September 5, 2025

Securing the Infrastructure, Straining the Constitution? Bill C-8's Cybersecurity Overhaul

By: Dav More and Tulika Bali

Matter Commented On: Bill C-8, *An Act respecting cyber security* (1st Sess, 45th Parl, 2025)

Cyberattacks targeting vital infrastructure have intensified globally. Recent high-profile incidents in the United States and Europe prompted national governments to tighten regulation (see Industrial Cyber, The National Law Review, CER, and AP News). The EU's NIS2 Directive mandates stricter cybersecurity standards across member states by 2024. In Canada, the federal government introduced Bill C-26 in June 2022, aiming to overhaul cybersecurity regulation, but that bill died when Parliament was prorogued in early 2025 (Miller Thomson at para 2-3).

Bill C-8, introduced in Parliament in June 2025, is a reboot of the former Bill C-26 (Dentons Data at paras 1–3). Indeed, the new Bill is nearly identical to its predecessor and was read on June 18, 2025 (see Bill C-8). Bill C-8 combines sweeping government powers with major obligations for the private sector in designated critical sectors (Summary, Bill C-8). While Bill C-8 removes one of the most criticized features of its predecessor (secret evidence in judicial review), it leaves intact a broader architecture of secrecy and unchecked ministerial power that continues to raise serious constitutional red flags (Dentons Data, at para 10-15).

In what follows, we first unpack Bill C-8's two-pronged legislative framework (Telecommunications Act amendments and the new Critical Cyber Systems Protection Act). We then turn to the Bill's controversial features, secrecy, judicial review, and surveillance risks, before analyzing the sharing of information and law enforcement implications. Next, we compare Canada's approach to international norms such as the EU's NIS2 Directive, noting points of alignment and divergence. We also examine the Bill's limits of scope, including gaps in coverage of provincial/municipal systems and elections. Finally, we conclude with a critical assessment of Bill C-8's constitutional and governance implications.

Two-Pronged Framework

Bill C-8 is based around two legislative pillars. First, the Bill amends the *Telecommunications Act, SC 1993, c 38* to empower the Minister of Industry and the Governor in Council to issue binding directives to telecom providers to "do anything or refrain from doing anything" to protect the Canadian telecom system (Bill C-8, Summary; Part 1, cl 2, s 15.1(a)–(b)). These orders may include vendor bans, forced contract terminations, or restrictions on foreign technology use (Bill C-8). Providers would receive no compensation if directed to cease or avoid such dealings (Dentons Data, at para 5). Enforcement mechanisms include administrative penalties (AMPs) of

up to $15 million per day for corporations and criminal liability for directors and officers (Dentons Data, at para 5).

Second, the Bill introduces the *Critical Cyber Systems Protection Act* (CCSPA), establishing a regulatory regime for federally regulated industries deemed critical to national security. These include telecom, nuclear energy, banking, transportation, and interprovincial power and pipeline systems (Dentons Data, at para 7). Companies designated under the Act must create cybersecurity programs within 90 days, including supply-chain risk controls and incident reporting duties (Bill C-8, Part 2, cl 9(1)(a)–(e)). Significant changes, such as acquisitions or system redesigns, must be reported, and operators are required to keep in Canada detailed records of cybersecurity programs, incident responses, supply-chain risks, and compliance measures (Bill C-8, Part 2, cls 13(3), 14(1)– (2)). Operators must also comply with binding cybersecurity orders issued by government officials (Bill C-8, Part 2, cls 20–25).

The Bill's Controversies: Secret Directives, Judicial Review, and Surveillance Risk

A central controversy in C-26 was the use of secret evidence to compel confidential "cyber security directions" issued to private companies, which would have been barred from disclosing their existence or content (CIGI at para 4). In particular, that Bill allowed the government to defend cyber orders in court without disclosing the evidence to the affected company, a move widely condemned by academics and civil liberties groups (Citizen Lab at 23-24). Bill C-8 removes this provision. Now under Bill C-8, where a company challenges a directive in court, the government must disclose the evidence, and significantly no confidential or ex parte proceedings are allowed (Dentons Data, at para 11).

However, secrecy concerns persist under Bill C-8. The Bill bars public disclosure of cyber directives, including their very existence, except to the extent necessary for compliance (Bill C-8, Part 2, cl 25(2)). Unlike other national security measures, these orders are neither subject to automatic review nor tied to a formal oversight process. The only safeguard is a requirement to notify the National Security and Intelligence Committee of Parliamentarians (NSICOP) and the National Security and Intelligence Review Agency (NSIRA) when an order issued under sections 15.1 or 15.2 stipulates that its existence must remain confidential (Bill C-8, Part 1, cl 15(22)).

This structure amounts to a blueprint for shadow governance. Without requirements for judicial review, public reporting, or even basic sunset clauses, ministerial cybersecurity orders under Bill C-8 could persist indefinitely, immune from democratic checks, legal challenge, and invisible to the public they ultimately affect. Once issued, these directives are not subject to automatic expiry, periodic review, or external oversight. In effect, a single cabinet directive could silently shape or constrain private infrastructure operations for years, all while bypassing Parliament, the courts, and the public. In the