Duan

A Practicum submitted to the
Faculty of Graduate and Postdoctoral Studies
of the University of Manitoba in partial fulfilment of the
requirements of
the degree of

Master of Human Rights

Faculty of Law
University of Manitoba
Winnipeg

Contents

Abstract

This research examines the extent to which Canada's *Special Economic Measures Act* (SEMA) can engage with foreseeable, technology-enabled human rights harm. As surveillance and censorship technologies become increasingly embedded within digital infrastructure, human rights risks may arise through technological capacity, institutional context, and patterns of foreseeable misuse before specific violations are fully documented or formally attributed. This creates a challenge for sanctions law, which has traditionally been structured around identifiable actors, established wrongdoing, and serious violations that have already become legally and politically visible.

Using doctrinal legal analysis, policy analysis, and the case study of Geedge Networks' reported involvement in Myanmar's digital surveillance and censorship infrastructure, this research evaluates whether SEMA can respond meaningfully to infrastructure-mediated human rights risk. It argues that SEMA remains predominantly reactive in both statutory design and practical operation. Its legal thresholds, including "grave breach" and "gross and systematic" human rights violations, generally require a serious factual record before sanctions can be imposed. As a result, SEMA is not well suited to acting as an *ex ante* technology-governance or export-control mechanism.

At the same time, this research argues that SEMA should not be dismissed as irrelevant to prevention. Where a sufficient evidentiary record exists and a defensible nexus can be established between an actor and a serious human rights situation, SEMA may play a limited preventive role by increasing legal, economic, and reputational costs and by helping to prevent the further consolidation of harmful technological infrastructure. The Geedge case illustrates the importance of analyzing technology-enabled harm through capacity, context, nexus, and foreseeability, rather than through completed violations alone.

The research concludes that SEMA cannot replace broader preventive mechanisms such as export controls, corporate human rights due diligence, procurement safeguards, and transparency requirements. However, it can form part of a wider preventive human rights architecture. More broadly, the paper suggests that technology-enabled human rights harm is placing increasing pressure on the boundary between retrospective accountability and preventive legal intervention.

Acknowledgements

I owe my deepest thanks to Professor Mary Shariff, whose guidance, patience, and generosity sustained this practicum from its early stages through to completion. Her careful reading and thoughtful comments continually pushed me to clarify my ideas and strengthen the paper, while her encouragement gave me confidence at moments when the process felt especially demanding. I am particularly indebted to her for the extraordinary amount of time and care she devoted to the revision process, as well as for guiding me through the many academic and administrative steps involved in bringing this project to its final form. It has been a privilege to learn from her, and this paper would not be what it is without her support.

I would also like to acknowledge Dr. Opeyemi Bello for serving as the examiner of this practicum. His positive evaluation of the paper, and his recommendation that the practicum receive a pass, meant a great deal to me and marked an especially meaningful point at the end of this process.

My practicum experience at the Raoul Wallenberg Centre for Human Rights was equally important to the development of this work, and I am especially thankful to Kimberly Lenz for her mentorship during that time. There is something wonderfully serendipitous about the way our paths crossed. We first came into contact unexpectedly in 2023, only to meet again two years later when the Centre became my practicum site in 2025. What began as a chance encounter eventually became an important part of my academic journey. Working with Kimberly allowed me to encounter human rights practice beyond the classroom, and many of the questions and ideas that ultimately shaped this paper grew out of that experience. Her trust, guidance, and willingness to share her experience with me left a lasting impression.

The Master of Human Rights program also brought me into contact with professors, staff, and classmates from whom I learned in many different ways. The discussions we shared, the perspectives I encountered, and the friendships formed along the way expanded my understanding of human rights far beyond what could be captured in any single paper or course. I feel fortunate to have studied in a community where people brought such different experiences, interests, and ways of thinking to the same questions.

Lastly, Winnipeg and Canada have become an important part of this chapter of my life. Winnipeg has been a memorable place in which to study, learn, and grow, and my time in Canada has given me experiences and opportunities that I will carry with me well beyond this program. As this practicum comes to an end, I hope it marks not only the completion of one stage, but the beginning of a new chapter. I leave this program with appreciation for the people I have met, the lessons I have learned, and the possibilities ahead.

I. Introduction: Technology, Human Rights, and the Limits of Sanctions Law

Serious human rights violations not only involve direct physical violence; they are increasingly enabled through the deployment of surveillance and security technologies that operate at scale and often remain partially invisible.[1] Digital infrastructures, such as network monitoring systems, deep packet inspection tools, and large-scale data interception platforms can facilitate restrictions on privacy, freedom of expression, and freedom of association in ways that are indirect, continuous, and difficult to attribute to discrete acts or actors.[2] These systems do not merely support repression; they can fundamentally restructure how the system is exercised, shifting it from episodic intervention to continuous governance embedded within technical systems. As a result, human rights harm is increasingly mediated through infrastructure rather than identifiable acts. This development places pressure on the more classical, violation-based model of human rights law which typically focuses on identifying discrete acts of wrongdoing, attributing responsibility to specific actors, and providing remedies and reparations for victims of established violations.[3]

---

[1] Office of the United Nations High Commissioner for Human Rights, *The Right to Privacy in the Digital Age*, UN Doc A/HRC/60/45 (29 August 2025) at paras 1–3, online (pdf): OHCHR <https://www.ohchr.org/en/documents/thematic-reports/ahrc6045-right-privacy-digital-age-report-office-united-nations-high>.

[2] For introductory discussion see Steven Feldstein, *The Global Expansion of AI Surveillance* (Washington, DC: Carnegie Endowment for International Peace, 2019) at 5–8; Freedom House, *Freedom on the Net 2024* (Washington, DC: Freedom House, 2024) at 1–4, online (pdf): Freedom House <http://freedomhouse.org/sites/default/files/2024-10/FREEDOM-ON-THE-NET-2024-DIGITAL-BOOKLET.pdf>.

[3] See e.g. UN General Assembly, Basic Principles and Guidelines on the Right to a Remedy and Reparation for Victims of Gross Violations of International Human Rights Law and Serious Violations of

For the purposes of this paper, "surveillance" refers broadly to the systematic monitoring, collection, or analysis of communications, network activity, or related data in ways capable of identifying, tracking, or assessing individuals or their activities. "Traffic management", by contrast, refers to techniques used to monitor, prioritize, shape, filter, or otherwise manage network traffic for purposes such as cybersecurity, congestion management, service reliability, or lawful regulatory compliance. The two categories are analytically distinct, but they may overlap in practice. Technologies used for legitimate network administration may also enable monitoring, blocking, user identification, or censorship when configured or deployed for those purposes. This overlap is central to the dual-use problem examined later in this paper.

At the same time, Canada's foreign policy is undergoing a subtle but important transformation. Under the leadership of the Carney government, Canada appears to be moving away from a more explicitly ideology-driven foreign policy[4] toward a more pragmatic model of international engagement, influenced and shaped by geopolitical fragmentation, economic interdependence, and technological competition.[5] This shift is

---

International Humanitarian Law, GA Res 60/147, UNGAOR, 60th Sess, Supp No 49, UN Doc A/RES/60/147 (16 December 2005), principles 1–3, 11–23, online: OHCHR <https://www.ohchr.org/en/instruments-mechanisms/instruments/basic-principles-and-guidelines-right-remedy-and-reparation>; Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, supra note 1 at paras 1–3.

[4] Kim Richard Nossal, Stéphane Roussel & Stéphane Paquin, *The Politics of Canadian Foreign Policy*, 4th ed (Montreal & Kingston: McGill-Queen's University Press, 2015) at 135–40; Stephen Nagy & Saroj Kumar Rath, "Canada's New Indo-Pacific Calculus: Beyond the Old Atlantic Order" (6 March 2026), online: Macdonald-Laurier Institute <https://macdonaldlaurier.ca/canadas-new-indo-pacific-calculus-beyond-the-old-atlantic-order-stephen-nagy-and-saroj-kumar-rath-for-inside-policy/>.

[5] See e.g. Nagy & Rath, supra note 4; Prime Minister of Canada, "Principled and Pragmatic: Canada's Path" (20 January 2026), online: Prime Minister of Canada <https://www.pm.gc.ca/en/news/speeches/2026/01/20/principled-and-pragmatic-canadas-path-prime-

reflected in Prime Minister Mark Carney's own framing of Canada's position in the international system. For example, at the 2026 World Economic Forum in Davos, Carney emphasized that "if you are not at the table, you are on the menu," underscoring the strategic necessity of continued engagement.[6] He also noted that Canada must be prepared to "take on the world as it is, not wait for a world we wish to be", [7] signaling a willingness to operate within complex and imperfect global conditions.

This emerging shift in Canada's approach to international engagement does not necessarily suggest a retreat from Canada's commitment to human rights.[8] Rather, it can be understood as reshaping and/or expanding the context in which human rights risks may emerge, particularly as these risks increasingly arise from forms of economic and technological interaction involving states or markets where human rights protections may be weaker or unevenly enforced. These shifts increase pressure to respond to human rights violations using existing legal frameworks – many of which operate on an *ex post facto* basis i.e. after a violation(s) has occurred.

Within the evolving geopolitical, economic and technological landscape, Canada's *Special Economic Measures Act* ("SEMA" or the "Act") [9] occupies a central and

---

minister-carney-addresses>.

[6] Prime Minister of Canada, supra note 5.

[7] Ibid.

[8] Shannon Proudfoot, "It's clear Carney is now dealing with the world 'as it is'" *The Globe and Mail* (17 January 2026), online: *The Globe and Mail* <https://www.theglobeandmail.com/politics/opinion/article-its-clear-carney-is-now-dealing-with-the-world-as-it-is/>; Alex Boutilier, "'A foreign policy based on short memory': Carney continues push to diversify from the U.S." Global News (2026), online: Global News <https://globalnews.ca/news/11718383/foreign-policy-based-on-short-memory/>; Prime Minister of Canada, supra note 5.

[9] *Special Economic Measures Act*, SC 1992, c 17 [SEMA].

illustrative role. As one of Canada's principal autonomous sanctions statutes,[10] SEMA allows the Canadian government to impose economic measures in response to grave international situations, including those involving "gross and systematic human rights violations."[11] SEMA has become an increasingly prominent tool of Canadian foreign policy in respect of human rights violations, reflecting their role in linking foreign policy objectives with human rights considerations.[12]

While SEMA is not a specialized human rights statute, it is selected as the principal focus of this paper because it combines broad autonomous sanctions authority with express statutory thresholds concerning serious international situations, including gross and systematic human rights violations. Its ability to support measures directed at both individuals and entities also makes it particularly useful for examining the position of private technology providers alongside more conventional state, military, or security actors. The choice of SEMA is analytical rather than exclusive. Aspects of the capacity-and-

---

[10] See e.g. Global Affairs Canada, "Canadian Sanctions: Essential Information" (18 March 2026), online: Government of Canada <https://www.international.gc.ca/world-monde/international_relations-relations_internationales/sanctions/essential-informations-essentielles.aspx?lang=eng>. Canada may impose autonomous sanctions, that is, sanctions adopted without a United Nations Security Council resolution, under statutes including SEMA, supra note 9, and the Justice for Victims of Corrupt Foreign Officials Act, SC 2017, c 21. The latter is directed to measures in relation to foreign nationals where the circumstances set out in s 4(2) are met, whereas SEMA provides broader foreign-state and international-situation triggers, including gross and systematic human rights violations. See Justice for Victims of Corrupt Foreign Officials Act, ss 2, 4(1)–(2); SEMA, supra note 9, ss 3.1, 4(1.1).

[11] SEMA, supra note 9, s 4.

[12] See discussion in Michael Saunders, "Capabilities and Gaps in the Canadian *Special Economic Measures Act* Regime" (2023) 29:1 *Canadian Foreign Policy Journal* 1 at 1, online: Taylor & Francis <https://www.tandfonline.com/doi/full/10.1080/11926422.2022.2145323>; Andrea Charron, "Canada's Sanctions Regime" (Brief submitted to the House of Commons Standing Committee on Foreign Affairs and International Development, 3 June 2023) at 4, online (pdf): House of Commons <https://www.ourcommons.ca/Content/Committee/441/FAAE/Brief/BR12534345/br-external/CharronAndrea-e.pdf>; Michael Nesbitt, "Canada's 'Unilateral' Sanctions Regime Under Review: Extraterritoriality, Human Rights, Due Process, and Enforcement in Canada's *Special Economic Measures Act*" (2017) 48:2 *Ottawa L Rev* 507 at 515–18.

context inquiry developed below may also illuminate questions arising under other targeted sanctions frameworks, including the *Justice for Victims of Corrupt Foreign Officials Act* S.C. 2017, c. 21. The specific statutory conclusions advanced in this paper, however, remain confined to SEMA.

Both the structure of the Act and its application in practice, however, indicate that SEMA is primarily oriented toward reactive or *ex post facto* accountability. The statutory thresholds for action, as well as the government's own articulation of sanctions policy, suggest that measures are typically imposed once a situation has already been recognized as involving serious wrongdoing and where sufficient evidence exists to support designation decisions.[13] In practice, this has often meant that sanctions follow the consolidation of violations, rather than preceding them. While such an approach is consistent with traditional understandings of sanctions as tools of response and deterrence, it raises questions about their capacity to engage with forms of harm that are less discrete, more cumulative, and increasingly foreseeable. Rather than rendering the potential of SEMA irrelevant in emergent contexts as earlier described, these apparent limitations make SEMA a particularly important object of analysis: 1) they can help expose the structural boundaries of Canada's existing sanctions framework; and 2) they provide a concrete basis for assessing whether it can adapt to emerging forms of technology-enabled human rights harm. This also raises a threshold question, namely whether harms that are anticipatory,

[13] Global Affairs Canada, "Canadian Sanctions: Essential Information", supra note 10. That page defines a designation as the formal listing of an individual or entity under Canadian sanctions regulations, which triggers legal consequences such as asset freezes and prohibitions on dealings.

cumulative, or infrastructure-based can satisfy the statutory criteria required to trigger sanctions under SEMA.

Technology-enabled human rights harm presents a particularly acute challenge in this regard. The provision of surveillance and security technologies can create the *capacity* for repression well before any specific violation is potentially formally recognized. These technologies are frequently "dual-use" in nature, capable of serving legitimate regulatory or security functions while also enabling systematic rights restrictions / violations depending on how and where they are deployed.[14] This dual-use character is often reinforced by neutral product framing: technologies may be presented in the language of cybersecurity, traffic management, network optimization, or lawful regulatory compliance, even though the same capabilities may be repurposed for surveillance, censorship, or political control in contexts with weak safeguards. As a result, the *risk* of human rights harm could become identifiable *in advance*, even in the absence of clearly attributable conduct that would satisfy the evidentiary thresholds typically required for sanctions. This creates a structural tension between the anticipatory nature of risk and the retrospective logic of sanctions law.

This tension is illustrated by the case of Geedge Networks, a Chinese technology company whose leaked internal documents and subsequent technical analyses revealed that the company was exporting network-level surveillance and censorship systems to third-

[14] For discussion of the term "dual-use" or "dual use" see e.g. Lena Riecke, "Unmasking the Term 'Dual Use' in EU Spyware Export Control" (2023) 34:3 *European Journal of International Law* 697 at 699–705, online: Oxford Academic <https://doi.org/10.1093/ejil/chad039>.

country governments, including Myanmar.[15] These systems reportedly enable capabilities such as deep packet inspection, lawful interception, real-time traffic monitoring, and individual user identification at the level of national internet infrastructure.[16] In documented contexts, these capabilities have been deployed in ways that facilitate restrictions that may be difficult to justify from a human rights perspective, particularly in relation to privacy, freedom of expression, and access to information within politically repressive environments.[17]

The analytical value of the Geedge case lies not in attributing direct responsibility for specific violations, but in demonstrating how human rights harm can be enabled indirectly through the provision of technological capacity across borders. The technical characteristics of the systems involved, combined with the regulatory and political environments in which they are deployed, may make the risk of misuse identifiable and certain forms of human rights harm reasonably foreseeable, even before specific violations are formally recognized after the fact. At the same time, from the perspective of sanctions law, such cases may fall into a grey area: while the potential for harm is evident, the legal basis for action under a reactive framework such as SEMA may be less clear, particularly

---

[15] Justice For Myanmar, *Silk Road of Surveillance: The Role of China's Geedge Networks and Myanmar Telecommunications Operators in the Junta's Digital Terror Campaign* (2025) at 1–2, online (pdf): Justice For Myanmar <https://jfm-files.s3.us-east-2.amazonaws.com/public/Silk+Road+of+Surveillance+EN.pdf>; InterSecLab, *The Internet Coup: A Technical Analysis on How a Chinese Company is Exporting the Great Firewall to Autocratic Regimes* (September 2025) at 12–14, online: InterSecLab <https://interseclab.org/research/the-internet-coup/>.

[16] InterSecLab, *The Internet Coup*, supra note 15 at 18–21.

[17] Justice For Myanmar, *Silk Road of Surveillance*, supra note 15 at 1–3; Zeyi Yang, "Massive Leak Reveals How a Chinese Firm Helps Censorship Worldwide" *Wired* (8 September 2025), online: *Wired* <https://www.wired.com/story/geedge-networks-mass-censorship-leak/>.

where sanctions must be grounded in existing country-specific regimes or established patterns of wrongdoing.

Comparative developments among Canada's allies also indicate that related human rights risks are being addressed through legal tools operating at different points in the technology-transfer chain. United States export controls and entity listings,[18] European Union controls concerning dual-use and cyber-surveillance exports,[19] and Australia's thematic human rights sanctions framework[20] provide relevant points of comparison. These approaches are considered more fully in Part V.

Against this backdrop, this research examines whether, and to what extent, a reactive sanctions framework such as SEMA can meaningfully engage with foreseeable, technology-enabled human rights harm. It does not seek to propose a comprehensive

---

[18] See e.g. US Department of Commerce, Bureau of Industry and Security, "Commerce Adds 8 Entities to the Entity List for Enabling Human Rights Abuses" (10 December 2024), online: BIS <https://www.bis.gov/press-release/commerce-adds-8-entities-entity-list-enabling-human-rights-abuses>; Export Administration Regulations: Crime Controls and Expansion/Update of U.S. Persons Controls, 89 Fed Reg 60998 (29 July 2024), online: Federal Register <https://www.federalregister.gov/documents/2024/07/29/2024-16498/export-administration-regulations-crime-controls-and-expansionupdate-of-us-persons-controls>.

[19] See e.g. Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items, [2021] OJ L 206/1, recitals 2, 8, arts 2(20), 5; European Commission, "Commission publishes guidelines for cyber-surveillance exporters" (16 October 2024), online: European Commission <https://policy.trade.ec.europa.eu/news/commission-publishes-guidelines-cyber-surveillance-exporters-2024-10-16_en>; Riecke, supra note 14.

[20] See e.g. Australian Department of Foreign Affairs and Trade, "Serious violations or serious abuses of human rights sanctions framework" (accessed 2 June 2026), online: DFAT <https://www.dfat.gov.au/international-relations/security/sanctions/sanctions-regimes/serious-violations-or-serious-abuses-human-rights-sanctions-framework>; *Autonomous Sanctions Amendment (Magnitsky-style and Other Thematic Sanctions) Act 2021* (Cth).

reform agenda or to define fixed human rights "red lines." Rather, it aims to identify and analyze the structural limitations, if any, that arise when autonomous sanctions law encounters indirect, capacity-based forms of harm, and to consider the extent to which SEMA may nevertheless play a role - even if limited - in signaling risk, shaping expectations, and complementing other regulatory approaches. In doing so, it is hoped that the discussion also contributes to a foundational understanding of how sanctions law operates in an increasingly technologically mediated human rights landscape.

Accordingly, the discussion proceeds in several stages. It first examines how technology-enabled human rights harm reshapes the structure of harm and challenges traditional, violation-based models of accountability. It then turns to the design and implementation of SEMA, highlighting its predominantly reactive orientation and the evidentiary thresholds that govern its use. Building on this, the paper considers illustrative cases involving the cross-border export of surveillance technologies, demonstrating how capacity-based risks may become identifiable before specific violations are consolidated, and how those risks may make certain forms of human rights harm reasonably foreseeable. The analysis then situates these developments within a comparative perspective, drawing on approaches adopted by other jurisdictions. Finally, the paper assesses whether, and to what extent, SEMA can meaningfully function as a preventive safeguard in the face of emerging forms of technology-enabled human rights harm.

Limitations of research

This paper proceeds within a defined scope and set of assumptions. It does not seek to provide an exhaustive account of international human rights law or a comprehensive doctrinal analysis of the rights at issue. Rather, the discussion focuses on a subset of rights most directly implicated in technology-enabled forms of harm, in particular the rights to privacy, freedom of expression, and freedom of association. The analysis is primarily concerned with the structural features of sanctions law and the ways in which these frameworks engage with indirect, capacity-based harms. As such, the discussion is intended to be illustrative rather than comprehensive, and aims to identify key tensions and limitations rather than to resolve them in full.

II. Technology-Enabled Human Rights Harm and the Challenge of Prevention

This section examines how technology-enabled human rights harm reshapes the structure of harm and challenges traditional, violation-based models of accountability. The purpose of this section is to establish the conceptual and structural challenges that technology-enabled human rights harm poses to traditional models of accountability, while also examining how surveillance and security technologies interfere with the exercise of rights such as privacy, freedom of expression, and freedom of association. In doing so, the section provides the analytical foundation for assessing the adequacy of sanctions frameworks such as SEMA. It proceeds in three steps: first, by outlining how such harms are increasingly mediated through infrastructure rather than discrete acts; second, by analyzing their cumulative and anticipatory character; and third, by considering the implications of these shifts for existing legal frameworks.

A. Infrastructure-Mediated Harm

The increasing integration of surveillance and security technologies into systems of governance has both expanded and reshaped the ways in which technologically-enabled human rights harm. While human rights violations have traditionally been conceptualized as discrete acts attributable to identifiable actors,[21] contemporary forms of harm are increasingly mediated through digital infrastructures that operate continuously and at scale.[22] This shift is not merely technological, but conceptual. It changes how harm is

[21] International Law Commission, Articles on Responsibility of States for Internationally Wrongful Acts, UN Doc A/56/10 (2001) at 26; UN General Assembly, Basic Principles and Guidelines, supra note 3 at 6.
[22] Daragh Murray et al, "The Chilling Effects of Surveillance and Human Rights: Insights from Qualitative

produced, how it is experienced, and how it can be identified within legal frameworks. As Bernal observes, surveillance should not be understood as a series of isolated acts, but as a condition embedded in the continuous gathering and retention of data, where the existence of such systems itself produces human rights interference.[23]

A central feature of technology-enabled harm is its ***indirectness***. Surveillance technologies such as deep packet inspection systems, lawful interception platforms, and large-scale data collection architectures do not in themselves constitute discrete violations of rights. Rather, they create the conditions under which such violations can occur more efficiently and more systematically. Bernal argues that surveillance should be understood as a structural phenomenon that enables power to be exercised in ways that are not always immediately visible or attributable.[24] Similarly, Murray and colleagues emphasize that surveillance generates effects that extend beyond identifiable acts, shaping behavior and limiting the exercise of rights through subtle and often intangible mechanisms.[25] In this sense, harm is not located in a single action, but emerges through the operation of systems that facilitate control.

Research in Uganda and Zimbabwe" (2024) 16:1 *Journal of Human Rights Practice* 397 at 397–399.

[23] Paul Bernal, "Data Gathering, Surveillance and Human Rights: Recasting the Debate" (2016) 1:2 *Journal of Cyber Policy* 243 at 249–250.

[24] Ibid at 247–49.

[25] Murray et al, supra note 22 at 400–03.

B. Cumulative and Anticipatory Harm

(i) Cumulative Effects and Chilling Impacts

The *indirectness* is closely linked to the ***scalability*** of digital technologies. Once deployed, surveillance systems can operate across entire populations and over extended periods of time. Unlike traditional forms of repression, which are constrained by institutional and human capacity, digital systems can monitor and analyze vast quantities of data in real time. Rautenberg and Murray highlight that such systems produce long-term and cumulative effects, including pervasive chilling impacts on human expression and association.[26] These effects are not episodic, but continuous, and may reshape the informational environment within which individuals exercise their rights. More specifically, these cumulative effects are often experienced through what has been described as the chilling effect of surveillance. As Murray and colleagues demonstrate, such effects may manifest as behavioral changes, self-censorship, and reduced participation in public life.[27] Rather than arising from a single identifiable act, these harms emerge gradually through the operation of surveillance systems, shaping how individuals engage with their social and political environments. The Office of the United Nations High Commissioner for Human Rights similarly notes that digital surveillance can affect entire societies, extending beyond targeted individuals to broader populations.[28] As a result,

[26] Niclas Rautenberg and Daragh Murray, "Making Tangible the Long-Term Harm Linked to the Chilling Effects of AI-enabled Surveillance: Can Human Flourishing Inform Human Rights?" (2024) 25 *Human Rights Review* 293 at 294–298.
[27] Murray et al, supra note 22 at 404–06.
[28] Office of the United Nations High Commissioner for Human Rights, *Mapping Report: Human Rights and New and Emerging Digital Technologies*, UN Doc A/HRC/56/45 (20 August 2024) at paras 13–18.

harm becomes embedded within infrastructure, operating not only at the level of individual rights interference but also across broader populations and informational environments. From a capacity perspective, the significance of such systems lies not only in the violations they may directly facilitate, but in their ability to create scalable and enduring capacities for monitoring, interception, and control. In this sense, the embeddedness and indirectness of surveillance infrastructures raise important questions about identifiable, capacity-based risk and how legal frameworks assess the threshold at which such risk becomes legally relevant harm, particularly where the deployment of such capacity gives rise to a reasonable apprehension of human rights harm before specific violations are fully documented.

（ii） Diffusion of Harm and Responsibility

A further defining characteristic is ***diffusion***, which differs from *indirectness* in that it concerns the spatial and institutional dispersion of responsibility, rather than the attenuation of causal links between conduct and harm both in terms of actors and geography. Technology-enabled harm often arises through transnational arrangements involving multiple actors. For example, surveillance technologies may be developed by private companies, exported across borders, and deployed by state authorities in different political contexts.[29] This distribution of roles complicates traditional models of identifying

[29] Amnesty International, *Uncovering the Iceberg: The Digital Surveillance Crisis Wrought by States and the Private Sector*, DOC 10/4491/2021 (23 July 2021), online: Amnesty International <https://www.amnesty.org/en/documents/doc10/4491/2021/en/>; Bill Marczak et al, *Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries*, Citizen Lab Research Report No 113 (Toronto: University of Toronto, September 2018), online: Citizen Lab

or attributing responsibility, which are typically structured around clearly identifiable perpetrators operating within one or two jurisdictions.[30] Teo argues that AI-enabled systems contribute to what she describes as "slow violence,"[31] which "occurs gradually and out of sight,… dispersed across time and space, an attritional violence that is typically not viewed as violence at all"[32]. Bernal similarly notes that data-driven systems blur the boundaries between public and private actors, further complicating accountability.[33] These dynamics confront legal frameworks that rely on clear causal links between conduct and harm. From a capacity perspective, these dynamics also complicate how legal frameworks measure risk and determine thresholds for intervention. Where surveillance and security infrastructures create scalable capacities for monitoring, interception, or control across dispersed contexts, the risk of misuse may become identifiable, and future human rights harm may be reasonably foreseeable[34]even before specific violations are fully documented. This raises important questions about whether sanctions frameworks structured around reactive and violation-based models are adequately equipped to respond to technology-enabled forms of harm.

<https://citizenlab.ca/research/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/>.

[30] Traditional western legal frameworks often rely on geographically identifiable connections and clearly attributable actors in determining responsibility and jurisdiction. See e.g. *Club Resorts Ltd v Van Breda*, 2012 SCC 17 at paras 21–25, [2012] 1 SCR 572; *Canadian Dredge & Dock Co v The Queen*, [1985] 1 SCR 662 at 681–82.

[31] Sue Anne Teo, "Artificial Intelligence and Its 'Slow Violence' to Human Rights" (2025) 5 *AI and Ethics* 2265 at 2266–2268.

[32] Rob Nixon, *Slow Violence and the Environmentalism of the Poor* (Cambridge, Mass: Harvard University Press, 2011) at 2.

[33] Bernal, supra note 23 at 248–50.

[34] In this context, reasonable foreseeability refers not to certainty of harm, but to an objective assessment of whether the system's known capabilities, the conditions of deployment, and the surrounding political and legal safeguards make harmful use reasonably apprehensible.

（iii）Foreseeability and Risk-Based Harm

Perhaps the most significant feature of technology-enabled harm is its *foreseeability*. Notwithstanding various challenges associated with *indirectness* and *diffusion* and the attribution of responsibility, the risks associated with certain surveillance capabilities are well documented and, in many cases, predictable. Mantelero and Esposito argue that data-intensive systems require *ex ante* human rights impact assessment precisely because their potential effects can often be anticipated before deployment.[35] This reflects a broader shift toward risk-based approaches in the governance of emerging technologies. The deployment of systems capable of large-scale monitoring, interception, and data analysis in environments with weak legal safeguards may make capacity-based risk identifiable and give rise to a reasonable apprehension of human rights harm, including improper restrictions on privacy, freedom of expression, and freedom of association, for example through pervasive data collection and tracking (privacy)[36], the chilling of online speech and self-censorship (expression)[37], and the deterrence of collective organization or protest (association)[38].

---

[35] Alessandro Mantelero & Maria Samantha Esposito, "An Evidence-Based Methodology for Human Rights Impact Assessment (HRIA) in the Development of AI Data-Intensive Systems" (2021) 41 *Computer Law & Security Review* 105561 at 2–4; see also Rio Declaration on Environment and Development, UN Doc A/CONF.151/26 (1992), principle 15; United Nations Declaration on the Rights of Indigenous Peoples, GA Res 61/295 (2007), arts 10, 19.

[36] Privacy and Civil Liberties Oversight Board, *Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court* (23 January 2014) at 12–13.

[37] Jonathon W Penney, "Chilling Effects: Online Surveillance and Wikipedia Use" (2016) 31:1 *Berkeley Technology Law Journal* 117 at 119, 127.

[38] Murray et al, supra note 22 at 408–09.

As Rautenberg and Murray observe, the chilling effects of surveillance do not depend on the occurrence of specific violations but arise from the existence of monitoring capabilities themselves.[39] In this sense, harm is not only reactive, but anticipatory.

Taken together, these characteristics suggest that technology-enabled human rights harm is best understood as a *process*, rather than an event. Harm emerges through the interaction of technological capacity, institutional context, and patterns of use. This process-oriented nature of harm presents structural and significant challenges for legal and policy frameworks designed to respond to violations.

C. Implications for Legal Frameworks

Traditional accountability mechanisms in human rights law are primarily oriented toward post-violation responsibility. This traditional model depends on the identification of a wrongful act, the attribution of that act to a responsible actor, and the availability of sufficient evidence to support intervention.[40] In international human rights adjudication, domestic legal systems, or sanctions regimes, responses are typically triggered once a violation has been established.[41] As Lopez notes, economic sanctions have historically functioned as instruments of coercion and response, applied once a situation has been

---

[39] Rautenberg & Murray, supra note 26 at 297–99.

[40] International Law Commission, Articles on Responsibility of States for Internationally Wrongful Acts, supra note 21, art 2; UN General Assembly, Basic Principles and Guidelines, supra note 3, principles 1–3, 11–23.

[41] George A Lopez, "Enforcing Human Rights Through Economic Sanctions" in Dinah Shelton, ed, *The Oxford Handbook of International Human Rights Law* (Oxford: Oxford University Press, 2013) 770 at 778–779.

recognized as involving serious wrongdoing or crisis.[42] Similarly, Dupont highlights that sanctions frameworks are closely tied to political and legal thresholds that require identifiable violations and actors.[43]

(i) Attribution

This orientation creates particular difficulties in the context of infrastructural, technology-enabled harm. One challenge lies in the problem of *attribution*. Where harm is mediated through complex technological systems involving multiple actors, it may be difficult to establish a direct link between a specific actor and a specific violation. A technology provider may enable surveillance capabilities without directly carrying out the acts that constitute violations, and furthermore state actors may operate within systems that *diffuse* individual responsibility.[44] These dynamics complicate efforts to apply traditional legal categories of responsibility. These difficulties also raise broader questions about the threshold required to justify *ex ante* legal intervention. Where surveillance infrastructures create capacities that may foreseeably enable repression across dispersed institutional settings, reliance on direct attribution and completed violations may prove insufficient as a basis for timely response. This suggests that technology-enabled harm may require legal frameworks to engage more directly with questions of technological capacity, identifiable risk, and reasonable foreseeability when assessing whether earlier legal or policy

[42] Ibid at 772–74.
[43] Pierre-Emmanuel Dupont, "Human Rights Implications of Sanctions" in Masahiko Asada, ed, *Economic Sanctions in International Law and Practice* (Abingdon: Routledge, 2019) 37 at 40–42.
[44] Bernal, supra note 23 at 246–47, 259–60.

intervention may be justified, rather than focusing exclusively on clearly established violations.

(ii) Evidentiary Thresholds

A related challenge concerns evidentiary thresholds. Post-violation accountability mechanisms typically require clear and specific evidence of wrongdoing. However, the effects of surveillance systems are often diffuse and difficult to document. As discussed above, such harms may manifest through behavioral changes, self-censorship, and reduced participation in public life, which do not readily translate into conventional forms of evidence. More broadly, the societal impacts of digital surveillance are often indirect and difficult to quantify, complicating efforts to establish both the existence of harm and its attribution to particular actors. The technical complexity of surveillance systems further complicates the collection and interpretation of evidence. For example, where such systems rely on distributed or cloud-based infrastructures, relevant data may be fragmented, inaccessible, or controlled by multiple actors, making it difficult to reconstruct how monitoring was conducted[45]. These evidentiary difficulties raise broader questions about whether existing legal frameworks rely on thresholds of proof that are ill-suited to technology-enabled forms of harm. Where harmful effects emerge gradually through embedded surveillance capacities, intervention may depend less on documenting

[45] National Institute of Standards and Technology, NIST IR 8006: *NIST Cloud Computing Forensic Science Challenges* (Gaithersburg, MD: NIST, 2020) at 2–4, online (pdf): NIST <https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8006.pdf>.

completed violations and more on assessing the foreseeable risks associated with particular technological infrastructures and capabilities.

(iii) Temporal Limitations

The temporal structure of accountability mechanisms further exacerbates these challenges. As discussed above, because traditional frameworks are reactive, they are typically engaged only after harm has become visible and sufficiently substantiated. In the context of technology-enabled harm, this may result in delayed responses, by which time the underlying infrastructure is already entrenched.[46] Once surveillance systems are embedded within governance structures, their effects may be difficult to reverse or mitigate. This raises questions about the adequacy of reactive approaches in addressing harms that are cumulative and systemic. These dynamics may also underscore the importance of regulatory approaches that assess the human rights implications of surveillance infrastructures before harmful effects fully materialize. In this sense, the concern is not only with responding to the eventual consequences of technology-enabled harm, but also with evaluating whether the underlying technological capacities and methods are themselves compatible with human rights principles.

(iv) Limits of *Ex Ante* and Sanctions Frameworks

These challenges give rise to a broader conceptual tension between prevention and post-violation responsibility. While human rights law recognizes, at least in principle, the

[46] Giovanni De Gregorio & Roxana Radu, "*Digital Constitutionalism in the New Era of Internet Governance*" (2022) 30:1 *International Journal of Law and Information Technology* 68 at 69–70.

importance of preventing foreseeable harm,[47] many of the tools available to states remain oriented toward responding after violations occur. That said, emerging regulatory developments in several jurisdictions suggest a gradual shift toward *ex ante* approaches.[48]

Emerging *ex ante* approaches point to a gradual shift toward identifying technology-related risks before harm fully materializes. The European Union's Artificial Intelligence Act adopts a risk-based model,[49] while the United Kingdom's *Online Safety Act*[50] and Australia's *Online Safety Act*[51] impose proactive obligations in relation to online platforms and harmful content. These frameworks nevertheless remain primarily concerned with AI safety, platform governance, or content regulation rather than the cross-border surveillance infrastructure examined in this paper. They therefore do not resolve the attributional, evidentiary, and temporal difficulties identified above.[52]

---

[47] Office of the United Nations High Commissioner for Human Rights, *Guiding Principles on Business and Human Rights*: Implementing the United Nations "Protect, Respect and Remedy" Framework, UN Doc HR/PUB/11/04 (2011) at 3.

[48] Mantelero & Esposito, supra note 35 at 5–7.

[49] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), [2024] OJ L 1689, art 27.

[50] *Online Safety Act 2023* (UK), c 50.

[51] *Online Safety Act 2021* (Cth).

[52] See eg Herbert Smith Freehills Kramer, *Trust at Risk: Who's Accountable for the Online Safety Gap?* (2025), online: Herbert Smith Freehills Kramer <https://www.hsfkramer.com/insights/reports/2025/code-law/trust-at-risk-whos-accountable-for-the-online-safety-gap>; Mariana Olaizola Rosenblat, Ayushi Agrawal & Isaac Yap, *Online Safety Regulations Around the World: The State of Play and the Way Forward* (New York: NYU Stern Center for Business and Human Rights, 2025) at 1–5, online (pdf): NYU Stern Center for Business and Human Rights <https://bhr.stern.nyu.edu/wp-content/uploads/2025/04/NYU-CBHR-Online-Regulations_Updated-Apr-23.pdf>.

Taken together, the preceding analysis identifies a gap between reasonably foreseeable technology-enabled risk and legally actionable harm. Sanctions regimes and comparable accountability mechanisms[53] remain primarily retrospective. Surveillance infrastructures may create scalable capacities for monitoring, interception, and control before specific violations are fully documented, responsibility is clearly attributable, or harm is substantiated in the form ordinarily expected by such frameworks. This does not make sanctions or other accountability mechanisms inadequate; rather, it exposes the limits of a design centered on attribution, evidence, and post-violation response. The next section examines how that tension appears within SEMA, focusing on its statutory thresholds, designation practice, evidentiary orientation, and reliance on identifiable actors.

III. SEMA as a Human Rights Tool: Design, Practice, and Structural Limits

Canada's SEMA occupies a central position within the country's autonomous sanctions framework. Enacted in 1992, SEMA provides the principal legal basis for Canada to impose economic measures in response to international crises, including those involving serious human rights violations.[54]

SEMA operates through a statutory-regulatory structure. The Act authorizes the Governor in Council, where one of the statutory circumstances in s 4(1.1) is met, to make

---

[53] For the purposes of this discussion, "other accountability mechanisms" refers primarily to legal and institutional frameworks, including international human rights adjudication and domestic legal processes, that generally depend upon identifiable violations, attributable conduct, and sufficiently substantiated harm before responsibility or intervention may be justified.

[54] Nesbitt, supra note 12 at 511–16, 553–59; Scott McTaggart, Sanctions: The Canadian and International Architecture, Library of Parliament Publication No 2019-45-E (Ottawa: Library of Parliament, 18 November 2019) at 4, online: Library of Parliament <https://lop.parl.ca/sites/PublicWebsite/default/en_CA/ResearchPublications/201945E>.

orders or regulations restricting or prohibiting specified activities in relation to a foreign state.[55] In practice, those measures are implemented through country-specific regulations that identify listed persons or entities and impose prohibitions on persons in Canada and Canadians abroad.[56] In *Makarov*, the Federal Court accepted the explanation that SEMA regulations may target listed persons, but operate by "regulating the actions of Canadians and individuals within Canada" in relation to those persons, including by prohibiting dealings in property, transactions, the provision of services, and the making available of goods.[57] The practical effect is often an asset freeze and a prohibition on economic dealings with the listed person or entity.[58]

While not exclusively designed as a human rights instrument, SEMA has increasingly been used in contexts framed partly in human rights terms, including through regulations relating to Myanmar,[59] Iran,[60] Russia,[61] and other jurisdictions.[62] Its flexibility and broad scope make it an important sanctions mechanism through which Canada can express and operationalize aspects of its external human rights commitments, while remaining embedded within a broader foreign-policy and economic-sanctions framework. At the

---

[55] SEMA, supra note 9, ss 4(1)–(2), 4(1.1)(b)–(c).
[56] *Special Economic Measures (Russia) Regulations*, SOR/2014-58, ss 2–3.
[57] *Makarov v Canada* (Minister of Foreign Affairs), 2024 FC 1234 at para 7.
[58] Ibid; Special Economic Measures (Russia) Regulations, supra note 56, s 3.
[59] *Special Economic Measures (Myanmar) Regulations*, SOR/2007-285, s 2(b), (d)–(e).
[60] *Special Economic Measures (Iran) Regulations*, SOR/2010-165, s 2(a.1), Sch 1.1.
[61] *Special Economic Measures (Russia) Regulations*, supra note 56, s 2(a.1)–(c).
[62] SEMA, supra note 9, ss 3.1, 4(1.1)(c); Global Affairs Canada, "Canadian Sanctions: Essential Information", supra note 10.

same time, the structure of the Act and its application in practice reveal important limitations in how it engages with contemporary forms of harm.

A. SEMA's Statutory Structure and Human Rights Function

From a strictly legal perspective, SEMA authorizes the Governor in Council to impose sanctions through orders or regulations where certain statutory threshold conditions are met. Section 3.1 of the Act states its purpose in the following terms:

> The purpose of this Act is to enable the Government of Canada to take economic measures against certain persons in circumstances where an international organization of states or association of states of which Canada is a member calls on its members to do so, *a grave breach of international peace and security has occurred, gross and systematic human rights violations have been committed in a foreign state* or acts of significant corruption involving a national of a foreign state have been committed.[63]

The Act allows for a wide range of measures, including asset freezes,[64] prohibitions on dealings,[65] and restrictions on financial transactions[66]. Importantly, SEMA is designed as a discretionary instrument of foreign policy rather than a judicial mechanism.[67] Decisions to impose sanctions are made by the executive,[68] and the Act does not establish

---

[63] SEMA, supra note 9, s 3.1 [emphasis added]. See also ss 4(1), 4(1.1)(b)–(c), 4(2), 5.6.

[64] SEMA, supra note 9, s 4(1)(b); Global Affairs Canada, "Canadian Sanctions Related to Russia" (accessed 25 May 2026), online: Government of Canada <https://www.international.gc.ca/world-monde/international_relations-relations_internationales/sanctions/russia-russie.aspx?lang=eng>.

[65] SEMA, supra note 9, s 4(2)(a); Special Economic Measures (Russia) Regulations, supra note 56, s 3(a).

[66] SEMA, supra note 9, ss 4(2)(b), 4(2)(e); Global Affairs Canada, "Canadian Sanctions: Essential Information", supra note 10.

[67] McTaggart, supra note 54 at 1–2, 4–5; Standing Senate Committee on Foreign Affairs and International Trade, Strengthening Canada's Autonomous Sanctions Architecture: Five-Year Legislative Review of the Sergei Magnitsky Law and the Special Economic Measures Act (Ottawa: Senate of Canada, 2023) at 13–15, 22–24.

[68] SEMA, supra note 9, ss 4(1), 4(1.1), 4(2); Global Affairs Canada, "Canadian Sanctions: Essential Information", supra note 10; Makarov, supra note 57 at paras 51–53, 76–85.

a detailed evidentiary standard comparable to those found in criminal or civil proceedings.[69]

The objectives of SEMA reflect its hybrid character. On the one hand, sanctions are intended to respond to serious international situations and to signal Canada's condemnation of certain forms of conduct. On the other hand, they are also intended to exert pressure on targeted actors and to influence behavior. As Global Affairs Canada recently stated, sanctions are designed to "influence behavior" and to demonstrate Canada's commitment to "international norms and values", including with respect to human rights.[70] This dual function, combining expressive and coercive elements, shapes how SEMA operates in practice.

At the same time, the structure of SEMA reveals an orientation toward post-violation accountability. The statutory triggers for action are framed in terms of situations that have already reached a certain level of seriousness. Concepts such as "grave breach" and "gross and systematic violations" imply that harm has already materialized and is expressly stated – "has occurred".[71]

---

[69] Makarov, supra note 57 at paras 5, 64, 69, 76, 89–90; Allard International Justice and Human Rights Clinic, Brief to the House of Commons Standing Committee on Foreign Affairs and International Development on Canada's Human Rights Sanctions Regime (13 December 2023) at 2–4, online (pdf): Peter A Allard School of Law <https://allard.ubc.ca/sites/default/files/2024-01/Allard%20IJHR%20Clinic%20Brief%20to%20FAAE%20on%20Canada%27s%20Sanctions%20Regime_final.pdf>.

[70] McTaggart, supra note 54 at 1–2; Global Affairs Canada, "Canadian Sanctions: Essential Information", supra note 10.

[71] SEMA, supra note 9, ss 4(1), 4(1.1)(b)–(c).

As a result, the framework is not designed primarily to address risks in their early stages, but to respond once those risks have developed into identifiable patterns of wrongdoing. This reactive orientation should not, however, be understood simply as a defect in the design of sanctions law. Sanctions may impose significant legal, economic, and reputational consequences on designated persons and entities. Requiring an established serious situation, a defensible evidentiary basis, and an identifiable connection between the targeted actor and the relevant conduct serves important institutional interests, including legal certainty, procedural fairness, proportionality, and the legitimacy of executive decision-making. It also reduces the risk that coercive economic measures will be imposed solely on the basis of speculative future harm. The difficulty identified in this paper is therefore better understood as a trade-off: some of the features that make sanctions decisions credible and legally defensible may also reduce the framework's ability to respond when the strongest available evidence concerns capacity, context, and foreseeable risk rather than completed and attributable violations.[72]

This orientation is further reinforced by how SEMA conceptualizes responsibility. In practice, sanctions are typically imposed on individuals or entities that are considered to be directly or indirectly responsible for the relevant situation.[73] This often includes government officials, military leaders, and other actors associated with the implementation

[72] Lopez, supra note 41 at 772–73; McTaggart, supra note 54 at 1–2; see also Makarov, supra note 57 at paras 51–53, 76–85; Standing Senate Committee on Foreign Affairs and International Trade, Strengthening Canada's Autonomous Sanctions Architecture, supra note 67 at 35–43; Allard International Justice and Human Rights Clinic, supra note 69 at 2–4, 7–8.

[73] Lopez, supra note 41 at 773, 776; SEMA, supra note 9, ss 4(1)–(2); Special Economic Measures (Russia) Regulations, supra note 56, s 2(a)–(c).

of policies or actions that give rise to human rights concerns.[74] The focus on identifiable actors reflects a model of responsibility that is closely tied to attribution and involvement in wrongdoing.

B. Technology-Enabled Harm, Attribution, and Corporate Capacity

When applied to technology-enabled harm, this model encounters difficulties. As discussed in Part II, technology-enabled harm is often mediated through systems involving multiple actors, including private companies that develop or supply technologies.[75] In those cases, the relationship between the provider of a technology and the resulting harm may be indirect, diffused across multiple actors, and shaped by the scalable capacity of the system supplied, rather than by a single discrete act of wrongdoing.

While SEMA allows for the designation of entities as well as individuals,[76] its human-rights-related use has more commonly focused on state officials, military or security actors, associates, and entities closely connected to sanctioned governments or listed persons[77]. The more difficult question for this paper is therefore not whether entities can be listed in principle, but whether SEMA is well suited to address private technology companies whose contribution lies in supplying surveillance capacity that may later be used by state actors to facilitate human rights harm.

---

[74] Special Economic Measures (Myanmar) Regulations, supra note 59, s 2(b), (d)–(e); Special Economic Measures (Iran) Regulations, supra note 60, s 2(a.1)–(c); Special Economic Measures (Russia) Regulations, supra note 56, s 2(a.1)–(c).

[75] See discussion in Part II, supra notes 29, 33, 44 and accompanying text.

[76] SEMA, supra note 9, ss 2, 4(1)(a)–(b).

[77] Special Economic Measures (Myanmar) Regulations, supra note 59, s 2(b), (d)–(e); Special Economic Measures (Iran) Regulations, supra note 60, s 2(a.1)–(c); Special Economic Measures (Russia) Regulations, supra note 56, s 2(a.1)–(c).

This suggests that although SEMA can reach entities in principle, its existing structure and practice remain more readily aligned with responsibility models based on identifiable actors, official status, association, or contribution to an established sanctioned situation than with more diffuse forms of harm.

C. Threshold Conditions under SEMA

(i) The "Grave" and "Gross and Systematic" Requirements

A preliminary issue concerns the threshold conditions for sanctions, and in particular how SEMA conceptualizes the seriousness of the conduct or circumstances capable of triggering action. As noted above, SEMA authorizes action where the Governor in Council is of the opinion that one of the statutory circumstances in s 4(1.1) has occurred. The relevant language refers, among other things, to circumstances in which *"grave* breach of international peace and security has occurred, *gross and systematic* human rights violations".[78]

For the purposes of this paper, these terms are treated as threshold concepts rather than fixed doctrinal definitions. "Grave" suggests a level of seriousness sufficient to engage international peace and security concerns, particularly where the situation has resulted in, or is likely to result in, a serious international crisis. "Gross and systematic" requires attention to both severity and pattern. "Gross" points to the seriousness or scale of the violations, while "systematic" suggests repeated, organized, or patterned conduct rather

[78] SEMA, supra note 9, ss 4(1), 4(1.1)(b)–(c) [emphasis added].

than isolated incidents.[79] This distinction matters because the technology-enabled harm discussed in Part II may emerge earlier, through scalable surveillance capacity, diffused responsibility, and identifiable risks that make future human rights harm reasonably foreseeable before specific violations are fully documented.[80]

(ii) Capacity-Based Risk and the "Gross and Systematic" Threshold

This threshold plays an important role in ensuring that sanctions are reserved for serious and sufficiently established patterns of concern. However, it may also create a barrier to action in cases where harm is emerging but has not yet reached a level that can be clearly characterized as gross and systematic. In the context of technology-enabled harm, the difficulty is that individual rights interferences may not yet be documented as systematic, even where the underlying infrastructure already has systemic qualities. Surveillance infrastructure may operate continuously, at scale, and across dispersed populations, thereby creating the conditions for systematic harm before that harm is fully realized or legally substantiated. In such cases, the threshold *may* limit the scope for intervention even where capacity-based risk is identifiable and future human rights harm is reasonably foreseeable.

D. Evidence, Designation Practice, and Identifiable Actors

The question of evidence further illustrates the reactive orientation of SEMA. The Act does not prescribe a formal evidentiary standard comparable to those found in criminal or

[79] Charron, supra note 12 at 9; McTaggart, supra note 54 at 4–5.
[80] See discussion in Part II, supra notes 26–29, 33–35 and accompanying text.

civil proceedings. Rather, SEMA operates through executive decision-making: where the Governor in Council is of the opinion that one of the statutory circumstances in s 4(1.1) has occurred, the Act authorizes orders or regulations restricting or prohibiting specified activities in relation to a foreign state.[81] Canada's public sanctions guidance similarly describes sanctions as restrictions imposed in relation to foreign states, individuals, and entities, including measures such as asset freezes, dealings prohibitions, arms embargoes, and restrictions on financial transactions.[82] This structure places emphasis on identified crises, listed persons, and regulatory decision-making, rather than on a court-based process requiring proof according to formal civil or criminal evidentiary standards.[83]

These institutional concerns also arise at the designation stage. Parliamentary reviews of Canada's sanctions regime have emphasized transparency, accountability, the identification of sanctioned persons and entities, and clear rationales for autonomous listings.[84] Listing decisions may carry serious legal, economic, and reputational consequences and may also be challenged through judicial review.[85]

---

[81] SEMA, supra note 9, ss 4(1), 4(1.1), 4(2). SEMA s 4(1) provides that the Governor in Council may make orders or regulations where it is of the opinion that one of the circumstances in s 4(1.1) has occurred.
[82] Global Affairs Canada, "Canadian Sanctions: Essential Information", supra note 10. GAC states that Canadian sanctions restrict activities between Canadians and foreign states, individuals, and entities, and may include asset freezes, dealings prohibitions, arms embargoes, financial restrictions, and technical assistance prohibitions.
[83] Makarov, supra note 57 at paras 5, 64, 69, 76.
[84] House of Commons, Standing Committee on Foreign Affairs and International Development, Canada's Sanctions Regime: Transparency, Accountability and Effectiveness, 44th Parl, 1st Sess, No 23 (January 2024) at 18, 27; Standing Senate Committee on Foreign Affairs and International Trade, Strengthening Canada's Autonomous Sanctions Architecture, supra note 67 at 35–39, 41–43.
[85] Makarov, supra note 57 at paras 51–53, 76–85; Allard International Justice and Human Rights Clinic, supra note 69 at 2–4, 7–8.

In cases involving technology-enabled harm, however, the evidentiary landscape is often more complex. As discussed in Part II, the effects of surveillance systems may be diffuse, cumulative, and difficult to document in ways that meet traditional expectations of proof. [86] The relevant evidence may initially demonstrate technological capacity, deployment context, and foreseeable risk, rather than a completed violation by a single actor. A company may supply infrastructure capable of monitoring, interception, or control, while the rights interference may later be carried out by state authorities, security agencies, or other institutional actors. The evidentiary problem is therefore not only whether harm has occurred, but whether evidence of capacity, context, and foreseeable misuse can be sufficient before harm becomes fully visible, attributable, and substantiated.

Diffusion further complicates this inquiry. Where a private company develops or supplies a surveillance system, and a state authority later deploys that system in a repressive or weakly regulated environment, the evidence may be distributed across technical architecture, corporate conduct, procurement relationships, state practice, and observed social effects. This makes it harder to establish a direct link between the provider and a specific violation, even where the overall risk of harm is identifiable. The difficulty is particularly acute where the contribution of the corporate actor lies not in directly committing the violation, but in supplying scalable technological capacity that enables monitoring or control across a population.

---

[86] See discussion in Part II, supra notes 26–29, 33–35, 39, 45 and accompanying text, addressing cumulative and chilling effects, diffusion of responsibility, capacity-based risk, anticipatory harm, and the evidentiary difficulties associated with documenting technology-enabled surveillance harms.

The concept of "systematic" is also important from an evidentiary perspective. Individual rights interferences may not yet be documented as systematic violations, even where the infrastructure itself already has systemic qualities. A system that operates continuously, at scale, and across dispersed populations may create the conditions for systematic harm before that harm is fully realized or legally substantiated. The evidentiary challenge is therefore that SEMA is more readily aligned with evidence of recognized crises, identified actors, and substantiated wrongdoing, whereas technology-enabled harm may first appear as evidence of infrastructure, capacity, and foreseeable risk.

Canada's sanctions practice illustrates this tension. Examples from Canada's human rights-related sanctions regimes suggest that designations often include state officials, political leaders, security actors, and associates directly connected to the relevant sanctioned situation.[87] SEMA also permits measures to be directed at entities, including corporations, because the Act defines "person" to include both individuals and entities.[88] In practice, entity designations under Canadian autonomous sanctions are frequently found in country-specific regimes involving state-linked enterprises, defence-sector entities, financial institutions, military technology companies, or broader economic and security

[87] Global Affairs Canada, "Justice for Victims of Corrupt Foreign Officials Act" (15 December 2025), online: Government of Canada <https://www.international.gc.ca/world-monde/international_relations-relations_internationales/sanctions/victims_corrupt-victimes_corrompus.aspx?lang=eng>; Special Economic Measures (Myanmar) Regulations, supra note 59, s 2(b), (d)–(e); Special Economic Measures (Iran) Regulations, supra note 60, s 2(a.1)–(c); Special Economic Measures (Russia) Regulations, supra note 56, s 2(a.1)–(c).

[88] SEMA, supra note 9, ss 2, 4(1)(a)–(b). Section 2 defines "person" as including "an individual or an entity" and defines "entity" to include, among other things, a corporation, trust, partnership, fund, unincorporated association or organization, or a foreign state.

measures.[89] The more difficult question for this paper is whether SEMA is equally well suited to address private technology companies whose contribution to human rights harm lies primarily in supplying surveillance capacity rather than directly carrying out violations.

This emphasis on identifiable actors reflects both legal and policy considerations. Targeting specific individuals allows for a more direct connection between conduct and responsibility, which can support the legitimacy and defensibility of sanctions. It also aligns with broader trends in targeted or "Magnitsky-style" sanctions practice, which focused on specific actors rather than comprehensive sanctions against an entire state.[90] However, this orientation may also limit the ability of sanctions frameworks to engage with forms of harm that are mediated through corporate activity, technological infrastructure, and distributed systems.

Taken together, these evidentiary considerations point to a structural tension within SEMA. The framework is not necessarily incapable of addressing technology-enabled human rights harm. Rather, the difficulty is that the evidence most available at an early stage may demonstrate capacity, context, diffusion, and foreseeable risk, while the

---

[89] Global Affairs Canada, "Consolidated Canadian Autonomous Sanctions List" (accessed 25 May 2026), online: Government of Canada <https://www.international.gc.ca/world-monde/international_relations-relations_internationales/sanctions/consolidated-consolide.aspx?lang=eng>; Global Affairs Canada, "Canadian Sanctions Related to Russia", supra note 64; Special Economic Measures (Russia) Regulations, supra note 56, Sch 1, Parts 1–2.

[90] "Magnitsky-style" sanctions generally refer to targeted restrictive measures directed at specific foreign nationals responsible for, complicit in, or associated with gross human rights violations or significant corruption, rather than comprehensive sanctions against an entire state. See Justice for Victims of Corrupt Foreign Officials Act, supra note 10, ss 2, 4(1)–(2); SEMA, supra note 9, s 4(1.1)(c)–(d); Standing Senate Committee on Foreign Affairs and International Trade, Strengthening Canada's Autonomous Sanctions Architecture, supra note 67 at 13–15, 20–23; Global Affairs Canada, "Justice for Victims of Corrupt Foreign Officials Act", supra note 87.

evidence most clearly aligned with SEMA's existing designation practice tends to concern identified actors, recognized crises, and substantiated wrongdoing. This reinforces the broader argument of this paper: SEMA remains an important human rights-related sanctions tool, but its evidentiary orientation may constrain its ability to respond to indirect, cumulative, and capacity-based forms of harm before they become fully documented violations.

The following section builds on this analysis by examining the case of Geedge Networks in greater detail. It uses the Geedge case not to argue that surveillance capacity should automatically be treated as liability, nor to suggest that SEMA necessarily requires designation in any particular case, but to test how the structural limits identified above operate in practice. In particular, the next section considers how the export of surveillance infrastructure may create reasonably foreseeable human rights risks where technical capacity, political context, state deployment, telecommunications infrastructure, and downstream coercive use interact across borders. It then assesses how such a case exposes the attributional, evidentiary, and temporal difficulties faced by a reactive sanctions framework when the most visible concern is not yet a fully documented violation, but the provision of scalable capacity capable of enabling monitoring, censorship, and control in a repressive environment.

IV. Surveillance Capacity and the Threshold Problem under SEMA: Geedge Networks

The preceding sections have argued that technology-enabled human rights harm creates difficulties for legal frameworks structured around identifiable violations, attributable conduct, evidentiary substantiation, and post-violation responsibility. These difficulties are both exposed and amplified in the context of cross-border surveillance technology exports.

Geedge Networks (Geedge) is a useful case study not because it resolves the threshold question, but because it illustrates how surveillance capacity can be exported as infrastructure, embedded in telecommunications systems, and placed at the disposal of state authorities in contexts where misuse is reasonably foreseeable.[91]

The Geedge case can therefore serve as a stress test or form of test case for the argument developed in this paper. This does not mean that technological capacity alone should be treated as a basis for liability, nor does it establish that SEMA necessarily requires the designation of Geedge or any other technology provider, under a human-rights-related sanctions regime in any particular case. Rather, Geedge helps show why a reactive sanctions framework may struggle where the relevant human rights concern arises *before* violations are fully documented, *before* responsibility can be clearly attributed, and *before* harm can be reduced to a single discrete event or sequence of discrete events.

[91] Justice For Myanmar, Silk Road of Surveillance, supra note 15 at 1–2; InterSecLab, The Internet Coup, supra note 15 at 2–5; Yang, supra note 17.

A. China's Great Firewall and the Dual-Use Logic of Network Control

China's Great Firewall is best understood not as a single filtering tool, but as a layered technical architecture for managing, filtering, and controlling internet traffic at scale. It combines multiple techniques, including domain-name filtering, IP blocking, keyword-based filtering, connection disruption, and inspection of network traffic.[92] These techniques operate at different layers of internet infrastructure. For example, DNS-based censorship can interfere with the process by which a domain name is resolved into an IP address, while TCP reset injection or TLS interference can interrupt a connection after a user attempts to access a targeted service.[93] Deep packet inspection is more intrusive: it allows network operators to examine aspects of data packets as they move through a network, making it possible to identify, classify, or block particular types of traffic.[94]

These capabilities are not inherently unlawful or illegitimate. Network operators may use traffic management, cybersecurity monitoring, and network optimization tools to maintain service quality, detect malicious activity, manage congestion, or comply with lawful regulatory requirements.[95] In this sense, many of the technologies associated with network monitoring and filtering have a dual-use or dual-purpose character. The same

---

[92] Nart Villeneuve, "Breaching Trust: An Analysis of Surveillance and Security Practices on China's TOM-Skype Platform" (2008) Citizen Lab Research Report No 2008-01 at 4–6, online: Citizen Lab <https://idl-bnc-idrc.dspacedirect.org/items/ec95a951-1bde-4231-b857-da708b5cdd32>; Nguyen Phong Hoang et al, "How Great is the Great Firewall? Measuring China's DNS Censorship" (2021) 30th *USENIX Security Symposium* 3381 at 3381–83, online: USENIX <https://www.usenix.org/conference/usenixsecurity21/presentation/hoang>.

[93] Open Observatory of Network Interference, "China is Blocking OONI" (28 July 2023), online: OONI <https://ooni.org/post/2023-china-blocks-ooni/>; Hoang et al, supra note 92 at 3382–84.

[94] For discussion of deep packet inspection as a technology capable of examining network traffic and enabling filtering or surveillance, see Riecke, supra note 14 at 701–05; Bernal, supra note 23 at 247–50.

[95] Riecke, supra note 14 at 699–705.

technical architecture that can support cybersecurity, fraud prevention, or network reliability may also enable granular control over internet traffic, real-time monitoring, censorship, and the identification of users or communications of interest.[96] This dual-use character also helps explain the problem of neutral product framing: a system may be described in ordinary technical or commercial terms while retaining the capacity to be repurposed for censorship, surveillance, or control when deployed in a different institutional and political context. The human rights significance therefore lies not only in the existence of the technology itself, but in the relationship between its capabilities, the institutional context in which it is deployed, and the safeguards governing its use. This distinction is important for the analysis that follows. The line between legitimate network management and human rights-invasive surveillance or censorship is not always found in the technical capability alone. It may depend on *how* the system is used, for example, whether it is used to impose improper restrictions on access to information, monitor political or social activity, identify individuals for enforcement purposes, or chill the exercise of rights such as privacy, freedom of expression, and freedom of association.[97] Furthermore, in *environments* where legal safeguards are weak, independent oversight is limited, or state authorities use infrastructures (including telecommunications) for political control, dual-use systems may become part of a broader architecture of repression.

---

[96] Riecke, supra note 14 at 699–705; Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, supra note 1 at paras 1–3.

[97] Freedom House, Freedom on the Net 2025: China (2025), online: Freedom House <https://freedomhouse.org/country/china/freedom-net/2025>; Murray et al, supra note 22 at 400–09; Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, supra note 1 at paras 1–3.

The human rights significance of the Great Firewall lies not only in its technical capacity to filter, monitor, and disrupt internet traffic, but also in the way such capacity has been associated with restrictions on access to information, online expression, privacy, and political participation. Human Rights Watch describes the Great Firewall as part of a broader censorship and surveillance mechanism aimed at restricting content, identifying and locating individuals, and enabling access to personal records. At the same time, the system is also defended by some users and state-oriented narratives through the language of protection from false information, social instability, cyber sovereignty, public order, and national security. This tension illustrates why network-control technologies must be assessed not only by reference to their technical capabilities, but also by reference to the political and institutional context in which those capabilities operate.[98]

The Great Firewall example also illustrates why context matters. The human rights significance of network-control technology depends not only on what the system can technically do, but also on the political and institutional environment in which it operates. Where the state exercises significant control over telecommunications infrastructure, where legal safeguards governing surveillance and data access are weak or opaque, where independent oversight is limited, and where there are documented patterns of repression, otherwise dual-use network-control tools may acquire a heightened human rights significance. These contextual considerations become especially important when similar

[98] Yaqiu Wang, "In China, the 'Great Firewall' Is Changing a Generation" *Politico Magazine* (1 September 2020), online: Politico <https://www.politico.com/news/magazine/2020/09/01/china-great-firewall-generation-405385>.

technical architectures are exported to, sold to, or deployed within other political and institutional environments.

The relevance of this background is that the Geedge case concerns not merely the sale of isolated software or equipment, but the possible export of a technical architecture capable of being embedded within telecommunications infrastructure and placed at the disposal of state authorities.

The question, therefore, is not whether network-management capacity is inherently unlawful. Rather, it is whether the *targeted export or sale* of such infrastructure to contexts of known repression may create reasonably foreseeable human rights risks *before* specific violations are fully documented, before responsibility can be clearly attributed, and before harm can be reduced to a single discrete event or sequence of discrete events.

B. Geedge: Case Study of Capacity-Based, Infrastructure-Mediated Harm

Geedge Networks publicly presents itself as a provider of network visibility, traffic control, and security-related products.[99] Its own product materials describe Tiangou Secure Gateway, or TSG, as a network perimeter security solution that performs deep packet inspection on network traffic and classifies content through stream-based

[99] Geedge Networks, "Greater than the Edge", online: Geedge Networks <https://www.geedgenetworks.com/>; Geedge Networks, "Products", online: Geedge Networks <https://www.geedgenetworks.com/products/>.

analysis.[100] Taken in isolation, this language resembles the ordinary vocabulary of cybersecurity, traffic management, and network optimization.[101]

The significance of the Geedge case lies in the gap between the company's neutral product framing (which presents its systems as tools for network visibility, traffic control, and security) and the products' surveillance and censorship functions (attributed to the same systems through leaked materials and subsequent technical investigations).

A large dataset of Geedge-related materials was reviewed through the "Great Firewall Export investigation", involving InterSecLab, Amnesty International, Justice For Myanmar, The Globe and Mail, Paper Trail Media, the Tor Project, Der Standard, and Follow The Money.[102] Public technical discussions of the leaked Geedge materials describe more than 100,000 internal materials associated with Geedge, including Jira, Confluence, GitLab, source-code-related materials, technical documentation, and deployment files.[103]

For the purposes of this paper, the relevant issue is not simply whether Geedge is a Chinese company or whether its products which it exports or sells are formally described

---

[100] Geedge Networks, "TIANGOU Secure Gateway (TSG)", online: Geedge Networks <https://www.geedgenetworks.com/tiangou-secure-gateway-english/>.

[101] For discussion of the technical architecture of network control, including traffic filtering, deep packet inspection, cybersecurity monitoring, traffic management, network optimization, and the dual-use character of such technologies, see supra notes 92–96 and accompanying text.

[102] InterSecLab, The Internet Coup, supra note 15; Justice For Myanmar, Silk Road of Surveillance, supra note 15 at 1; Yang, supra note 17.

[103] Net4People, "Leak of Geedge Networks Internal Documents (100,000+ from Jira, Confluence, GitLab)" GitHub Issue No 519 (9 September 2025), online: GitHub <https://github.com/net4people/bbs/issues/519>; Enlace Hacktivista, "Geedge" (accessed 18 May 2026), online: Enlace Hacktivista <https://files.enlacehacktivista.org/geedge/>.

as cybersecurity or network-management tools. The critical issue is the kind of **capacity** those systems appear to provide when deployed in national telecommunications **environments**. The tension lies in the fact that the same technical architecture can be framed as ordinary network security while also functioning as infrastructure for repression when deployed in a particular political and institutional context. This tension points to the central legal and policy question developed in this section: when does the transfer of surveillance-capable infrastructure into a particular context make human rights harm reasonably foreseeable?

InterSecLab describes Geedge as offering a suite of products resembling China's Great Firewall, with capabilities including deep packet inspection, real-time monitoring of mobile subscribers, granular control over internet traffic, and censorship rules tailored to particular regions.[104] Wired similarly reports that leaked documents show Geedge packaging censorship and surveillance capabilities into a commercialized Great Firewall-style system consisting of hardware capable of being installed in telecommunications data centers and software operated by local government officials.[105]

The technical architecture suggests an infrastructure-level model of harm. InterSecLab identifies three key components of Geedge's system:[106]

- *Monitoring and Blocking*: Tiangou Secure Gateway is described as a national firewall and traffic-management solution capable of monitoring user traffic at

[104] InterSecLab, *The Internet Coup*, supra note 15 at 2–5.
[105] Yang, supra note 17.
[106] InterSecLab, *The Internet Coup*, supra note 15 at 13–18.

scale while facilitating the identification and blocking of web content and applications.[107]

- *Storage, Aggregation and Identification*: TSG Galaxy is described as a data warehouse for mass surveillance, capable of storing and aggregating internet and communications traffic and linking it to individual users through identifiers such as IP addresses, subscriber IDs, IMEI, and IMSI.[108]
- *Real-time Data Analysis, Interpretation and Monitoring:* Cyber Narrator is described as the analytical interface through which government users may access and interpret the collected data.[109] Cyber Narrator can track network traffic at the individual customer level and identify the geographic location of mobile subscribers in real time by linking their activity to specific cell identifiers.[110] Cyber Narrator can be used to monitor groups of internet users in specific geographic areas, including during protests or large crowded events.[111]

Investigative journalists with media outlets *The Diplomat* and *Heise Online* provide further corroboration of the broader export pattern and reported Geedge-related capabilities, including VPN blocking, individual-user surveillance, and, in Heise's account, malware injection.[112]

---

[107] InterSecLab, The Internet Coup, supra note 15 at 17–18.
[108] Ibid at 15–16.
[109] Ibid at 13–14.
[110] Ibid at 14.
[111] Ibid.
[112] Catherine Putz, "Did Kazakhstan Import a Commercialized Version of China's Great Firewall?" *The Diplomat* (15 September 2025), online: *The Diplomat* <https://thediplomat.com/2025/09/did-kazakhstan-

These relevant types of capability support the key analytical point for the purposes of this discussion: harm may arise not only from discrete acts of surveillance or censorship, but from the transfer of technological infrastructure capable of enabling those acts at scale. The relevant capacity is not limited to a single feature, a single intercepted communication, or a single discrete act of surveillance. They include monitoring network traffic, classifying users, identifying circumvention tools, blocking applications, locating mobile subscribers, and potentially connecting online behavior to geographic and physical identity. In this sense, Geedge provides a concrete example of *infrastructure-mediated harm*. Again, the concern is not only what a particular state actor does with the system at a particular moment, but what such a system makes possible once embedded in telecommunications infrastructure.

At the same time, *capacity* alone cannot be treated as automatically unlawful or equivalent to a completed human rights violation. As discussed above, network management, cybersecurity, and traffic filtering technologies may serve legitimate functions in some settings. The legal difficulty is therefore more precise: **how and when does the transfer of surveillance and censorship capacity into a particular political and institutional environment create a foreseeable human rights risk sufficient to justify legal or policy scrutiny?**

---

import-a-commercialized-version-of-chinas-great-firewall/>; Gesine Peymann, "Report: China's Geedge Networks Supplies Censorship Systems to Countries" *Heise Online* (10 September 2025), online: *Heise Online* <https://www.heise.de/en/news/Report-China-s-Geedge-Networks-supplies-censorship-systems-to-countries-10639548.html>.

C. Foreseeability, Context, and the Threshold Problem

In addition to technical *capacity*, the foreseeability of harm depends on the *context* into which that capacity was allegedly transferred, sold, or deployed. For the purposes of this analysis, and drawing from the China's Great Firewall example, the capacity-and-context inquiry should therefore incorporate at least two steps:

1. Technological capacity: what the system is capable of doing; and
2. Contextual analysis: the political and institutional environment into which that technological capacity is transferred, including:
    - the degree of state control over telecommunications infrastructure;
    - the availability of legal safeguards governing surveillance, interception, and access to communication data;
    - the existence of independent oversight; and
    - documented patterns of political repression, including the treatment of online activity, expression, association, or dissent as a basis for coercive enforcement.

Myanmar is the principal example considered in this section, but the broader significance of the Geedge case lies in the reported export or attempted deployment of similar Great Firewall-style capabilities in jurisdictions with prima facie restrictive information environments or weak safeguards governing surveillance and data access.[113]

[113] InterSecLab, *The Internet Coup*, supra note 15 at 2–5, 18–20; Yang, supra note 17; Peymann, supra note 112.

This does not mean that every contextual factor must be present before risk becomes legally or politically relevant. Rather, the factors identified above operate as contextual indicators. Their significance depends on their strength, their combination, and their alignment with the specific capabilities of the technology at issue.

Although technological capability provides the initial trigger for the inquiry, the analysis that follows begins with Myanmar's political and institutional context because that context establishes the baseline against which the relevant capability must be assessed. The inquiry then turns to the more specific question of alignment: whether the imported or deployed capability is capable of reinforcing existing patterns of surveillance, censorship, or coercive enforcement. In this sense, the capacity -and-context inquiry is sequential but interactive. A surveillance-capable system may trigger contextual analysis, but reasonable foreseeability depends on the relationship between what the system can do and the environment in which it is transferred, sold, or deployed.

The two-step inquiry can therefore be refined into three analytical stages. First, the export, sale, or deployment of a system with surveillance, censorship, identification, or network-control capacity may trigger further inquiry. Second, that inquiry requires both a general assessment of the importing jurisdiction's political and institutional context and a more specific assessment of whether the technology's capabilities align with existing patterns of repression or weak safeguards. Third, where capability and context strongly align, a presumption of reasonably foreseeable human rights risk may arise, subject to

rebuttal by evidence of safeguards, limited use, lack of deployment, absence of continuing support, or a weak nexus between the provider and the relevant human rights situation.

Contextual considerations - general

In Myanmar, for example, the context relevant to the alleged transfer, sale, or deployment of surveillance technology is defined by the military's attempted coup in February 2021, the junta's control over state institutions, pervasive surveillance and censorship, arbitrary arrests, internet shutdowns, and violence against critics.[114] These factors help define the political and institutional environment in which the transferred capacity would operate. For the purposes of the capacity-and-context inquiry developed in this paper, they also correspond to the contextual criteria identified above: state control, weak or opaque legal safeguards governing surveillance and data access, limited independent oversight, and documented patterns of political repression.

The fourth criterion is particularly important in the Geedge context because the relevant pattern of repression includes the treatment of online expression and digital activity as a basis for coercive enforcement. Justice For Myanmar describes Myanmar's internet environment since the attempted coup as marked by pervasive surveillance, censorship, and internet shutdowns, with online expression carrying serious risks for users.[115] In this setting, online activity is not merely expressive or private conduct;

[114] Justice For Myanmar, *Silk Road of Surveillance*, supra note 15 at 3–6.
[115] Ibid at 3.

depending on the surrounding political and institutional circumstances, it may become a trigger for surveillance, arrest, detention, or violence.

The human rights context surrounding the Geedge tech transfer is therefore not incidental. Justice For Myanmar states that telecommunications users have practiced self-censorship and limited digital resistance because of risks of arbitrary arrest, torture, enforced disappearance, and execution.[116] This point matters not only because self-censorship may precede more visible forms of coercion, but also because behavior modification can itself reflect a form of human rights interference. As discussed in Part II, surveillance may chill expression, deter association, and reduce participation in public life even before a discrete act of arrest, detention, or physical violence occurs.[117] The same report refers to nearly 1,500 arrests between 2022 and 2024 for anti-junta content on Facebook, TikTok, and Telegram, as well as additional arrests following the scanning of private messages.[118] Finance Uncovered and Myanmar Now also reported allegations that nearly 2,000 people had been arrested since the coup for criticizing the junta online or posting support for anti-regime groups.[119] These materials establish an important

---

[116] Justice For Myanmar, *Silk Road of Surveillance*, supra note 15 at 3–4.

[117] See discussion in Part II, supra notes 25, 27, 38 and accompanying text; Murray et al, supra note 22 at 400–06, 408–09.

[118] Justice For Myanmar, Silk Road of Surveillance, supra note 15 at 4.

[119] Caroline Henshaw & Aung Naing, "Chinese Technology Capable of Mass Surveillance 'Installed' by Myanmar Internet Company Funded by UK" *Finance Uncovered* (21 May 2025), online: *Finance Uncovered* <https://www.financeuncovered.org/stories/british-norwegian-and-danish-governments-back-internet-provider-in-military-run-myanmar-which-hosts-notorious-chinese-surveillance-system>; Aung Naing & Caroline Henshaw, "European Govts Back Company That Uses Chinese Tech to Monitor Myanmar Internet Users" *Myanmar Now* (23 May 2025), online: *Myanmar Now* <https://myanmar-now.org/en/news/european-govts-back-company-that-uses-chinese-tech-to-monitor-myanmar-internet-users/>.

contextual consideration: online activity is not neutral in all political and institutional environments. In some contexts, it may remain primarily expressive, private, or associational conduct. In others, particularly where state authorities have a documented practice of treating online expression as a basis for coercive enforcement, the same activity may become a trigger for surveillance, arrest, detention, or violence. For the purposes of the capacity-and-context inquiry developed in this paper, context is therefore not a background factor but a material part of the foreseeability analysis. The more closely a deployment context links online activity to coercive state action, and the weaker the legal safeguards governing surveillance and data access, the stronger the case that the transfer of high-capacity monitoring infrastructure creates a foreseeable human rights risk.

Specific Alignment Between Technical Capability and Human Rights Risk

Against this background, it is easy to see how the deployment of systems capable of individual-level tracking, traffic analysis, VPN blocking, and location identification raises some level of *foreseeable* risk to the subset of rights considered in this paper to illustrate technology-enabled human rights harm.[120] For example, individualized traffic monitoring and the linking of online activity to subscriber identifiers directly implicate the *right to privacy.* Website blocking, VPN interference, and the targeting of tools such as Signal

[120] See Part I, "Limitations of Research," above, where this paper explains that it does not seek to provide an exhaustive account of international human rights law or a comprehensive doctrinal analysis of the rights at issue, but focuses on privacy, freedom of expression, and freedom of association as rights most directly implicated in technology-enabled forms of harm. See also Part II, supra notes 36–39 and accompanying text, discussing privacy, freedom of expression, freedom of association, and the chilling effects of surveillance.

implicate *freedom of expression* and *access to information*.[121] The capacity to identify users in specific geographic areas, including protests or crowded events, implicates *freedom of association and assembly*.[122] Justice For Myanmar states that Geedge's hardware, software, and support enable the tracking of network traffic at the individual level and the real-time identification of mobile subscribers' geographic locations through cell identifiers.[123] InterSecLab provides the technical basis for this claim through its analysis of Cyber Narrator, TSG Galaxy, and Tiangou Secure Gateway (as earlier described).[124]

In the discussion that follows, "repression" is used to capture this broader pattern of rights interference. The term refers not only to direct coercive acts such as arrest or detention, but also to the use of surveillance, censorship, user identification, and network control to restrict or chill the exercise of privacy, freedom of expression, access to information, and freedom of association and assembly. This use of the term is illustrative rather than exhaustive, consistent with the limited scope of the rights analysis in this paper.

These human rights risks are heightened by the way the system is allegedly embedded in Myanmar's telecommunications infrastructure. Justice For Myanmar states that Geedge

---

[121] See International Covenant on Civil and Political Rights, 19 December 1966, 999 UNTS 171, arts 19, 21–22; UN Human Rights Committee, General Comment No 34: Article 19: Freedoms of Opinion and Expression, UN Doc CCPR/C/GC/34 (12 September 2011) at paras 11–13, 18–19; David Kaye, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc A/HRC/29/32 (22 May 2015) at paras 12–16, 54–56.
[122] InterSecLab, *The Internet Coup*, supra note 15 at 14–18; Justice For Myanmar, *Silk Road of Surveillance*, supra note 15 at 1–4.
[123] Justice For Myanmar, *Silk Road of Surveillance*, supra note 15 at 1–2.
[124] InterSecLab, *The Internet Coup*, supra note 15 at 14–18.

systems were first installed and piloted on-site in Myanmar between June and November 2022. It further reports that Geedge technicians travelled to Myanmar to conduct an environment survey, visited Myanmar Posts and Telecommunications and the National Cyber Security Center, provided training for NCSC staff, and ran test cases involving VPN blocking and the control of voice communications.[125] Justice For Myanmar also states that documents it reviewed indicate that Geedge deployed, or supported the deployment of, its systems across data centres connected to thirteen internet service providers and internet gateways in Myanmar.[126] Wired similarly reports that by February 2024, Geedge equipment had been installed in twenty-six data centres across thirteen internet service providers in Myanmar, and that one dashboard showed the system monitoring 81 million internet connections simultaneously.[127]

Legally, foreseeability of harm cannot rest on speculative assumptions about possible misuse. The Geedge case instead suggests that foreseeability may arise from the relationship between technical capacity, the political and institutional context into which that capacity is transferred, and the infrastructure through which it operates. At the first level of contextual analysis, the general legal and institutional environment matters. In a jurisdiction with effective judicial oversight, transparent authorization procedures, data protection safeguards, and meaningful remedies, the risk analysis might be different. In Myanmar, by contrast, the alleged deployment occurred against a background of military

[125] Justice For Myanmar, *Silk Road of Surveillance*, supra note 15 at 9–11.
[126] Justice For Myanmar, *Silk Road of Surveillance*, supra note 15 at 14–15, 37–38.
[127] Yang, supra note 17.

control, weak safeguards governing surveillance and data access, limited independent oversight, and documented patterns of political repression.[128] At the second level, the analysis becomes more specific: whether the technology's capabilities align with the ways in which repression already operates. This alignment is particularly significant where repression is linked to online expression or digital activity. In that setting, systems capable of traffic monitoring, VPN blocking, user identification, and location tracking may reinforce the very practices through which coercive enforcement occurs. The risk is therefore no longer abstract; it becomes foreseeable from the relationship between what the system can do and how the state has already treated online dissent.

The Geedge -Myanmar capacity-context example therefore sharpens the threshold question that runs through this paper. The issue is not simply whether Geedge directly carried out a completed human rights violation. Nor is the issue whether every network-security product capable of monitoring traffic should be suspected or treated as inherently unlawful. The nuanced question is whether the transfer of high-capacity surveillance infrastructure into particular contexts – such as a context of known repression - may create a risk sufficiently foreseeable to justify earlier legal or policy scrutiny and action. By the time specific violations are fully documented and responsibility is legally established, the underlying infrastructure may already be embedded, operational, and capable of supporting further repression.

[128] Justice For Myanmar, *Silk Road of Surveillance*, supra note 15 at 3–6.

This conclusion follows from the two-layer contextual analysis developed above. Myanmar's general political and institutional context establishes the baseline risk, while the specific alignment between Geedge's reported capabilities and existing practices of online repression explains why the risk is not merely speculative. The point is not that context alone or capacity alone is sufficient, but that their interaction sharpens the threshold question.

D. What the Geedge Case Study Reveals About SEMA

The Geedge case study helps illustrate why SEMA may face structural difficulties if applied to capacity-based, infrastructure-mediated harm. As discussed in Part III, SEMA can apply to entities as well as individuals, and its statutory language is sufficiently broad to respond to serious international situations. However, in practice, its human rights function remains tied to specific serious wrongdoing, defensible designation decisions, with identifiable nexus or connection between the targeted actor and the relevant situation. The challenge for addressing cases like Geedge is not that risk is wholly invisible. Rather, the difficulty is that risk arises through a layered chain of technological provision, state deployment, telecommunications infrastructure, and downstream coercive use.

In terms of application of SEMA, the **attribution** problem becomes particularly evident. Geedge is alleged to have provided hardware, software, training, support, and continuing technical assistance to the state of Myanmar.[129] The Myanmar junta and its

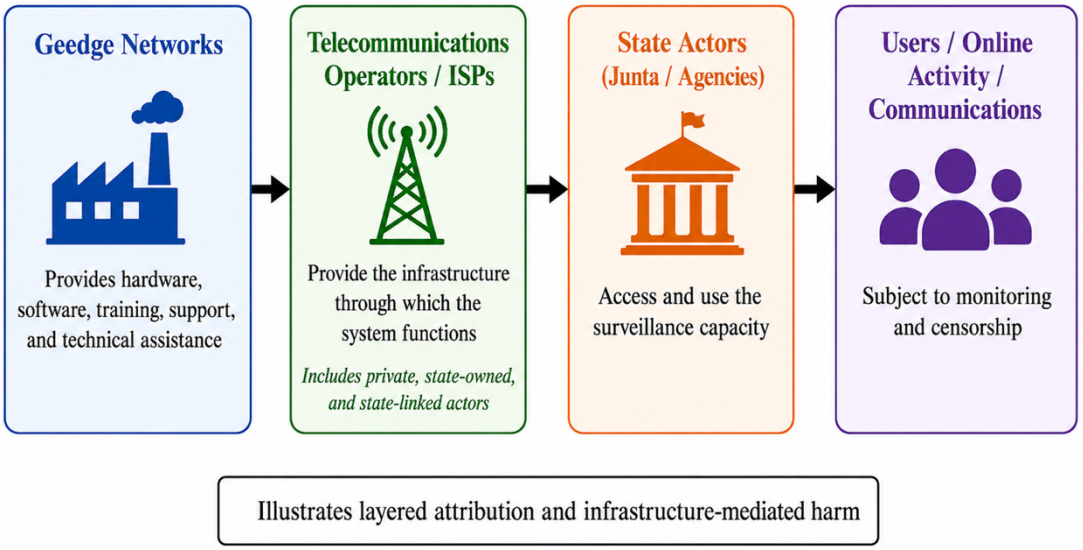
[129] Justice For Myanmar, *Silk Road of Surveillance*, supra note 15 at 1–2, 11–14.

agencies are the state actors operating within the broader repressive environment. A further layer is supplied by telecommunications operators and internet service providers, whose ownership and relationship to the state vary across the reported entities but include private, state-owned, and state-linked actors. These operators allegedly provide the infrastructure through which the system functions. Justice For Myanmar identifies thirteen telecommunications companies in Myanmar as integral to the continued functioning of Geedge's surveillance and censorship technology.[130] InterSecLab similarly reports that Geedge works directly with internet service providers to install its products, that data is captured and stored on ISP premises, and that government workers access the data remotely from command-and-control centers.[131]

[130] Justice For Myanmar, *Silk Road of Surveillance*, supra note 15 at 1–2, 15–29.

[131] InterSecLab, *The Internet Coup*, supra note 15 at 6.

Figure 1. Layered Structure of the Geedge Case



This distribution of roles makes legal characterization difficult. A technology provider may enable surveillance capacity without itself carrying out arrests, torture, or censorship orders. State actors may use the infrastructure as part of a broader apparatus of repression. Telecommunications companies may provide network premises, integration, or infrastructure access, while disputing whether they control or even know how the system is used. The Business & Human Rights Resource Centre records that Frontiir denied allegations that it had built, planned, or designed anything related to surveillance on its network, while Finance Uncovered reported that Frontiir appeared to have installed equipment developed by Geedge.[132] This assertion does not resolve the facts one way or

[132] Business & Human Rights Resource Centre, "Myanmar: ISP Company Denied Allegations Linking to the Use of Chinese Tech for Online Surveillance; incl Investors' Comments" (23 May 2025), online: Business & Human Rights Resource Centre <https://www.business-humanrights.org/en/latest-news/myanmar-isp-company-denied-allegations-linking-to-the-use-of-chinese-tech-for-online-surveillance-

another. It demonstrates why evidence and attribution may be contested even where the underlying human rights risks are serious. This point also suggests that contested evidence and attribution should operate not as reasons to ignore foreseeable risk, but as limiting considerations within the final stage of the proposed framework.

This evidentiary difficulty is also visible in the technical architecture itself. InterSecLab reports that it found no evidence that Geedge enables audit logging features that would allow observers to understand how its products are being used or abused, or how internet users' personal data are stored or shared.[133] The report further states that, across client countries, the systems are deployed in secret and lack accountability mechanisms for public oversight.[134] These features matter for sanctions analysis because they affect the ability to reconstruct the connection between system design, state use, and specific rights violations. Evidence may exist at the level of capacity, architecture, deployment, support, and foreseeable use. Yet that may not be the same as evidence of a particular violation attributable to a particular actor in the conventional sense.

The **temporal** problem follows from this uncertainty. Justice For Myanmar states that, by providing hardware and software to the Myanmar junta, Geedge may be aiding and abetting crimes against humanity, including torture and killing, while also noting that

---

incl-investors-comments/>; Caroline Henshaw & Aung Naing, "Chinese Technology Capable of Mass Surveillance 'Installed' by Myanmar Internet Company Funded by UK" *Finance Uncovered* (21 May 2025), online: *Finance Uncovered* <https://www.financeuncovered.org/stories/british-norwegian-and-danish-governments-back-internet-provider-in-military-run-myanmar-which-hosts-notorious-chinese-surveillance-system>.

[133] InterSecLab, *The Internet Coup*, supra note 15 at 4–5.

[134] Ibid.

further investigation is required.[135] That formulation captures the gap at the center of this paper. The risk may be visible at the level of technological capacity and political context, but legal responsibility may remain contested or under-investigated. A sanctions framework such as SEMA may therefore face difficulty where the strongest evidence shows that a system can foreseeably enable repression, but the evidentiary record does not yet clearly establish completed violations reasonably attributable or meaningfully connected to the technology provider.

The Geedge case also illustrates the practical limits of targeted sanctions where surveillance infrastructure is designed to be resilient. InterSecLab states that Geedge's products are designed for interoperability with a wide range of commercial hardware vendors, which may make targeted sanctions more challenging.[136] Wired similarly reports that Geedge appears able to repurpose existing infrastructure, and quotes an Amnesty technologist as observing that once sensitive technology has been exported, it may remain available for reuse.[137] This does not mean sanctions are irrelevant. It suggests that sanctions may have expressive, signaling, and deterrent value, while still being limited in their capacity to dismantle already-embedded technological systems.

The case therefore does not show that capacity should automatically be treated as liability. Nor does it prove that SEMA is incapable of addressing technology-enabled human rights harm. Rather, it shows why the legal threshold question is difficult. Where a

[135] Justice For Myanmar, *Silk Road of Surveillance*, supra note 15 at 2, 30–33.
[136] InterSecLab, *The Internet Coup*, supra note 15 at 4–5.
[137] Yang, supra note 17.

company provides surveillance infrastructure with known capabilities, where that infrastructure is transferred into a context of documented repression, and where the system can support monitoring, censorship, and user identification at scale, the human rights risk may become reasonably foreseeable before responsibility becomes legally straightforward. This is the gap identified in the earlier sections of this paper: the gap between foreseeable capacity-based risk and actionable harm.

In this respect, Geedge brings together the structural features discussed in Part II and the legal limits identified in Part III. The harm is infrastructure-mediated because it operates through national telecommunications systems rather than isolated acts. It is indirect because the provider of the technology may not be the same actor that ultimately arrests, censors, or tortures. It is diffuse because responsibility is distributed among technology providers, state agencies, telecommunications operators, and support networks. It presents evidentiary difficulties because system use may be secret, technically complex, and difficult to audit. It is temporal because risk becomes visible before violations are fully substantiated. The broader implication is not that sanctions law should abandon legality, evidence, or attribution. Rather, cases such as Geedge reveal a structural mismatch between capacity-based harm and post-violation legal design.

E. Refining the Capacity-and-Context Inquiry

The preceding analysis suggests that the capability-and-context inquiry can be refined into three stages. The first stage is a capability threshold. The inquiry is triggered where the exported, sold, or deployed system appears to provide surveillance, censorship,

identification, or network-control capacity. In the Geedge example, this includes capabilities such as monitoring and blocking, storage, aggregation and identification, and real-time data analysis, interpretation, and monitoring. Capacity alone is not sufficient to establish legal responsibility, but it identifies the type of system that may require further scrutiny.

At an operational level, this framework does not imply random or routine review of every technology transfer. An inquiry could instead be initiated where credible information indicates that a system with relevant surveillance, censorship, identification, or network-control capabilities has been exported, sold, deployed, or supported in a potentially high-risk environment. Such information may arise from complaints, civil society or investigative reporting, technical research, export-control or other regulatory processes, or information otherwise available to government. The capability threshold would then determine whether that information warrants the more structured contextual inquiry developed below. The precise institutional allocation and procedural design of such screening fall outside the scope of this paper.

The second stage is a contextual threshold. This stage has two related dimensions. The first is a general jurisdictional assessment of the political and institutional environment into which the technology is transferred. Relevant criteria include the degree of state control over telecommunications infrastructure, the availability of legal safeguards governing surveillance, interception, and access to communications data, the existence of independent oversight, and documented patterns of political repression, including the treatment of

online activity, expression, association, or dissent as a basis for coercive enforcement. The second is a more specific alignment inquiry: whether the system's capabilities reinforce or intensify the existing risks in that environment. This is where the analysis asks whether capabilities such as traffic monitoring, VPN blocking, user identification, location tracking, or large-scale data aggregation align with existing practices of surveillance, censorship, or coercive enforcement.

The third stage concerns rebuttal or limiting considerations. Even where capability and context strongly align, the result should not be automatic designation or liability. The presumption of reasonably foreseeable human rights risk may be limited or rebutted by evidence of safeguards, legitimate use, lack of deployment, absence of continuing technical support, contested evidence, lack of knowledge, distributed responsibility among technology providers, state actors, and telecommunications operators, or a weak nexus between the provider and the relevant human rights situation. These considerations are especially important under a sanctions framework such as SEMA, where legal and policy action must remain attentive to evidence, attribution, legality, and proportionality.

The foundational question is therefore not whether surveillance capacity alone should trigger sanctions, but when the interaction between technical capability, deployment context, and available evidence reaches a threshold of reasonable foreseeability sufficient to justify preventive legal or policy scrutiny. Further SEMA-specific analysis is still required, but the Geedge case helps identify the kind of framework through which

technology-enabled human rights risk can be assessed before harm is fully documented or responsibility is legally straightforward.

V. SEMA and the Possibility of Preventive Human Rights Protection

The preceding chapters have placed SEMA under a particular kind of pressure. Part II argued that technology-enabled human rights harm may be anticipatory, cumulative, diffuse, and mediated through infrastructure rather than through a single identifiable act. Part III showed that SEMA, while flexible, remains structured around serious situations that have already crystallized into legally and politically recognizable forms of wrongdoing. Part IV then used the Geedge case to show how this tension becomes concrete in the context of cross-border surveillance technology exports, and suggested a first iteration of a capacity-and-context framework for assessing when foreseeable human rights harm may justify sanctions-related scrutiny. In such cases, the risk may be visible before responsibility is straightforward; the infrastructure may be operational before individual violations are fully documented; and the actor who supplies the technological capacity may not be the same actor who ultimately censors, detains, or harms users.[138]

This final substantive chapter considers what follows from that analysis. The answer is not that SEMA should be transformed into a general technology-governance statute. Nor is it that technological capacity should automatically be treated as sanctionable conduct. Such conclusions would overstate both the design of SEMA and the argument developed in this paper. The more careful point is that SEMA may still have a limited preventive role, provided that prevention is understood realistically. In this context, prevention does not

[138] See Part II, discussing infrastructure-mediated, cumulative, and anticipatory human rights harm; see also Part IV, discussing the Geedge case as an example of capacity-based, infrastructure-mediated harm. See also Murray et al, supra note 22 at 397–409; Bernal, supra note 23 at 247–50.

mean that SEMA can screen every risky technology export before it occurs. Rather, it means that SEMA may help interrupt, stigmatize, or deter continued support for technological infrastructures that have become sufficiently connected to serious human rights situations.[139]

A. Prevention Within a Reactive Framework

SEMA's preventive potential is constrained by its legal form. The Act authorizes economic measures through orders and regulations where statutory conditions are met, including situations involving a grave breach of international peace and security or gross and systematic human rights violations in a foreign state.[140] Its practical mechanisms include asset freezes, prohibitions on dealings, and restrictions on making property, goods, or services available to listed persons or entities.[141] These are powerful tools, but they are not designed as *ex ante* licensing requirements. SEMA does not require exporters of surveillance technology to conduct human rights due diligence, assess end-users, or obtain prior authorization before transferring a system to a high-risk jurisdiction.[142]

This distinction matters because as earlier described, technology-enabled harm often emerges before a sanctions threshold is easy to satisfy. A surveillance system may be marketed as cybersecurity or network-management technology; exported as ordinary

---

[139] McTaggart, supra note 54 at 1–5; Charron, supra note 12 at 3–6; Standing Senate Committee on Foreign Affairs and International Trade, Strengthening Canada's Autonomous Sanctions Architecture, supra note 67 at 13–24.
[140] SEMA, supra note 9, ss 3.1, 4(1), 4(1.1)(b)–(c).
[141] Ibid, ss 4(1)–(2); Global Affairs Canada, "Canadian Sanctions: Essential Information", supra note 10.
[142] Compare Office of the United Nations High Commissioner for Human Rights, Guiding Principles on Business and Human Rights, supra note 47, principles 17–21; OECD, OECD Guidelines for Multinational Enterprises on Responsible Business Conduct (Paris: OECD Publishing, 2023), ch IV, especially paras 45–51; see also ch IX.

commercial infrastructure; integrated into telecommunications networks; and only later become publicly visible as part of a broader apparatus of repression. By that point, the system may already be embedded in state or telecommunications infrastructure, making the harm more difficult to prevent and the evidentiary record more difficult to reconstruct.[143]

Yet SEMA should not be dismissed as merely retrospective. Sanctions have always carried a prospective dimension. They do not only express condemnation for past conduct; they can also shape future behavior by restricting economic relationships, increasing reputational costs, and signaling that certain actors or forms of support fall outside acceptable engagement.[144] This is particularly important where the relevant harm depends not only on an initial transfer, but on continuing relationships of installation, training, maintenance, technical assistance, financing, or access to commercial intermediaries. In such cases, sanctions may not undo the original deployment, but they may make it harder for the infrastructure to expand, receive support, or become normalized.[145]

SEMA's preventive role is therefore best understood as indirect and secondary. It is not a comprehensive preventive regime. It cannot replace export controls or due diligence obligations. But once the factual record shows a serious situation and a defensible connection between an actor and that situation, SEMA may help prevent further

---

[143] Justice For Myanmar, *Silk Road of Surveillance*, supra note 15 at 1–2, 9–15; InterSecLab, *The Internet Coup*, supra note 15 at 4–6, 13–18.

[144] Lopez, supra note 41 at 772–76; McTaggart, supra note 54 at 1–2.

[145] Justice For Myanmar, *Silk Road of Surveillance*, supra note 15 at 9–15, 30–33; InterSecLab, *The Internet Coup*, supra note 15 at 4–6.

entrenchment of harmful infrastructure. This is a narrower claim than saying that SEMA can prevent technology-enabled harm at the point of origin. It is also a more plausible one.

B. From Capacity to Context: When Risk Becomes Legally Salient

The central difficulty is determining when risk becomes sufficiently concrete to matter for legal and policy purposes. The analysis in the preceding chapters suggests that this cannot be answered by looking at technical capacity alone. Many surveillance-related technologies are dual-use.[146] As discussed above, the problem arises when those same capabilities are transferred into contexts where legal safeguards are weak, state authorities exercise coercive control over telecommunications infrastructure, and online expression is already treated as a basis for repression.[147]

This is why a capacity-and-context inquiry is useful. It does not replace SEMA's statutory requirements, and it should not be mistaken for a rigid legal test. Rather, it helps organize the kinds of considerations that may show when a risk has moved beyond abstraction.

The capacity-and-context inquiry developed in Part IV provides a way of organizing this problem without replacing SEMA's statutory requirements. It begins by asking what the system is capable of doing, including whether it enables real-time monitoring,

---

[146] Eg Deep packet inspection, traffic analysis, network visibility, and content filtering may be used for legitimate purposes in some settings, including cybersecurity, network reliability, and lawful regulatory compliance. Riecke, supra note 14 at 699–705; Office of the United Nations High Commissioner for Human Rights, *The Right to Privacy in the Digital Age*, supra note 1 at paras 1–3.

[147] Justice For Myanmar, *Silk Road of Surveillance*, supra note 15 at 3–6; Murray et al, supra note 22 at 400–409.

subscriber identification, location tracking, VPN blocking, content classification, or large-scale aggregation of communications data.[148] That **capacity** must then be assessed in light of the legal and institutional safeguards governing its deployment.[149] The purpose is not to treat **capacity** itself as liability, but to identify when the interaction between **capability** and **context** makes a risk sufficiently concrete to warrant closer scrutiny.

The inquiry must also preserve the need for an identifiable nexus between the targeted actor, the relevant conduct, and the international situation.[150] In technology cases, that nexus may arise through provision, installation, training, continuing technical support, system integration, financing, or assistance after serious risks have become apparent.[151] Foreseeability therefore depends not on the abstract possibility that any technology could be misused, but on whether intrusive capacity, a high-risk deployment context, the relevant nexus, and the available evidence converge.[152] This does not create an alternative sanctions test. It structures the assessment of when technology-enabled risk has moved beyond abstraction before the ordinary statutory questions of designation and legal authority are reached.

---

[148] InterSecLab, *The Internet Coup*, supra note 15 at 13–18; Justice For Myanmar, *Silk Road of Surveillance*, supra note 15 at 1–2.

[149] Justice For Myanmar, *Silk Road of Surveillance*, supra note 15 at 3–6; Office of the United Nations High Commissioner for Human Rights, *The Right to Privacy in the Digital Age*, supra note 1 at paras 49, 53(c), 53(f), 54(a)–(b).

[150] See Part III, discussing SEMA's focus on listed persons or entities and defensible designation decisions; see also Makarov, supra note 57 at paras 51–53, 76–85.

[151] Justice For Myanmar, *Silk Road of Surveillance*, supra note 15 at 9–15, 30–33; InterSecLab, *The Internet Coup*, supra note 15 at 4–6.

[152] Justice For Myanmar, *Silk Road of Surveillance*, supra note 15 at 3–6; Murray et al, supra note 22 at 400–409.

This framing preserves an important **balance**. It avoids treating capacity itself as liability. It also avoids waiting until the harm is fully complete, publicly documented, and legally attributable before any legal or policy concern can arise. The relevant question is not whether sanctions should follow every risky transfer, but whether certain combinations of capacity, context, nexus, and evidence should trigger earlier scrutiny.

The capacity-and-context inquiry developed in the preceding chapter should therefore be understood as an organizing framework rather than a substitute for SEMA's statutory requirements. Its value lies in identifying when technology-enabled human rights risk has become sufficiently concrete to warrant legal or policy scrutiny, while preserving limits based on evidence, attribution, nexus, and the possibility of rebuttal. In this sense, the framework helps clarify when preventive scrutiny may be justified without collapsing capacity into liability.

C. SEMA Within a Broader Preventive Architecture

The comparative materials considered in this paper show why SEMA cannot bear the entire preventive burden. Export controls operate at an earlier point in the chain. The European Union's dual-use framework, for example, specifically addresses cyber-surveillance items and includes a mechanism for controlling non-listed items where they may be intended for use in connection with internal repression or serious human rights or international humanitarian law violations.[153] The European Commission's cyber-

[153] Regulation (EU) 2021/821, supra note 19, arts 2(20), 5.

surveillance guidelines are aimed at helping exporters assess such risks before export.[154] This is structurally different from SEMA. It focuses on the transfer before it occurs, rather than on the designation of an actor after a serious situation has already become apparent.

The United States has also used export-control tools to respond to surveillance-related human rights risks, including through Entity List designations where entities have enabled human rights abuses.[155] These measures are not the same as Canadian sanctions under SEMA, but they show how human rights concerns can be addressed through end-user restrictions, export licensing, and control over access to sensitive technologies. Australia's thematic human rights sanctions framework offers a different lesson. By applying to serious human rights violations wherever they occur, it provides a structure less dependent on country-specific regimes, although it still requires evidence and legal thresholds.[156]

These models should not be copied uncritically. Canada's legal framework, foreign-policy practice, and institutional design are different. **But they point to a broader lesson: foreseeable technology-enabled human rights harm is unlikely to be addressed effectively through one legal tool alone.** Export controls are better suited to screening transfers. Human rights due diligence is better suited to assessing customers, end-users,

---

[154] Commission Recommendation (EU) 2024/2659 of 11 October 2024 on guidelines on the export of cyber-surveillance items under Article 5 of Regulation (EU) 2021/821, [2024] OJ L 2024/2659; European Commission, "Commission publishes guidelines for cyber-surveillance exporters", supra note 19.

[155] US Department of Commerce, Bureau of Industry and Security, "Commerce Adds 8 Entities to the Entity List for Enabling Human Rights Abuses", supra note 18; Export Administration Regulations: Crime Controls and Expansion/Update of U.S. Persons Controls, supra note 18.

[156] Australian Department of Foreign Affairs and Trade, "Serious violations or serious abuses of human rights sanctions framework", supra note 20; Autonomous Sanctions Amendment (Magnitsky-style and Other Thematic Sanctions) Act 2021 (Cth), supra note 20.

and deployment contexts. Procurement and investment rules can reduce public or institutional support for high-risk suppliers. Transparency requirements, technical audits, civil society investigations, and investigative journalism can help reveal the architecture of harm before responsibility is fully settled.[157] SEMA enters this landscape later, but it can still matter where Canada can identify actors sufficiently connected to a serious situation and impose measures that restrict dealings, signal condemnation, and deter further support.[158]

This layered approach avoids two overstatements. It avoids the claim that SEMA is irrelevant because it is reactive. It also avoids the claim that SEMA can become a complete preventive regime by interpretation alone. The better view is that SEMA has a limited but meaningful role within a broader preventive architecture. Its value lies in responding to serious situations once a certain threshold is met, while reinforcing other tools that operate earlier in the technology-transfer chain.

This understanding also helps clarify the broader implication of the Geedge case. The case does not prove that capacity should be treated as liability. Nor does it prove that SEMA is incapable of addressing technology-enabled human rights harm. Rather, it shows that the

---

[157] Office of the United Nations High Commissioner for Human Rights, *Guiding Principles on Business and Human Rights*, supra note 47, principles 17–21; OECD Guidelines, supra note 142, ch IV; Regulation (EU) 2021/821, supra note 19, arts 5, 15; Commission Recommendation (EU) 2024/2659, supra note 154; see also InterSecLab, *The Internet Coup*, supra note 15 at 10–11; Justice For Myanmar, *Silk Road of Surveillance*, supra note 15 at 1.

[158] SEMA, supra note 9, ss 4(1)–(2); McTaggart, supra note 54 at 1–5; Global Affairs Canada, "Canadian Sanctions: Essential Information", supra note 10.

legal threshold problem must be understood in light of how contemporary harm is produced. Where a company supplies surveillance infrastructure with known intrusive capabilities, where that infrastructure is transferred into a context of documented repression, and where the system can support monitoring, censorship, identification, or coercive enforcement at scale, the human rights risk may become reasonably foreseeable before responsibility becomes legally straightforward.[159]

The challenge for Canada is therefore not simply whether SEMA can be used more often. It is whether SEMA can be situated more coherently within a wider set of preventive safeguards. If export controls identify risky transfers, SEMA may reinforce them by targeting actors who continue to support repressive infrastructure. If due diligence processes reveal foreseeable harm, SEMA may provide a foreign-policy response where the situation becomes sufficiently grave. If technical investigations expose infrastructure-mediated repression, SEMA may help translate those findings into legal and political consequences.

Prevention, in this sense, does not always mean acting before any risk exists. In the context of technology-enabled human rights harm, it may mean acting before risk becomes entrenched, before infrastructure becomes normalized, before support relationships become routine, and before responsibility becomes impossible to reconstruct. SEMA is not the complete answer to that problem. But used carefully, it can contribute to a broader

---

[159] Justice For Myanmar, *Silk Road of Surveillance*, supra note 15 at 1–6, 9–15; InterSecLab, *The Internet Coup*, supra note 15 at 4–6, 13–18.

architecture of human rights protection by making clear that Canada's response is not limited to those who directly commit violations, but may also extend to actors that materially support the infrastructure through which foreseeable violations become possible.[160]

[160] See Part I, "Limitations of Research,"; see also Part II, discussing infrastructure-mediated and anticipatory harm.

Conclusion

This research has examined the extent to which Canada's *Special Economic Measures Act* (SEMA) can engage with foreseeable, technology-enabled human rights harm. Through the case study of Geedge Networks, it has shown that surveillance-related risks may emerge through technological capacity, infrastructure, and institutional context before specific violations are fully documented or formally recognized. The case illustrates a central difficulty for sanctions law: human rights harm enabled by digital infrastructure may become reasonably foreseeable before legal responsibility becomes straightforward.

The analysis has argued that SEMA remains predominantly reactive in both its statutory design and practical operation. The legal thresholds embedded within the Act reflect a framework that is generally triggered only after a situation has reached a sufficient level of seriousness and visibility. This is consistent with the traditional function of sanctions as instruments of response and pressure. However, it creates difficulties where the relevant concern is not simply a completed violation, but a foreseeable risk arising from the transfer, deployment, or support of surveillance infrastructure.

The Geedge case highlights this difficulty. Its significance does not lie in proving that technological capacity alone should attract sanctions, nor in suggesting that any particular designation is legally required. Rather, it shows how infrastructure providers may occupy an important enabling position within broader systems of surveillance and control. Where such systems are transferred into political and institutional environments marked by weak

safeguards, state control over telecommunications infrastructure, and documented repression, the risk of human rights harm may become more than speculative.

At the same time, this research has shown that SEMA should not be dismissed simply because it is reactive. Although the Act is not designed to function as a comprehensive preventive mechanism, it may still play a limited preventive role within a broader legal and policy architecture. Once a sufficient evidentiary record exists, and once a defensible connection can be established between an actor and a serious human rights situation, sanctions may help prevent the further consolidation of harmful technological infrastructure by increasing economic, legal, and reputational costs. In this sense, SEMA occupies an intermediate position between retrospective accountability and earlier regulatory tools such as export controls, corporate human rights due diligence, procurement safeguards, and transparency requirements.

This research is necessarily subject to several limitations. First, the analysis is centered on a single case study. While Geedge Networks provides a useful illustration of the challenges posed by technology-enabled human rights harm, the findings should not be assumed to apply uniformly across all technology providers, surveillance companies, or digital infrastructure actors. Different technologies, commercial relationships, and political environments may generate different forms of risk and may engage sanctions frameworks in different ways. Second, the analysis relies primarily on publicly available information, including government documents, sanctions materials, investigative reporting, and civil society research. Access to internal corporate records, contractual arrangements, and

government communications remains limited. The conclusions reached in this paper should therefore be understood within those evidentiary constraints. Finally, this paper does not seek to establish a definitive legal threshold for when foreseeable technological risk should trigger sanctions measures. Determining when technological capacity becomes sufficiently connected to potential human rights harm remains a complex legal and policy question that requires further research.

Beyond its implications for Canadian sanctions policy, this research highlights a broader challenge for contemporary human rights governance. Traditional accountability frameworks are generally designed to respond to harms that have already occurred. Technology-enabled human rights risks, by contrast, may emerge through infrastructure, capacity, and foreseeability rather than immediately visible acts. The Geedge case demonstrates that some of the most serious concerns may arise when the technological conditions enabling repression are already being embedded, even though the resulting violations may not yet be fully visible or legally attributable.

This does not mean that SEMA should be transformed into a general technology-governance statute, or that technological capacity alone should become a basis for sanctions. The more careful conclusion is that technology-enabled human rights harm is placing pressure on the boundary between accountability and prevention. As surveillance infrastructure becomes increasingly central to the exercise of state power, legal frameworks will need to confront risks that are reasonably foreseeable before they fully materialize as documented violations. SEMA is not a complete answer to that problem. Used carefully,

however, it may contribute to a wider preventive architecture by making clear that Canada's response to serious human rights situations need not be limited only to those who directly commit violations, but may also extend to actors that materially support the infrastructure through which foreseeable violations become possible.

Bibliography

Legislation

Canada

Justice for Victims of Corrupt Foreign Officials Act, SC 2017, c 21.

Special Economic Measures Act, SC 1992, c 17.

Special Economic Measures (Iran) Regulations, SOR/2010-165.

Special Economic Measures (Myanmar) Regulations, SOR/2007-285.

Special Economic Measures (Russia) Regulations, SOR/2014-58.

Foreign and International

Autonomous Sanctions Amendment (Magnitsky-style and Other Thematic Sanctions) Act 2021 (Cth).

Commission Recommendation (EU) 2024/2659 of 11 October 2024 on guidelines on the export of cyber-surveillance items under Article 5 of Regulation (EU) 2021/821, [2024] OJ L 2024/2659.

Export Administration Regulations: Crime Controls and Expansion/Update of U.S. Persons Controls, 89 Fed Reg 60998 (29 July 2024), online: *Federal Register* <https://www.federalregister.gov/documents/2024/07/29/2024-16498/export-administration-regulations-crime-controls-and-expansionupdate-of-us-persons-controls>.

International Covenant on Civil and Political Rights, 19 December 1966, 999 UNTS 171.

Online Safety Act 2021 (Cth).

Online Safety Act 2023 (UK), c 50.

Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items, [2021] OJ L 206/1.

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), [2024] OJ L 1689.

Rio Declaration on Environment and Development, UN Doc A/CONF.151/26 (1992).

United Nations Declaration on the Rights of Indigenous Peoples, GA Res 61/295 (2007).

Jurisprudence

Canada

Canadian Dredge & Dock Co v The Queen, [1985] 1 SCR 662.

Club Resorts Ltd v Van Breda, 2012 SCC 17, [2012] 1 SCR 572.

Makarov v Canada (Minister of Foreign Affairs), 2024 FC 1234.

Secondary Materials

Books and Book Chapters

Dupont, Pierre-Emmanuel, "Human Rights Implications of Sanctions" in Masahiko Asada, ed, *Economic Sanctions in International Law and Practice* (Abingdon: Routledge, 2019) 37.

Lopez, George A, "Enforcing Human Rights Through Economic Sanctions" in Dinah Shelton, ed, *The Oxford Handbook of International Human Rights Law* (Oxford: Oxford University Press, 2013) 770.

Nixon, Rob, *Slow Violence and the Environmentalism of the Poor* (Cambridge, Mass: Harvard University Press, 2011).

Nossal, Kim Richard, Stéphane Roussel & Stéphane Paquin, *The Politics of Canadian Foreign Policy*, 4th ed (Montreal & Kingston: McGill-Queen's University Press, 2015).

Journal Articles and Conference Papers

Bernal, Paul, "Data Gathering, Surveillance and Human Rights: Recasting the Debate" (2016) 1:2 *Journal of Cyber Policy* 243, online: <https://doi.org/10.1080/23738871.2016.1228990>.

De Gregorio, Giovanni & Roxana Radu, "Digital Constitutionalism in the New Era of Internet Governance" (2022) 30:1 *International Journal of Law and Information Technology* 68.

Hoang, Nguyen Phong et al, "How Great is the Great Firewall? Measuring China's DNS Censorship" (2021) 30th USENIX Security Symposium 3381, online: USENIX <https://www.usenix.org/conference/usenixsecurity21/presentation/hoang>.

Mantelero, Alessandro & Maria Samantha Esposito, "An Evidence-Based Methodology for Human Rights Impact Assessment (HRIA) in the Development of AI Data-Intensive Systems" (2021) 41 *Computer Law & Security Review* 105561.

Murray, Daragh et al, "The Chilling Effects of Surveillance and Human Rights: Insights from Qualitative Research in Uganda and Zimbabwe" (2024) 16:1 *Journal of Human Rights Practice* 397.

Nesbitt, Michael, "Canada's 'Unilateral' Sanctions Regime Under Review: Extraterritoriality, Human Rights, Due Process, and Enforcement in Canada's Special Economic Measures Act" (2017) 48:2 *Ottawa L Rev* 507.

Penney, Jonathon W, "Chilling Effects: Online Surveillance and Wikipedia Use" (2016) 31:1 *Berkeley Technology Law Journal* 117.

Rautenberg, Niclas & Daragh Murray, "Making Tangible the Long-Term Harm Linked to the Chilling Effects of AI-enabled Surveillance: Can Human Flourishing Inform Human Rights?" (2024) 25 *Human Rights Review* 293.

Riecke, Lena, "Unmasking the Term 'Dual Use' in EU Spyware Export Control" (2023) 34:3 *European Journal of International Law* 697, online: <https://doi.org/10.1093/ejil/chad039>.

Saunders, Michael, "Capabilities and Gaps in the Canadian Special Economic Measures Act Regime" (2023) 29:1 *Canadian Foreign Policy Journal* 1, online: Taylor & Francis <https://www.tandfonline.com/doi/full/10.1080/11926422.2022.2145323>.

Teo, Sue Anne, "Artificial Intelligence and Its 'Slow Violence' to Human Rights" (2025) 5 *AI and Ethics* 2265.

Villeneuve, Nart, "Breaching Trust: An Analysis of Surveillance and Security Practices on China's TOM-Skype Platform" (2008) Citizen Lab Research Report No 2008-01, online: Citizen Lab <https://idl-bnc-idrc.dspacedirect.org/items/ec95a951-1bde-4231-b857-da708b5cdd32>.

Reports, Briefs, and Institutional Materials

Allard International Justice and Human Rights Clinic, *Brief to the House of Commons Standing Committee on Foreign Affairs and International Development on Canada's Human Rights Sanctions Regime* (13 December 2023), online (pdf): Peter A Allard School of Law <https://allard.ubc.ca/sites/default/files/2024-01/Allard%20IJHR%20Clinic%20Brief%20to%20FAAE%20on%20Canada%27s%20Sanctions%20Regime_final.pdf>.

Amnesty International, *Uncovering the Iceberg: The Digital Surveillance Crisis Wrought by States and the Private Sector*, DOC 10/4491/2021 (23 July 2021), online: Amnesty International <https://www.amnesty.org/en/documents/doc10/4491/2021/en/>.

Australian Department of Foreign Affairs and Trade, "Serious violations or serious abuses of human rights sanctions framework" (accessed 2 June 2026), online: DFAT <https://www.dfat.gov.au/international-

relations/security/sanctions/sanctions-regimes/serious-violations-or-serious-abuses-human-rights-sanctions-framework>.

Charron, Andrea, "Canada's Sanctions Regime" (Brief submitted to the House of Commons Standing Committee on Foreign Affairs and International Development, 3 June 2023), online (pdf): House of Commons <https://www.ourcommons.ca/Content/Committee/441/FAAE/Brief/BR12534345/br-external/CharronAndrea-e.pdf>.

European Commission, "Commission publishes guidelines for cyber-surveillance exporters" (16 October 2024), online: European Commission <https://policy.trade.ec.europa.eu/news/commission-publishes-guidelines-cyber-surveillance-exporters-2024-10-16_en>.

Feldstein, Steven, *The Global Expansion of AI Surveillance* (Washington, DC: Carnegie Endowment for International Peace, 2019).

Freedom House, *Freedom on the Net 2024* (Washington, DC: Freedom House, 2024), online (pdf): Freedom House <http://freedomhouse.org/sites/default/files/2024-10/FREEDOM-ON-THE-NET-2024-DIGITAL-BOOKLET.pdf>.

Freedom House, *Freedom on the Net 2025: China* (2025), online: Freedom House <https://freedomhouse.org/country/china/freedom-net/2025>.

Global Affairs Canada, "Canadian Sanctions Related to Russia" (accessed 25 May 2026), online: Government of Canada <https://www.international.gc.ca/world-monde/international_relations-relations_internationales/sanctions/russia-russie.aspx?lang=eng>.

Global Affairs Canada, "Canadian Sanctions: Essential Information" (18 March 2026), online: Government of Canada <https://www.international.gc.ca/world-monde/international_relations-relations_internationales/sanctions/essential-informations-essentielles.aspx?lang=eng>.

Global Affairs Canada, "Consolidated Canadian Autonomous Sanctions List" (accessed 25 May 2026), online: Government of Canada <https://www.international.gc.ca/world-monde/international_relations-relations_internationales/sanctions/consolidated-consolide.aspx?lang=eng>.

Global Affairs Canada, "Justice for Victims of Corrupt Foreign Officials Act" (15 December 2025), online: Government of Canada <https://www.international.gc.ca/world-monde/international_relations-relations_internationales/sanctions/victims_corrupt-victimes_corrompus.aspx?lang=eng>.

House of Commons, Standing Committee on Foreign Affairs and International Development, *Canada's Sanctions Regime: Transparency, Accountability and Effectiveness*, 44th Parl, 1st Sess, No 23 (January 2024).

InterSecLab, *The Internet Coup: A Technical Analysis on How a Chinese Company is Exporting the Great Firewall to Autocratic Regimes* (September 2025), online: InterSecLab <https://interseclab.org/research/the-internet-coup/>.

International Law Commission, *Articles on Responsibility of States for Internationally Wrongful Acts*, UN Doc A/56/10 (2001).

Justice For Myanmar, *Silk Road of Surveillance: The Role of China's Geedge Networks and Myanmar Telecommunications Operators in the Junta's Digital Terror Campaign* (2025), online (pdf): Justice For Myanmar <https://jfm-files.s3.us-east-2.amazonaws.com/public/Silk+Road+of+Surveillance+EN.pdf>.

Kaye, David, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, UN Doc A/HRC/29/32 (22 May 2015).

Marczak, Bill et al, *Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries*, Citizen Lab Research Report No 113 (Toronto: University of Toronto, September 2018), online: Citizen Lab <https://citizenlab.ca/research/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/>.

McTaggart, Scott, *Sanctions: The Canadian and International Architecture*, Library of Parliament Publication No 2019-45-E (Ottawa: Library of Parliament, 18 November 2019), online: Library of Parliament <https://lop.parl.ca/sites/PublicWebsite/default/en_CA/ResearchPublications/201945E>.

National Institute of Standards and Technology, *NIST IR 8006: NIST Cloud Computing Forensic Science Challenges* (Gaithersburg, MD: NIST, 2020), online (pdf): NIST <https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8006.pdf>.

OECD, *OECD Guidelines for Multinational Enterprises on Responsible Business Conduct* (Paris: OECD Publishing, 2023).

Office of the United Nations High Commissioner for Human Rights, *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework*, UN Doc HR/PUB/11/04 (2011).

Office of the United Nations High Commissioner for Human Rights, *Mapping Report: Human Rights and New and Emerging Digital Technologies*, UN Doc A/HRC/56/45 (20 August 2024).

Office of the United Nations High Commissioner for Human Rights, *The Right to Privacy in the Digital Age*, UN Doc A/HRC/60/45 (29 August 2025), online (pdf): OHCHR <https://www.ohchr.org/en/documents/thematic-reports/ahrc6045-right-privacy-digital-age-report-office-united-nations-high>.

Privacy and Civil Liberties Oversight Board, *Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court* (23 January 2014).

Rosenblat, Mariana Olaizola, Ayushi Agrawal & Isaac Yap, *Online Safety Regulations Around the World: The State of Play and the Way Forward* (New York: NYU Stern Center for Business and Human Rights, 2025), online (pdf): NYU Stern Center for Business and Human Rights <https://bhr.stern.nyu.edu/wp-content/uploads/2025/04/NYU-CBHR-Online-Regulations_Updated-Apr-23.pdf>.

Standing Senate Committee on Foreign Affairs and International Trade, *Strengthening Canada's Autonomous Sanctions Architecture: Five-Year Legislative Review of the Sergei Magnitsky Law and the Special Economic Measures Act* (Ottawa: Senate of Canada, 2023).

UN General Assembly, *Basic Principles and Guidelines on the Right to a Remedy and Reparation for Victims of Gross Violations of International Human Rights Law and Serious Violations of International Humanitarian Law*, GA Res 60/147, UNGAOR, 60th Sess, Supp No 49, UN Doc A/RES/60/147 (16 December 2005), online: OHCHR <https://www.ohchr.org/en/instruments-mechanisms/instruments/basic-principles-and-guidelines-right-remedy-and-reparation>.

UN Human Rights Committee, *General Comment No 34: Article 19: Freedoms of Opinion and Expression*, UN Doc CCPR/C/GC/34 (12 September 2011).

United States Department of Commerce, Bureau of Industry and Security, "Commerce Adds 8 Entities to the Entity List for Enabling Human Rights Abuses" (10 December 2024), online: BIS <https://www.bis.gov/press-release/commerce-adds-8-entities-entity-list-enabling-human-rights-abuses>.

News and Online Materials

Aung Naing & Caroline Henshaw, "European Govts Back Company That Uses Chinese Tech to Monitor Myanmar Internet Users" *Myanmar Now* (23 May 2025), online: *Myanmar Now* <https://myanmar-now.org/en/news/european-govts-back-company-that-uses-chinese-tech-to-monitor-myanmar-internet-users/>.

Boutilier, Alex, "'A foreign policy based on short memory': Carney continues push to diversify from the U.S." *Global News* (2026), online: *Global News* <https://globalnews.ca/news/11718383/foreign-policy-based-on-short-memory/>.

Business & Human Rights Resource Centre, "Myanmar: ISP Company Denied Allegations Linking to the Use of Chinese Tech for Online Surveillance; incl Investors' Comments" (23 May 2025), online: Business & Human Rights Resource Centre <https://www.business-humanrights.org/en/latest-news/myanmar-isp-company-denied-allegations-linking-to-the-use-of-chinese-tech-for-online-surveillance-incl-investors-comments/>.

Enlace Hacktivista, "Geedge" (accessed 18 May 2026), online: Enlace Hacktivista <https://files.enlacehacktivista.org/geedge/>.

Geedge Networks, "Greater than the Edge", online: Geedge Networks <https://www.geedgenetworks.com/>.

Geedge Networks, "Products", online: Geedge Networks <https://www.geedgenetworks.com/products/>.

Geedge Networks, "TIANGOU Secure Gateway (TSG)", online: Geedge Networks <https://www.geedgenetworks.com/tiangou-secure-gateway-english/>.

Henshaw, Caroline & Aung Naing, "Chinese Technology Capable of Mass Surveillance 'Installed' by Myanmar Internet Company Funded by UK" *Finance Uncovered* (21 May 2025), online: *Finance Uncovered* <https://www.financeuncovered.org/stories/british-norwegian-and-danish-governments-back-internet-provider-in-military-run-myanmar-which-hosts-notorious-chinese-surveillance-system>.

Herbert Smith Freehills Kramer, *Trust at Risk: Who's Accountable for the Online Safety Gap?* (2025), online: Herbert Smith Freehills Kramer <https://www.hsfkramer.com/insights/reports/2025/code-law/trust-at-risk-whos-accountable-for-the-online-safety-gap>.

Nagy, Stephen & Saroj Kumar Rath, "Canada's New Indo-Pacific Calculus: Beyond the Old Atlantic Order" (6 March 2026), online: Macdonald-Laurier Institute <https://macdonaldlaurier.ca/canadas-new-indo-pacific-calculus-beyond-the-old-atlantic-order-stephen-nagy-and-saroj-kumar-rath-for-inside-policy/>.

Net4People, "Leak of Geedge Networks Internal Documents (100,000+ from Jira, Confluence, GitLab)" GitHub Issue No 519 (9 September 2025), online: GitHub <https://github.com/net4people/bbs/issues/519>.

Open Observatory of Network Interference, "China is Blocking OONI" (28 July 2023), online: OONI <https://ooni.org/post/2023-china-blocks-ooni/>.

Peymann, Gesine, "Report: China's Geedge Networks Supplies Censorship Systems to Countries" *Heise Online* (10 September 2025), online: *Heise Online* <https://www.heise.de/en/news/Report-China-s-Geedge-Networks-supplies-censorship-systems-to-countries-10639548.html>.

Prime Minister of Canada, "Principled and Pragmatic: Canada's Path" (20 January 2026), online: Prime Minister of Canada <https://www.pm.gc.ca/en/news/speeches/2026/01/20/principled-and-pragmatic-canadas-path-prime-minister-carney-addresses>.

Proudfoot, Shannon, "It's clear Carney is now dealing with the world 'as it is'" *The Globe and Mail* (17 January 2026), online: *The Globe and Mail* <https://www.theglobeandmail.com/politics/opinion/article-its-clear-carney-is-now-dealing-with-the-world-as-it-is/>.

Putz, Catherine, "Did Kazakhstan Import a Commercialized Version of China's Great Firewall?" *The Diplomat* (15 September 2025), online: *The Diplomat* <https://thediplomat.com/2025/09/did-kazakhstan-import-a-commercialized-version-of-chinas-great-firewall/>.

Wang, Yaqiu, "In China, the 'Great Firewall' Is Changing a Generation" *Politico Magazine* (1 September 2020), online: Politico <https://www.politico.com/news/magazine/2020/09/01/china-great-firewall-generation-405385>.

Yang, Zeyi, "Massive Leak Reveals How a Chinese Firm Helps Censorship Worldwide" *Wired* (8 September 2025), online: *Wired* <https://www.wired.com/story/geedge-networks-mass-censorship-leak/>.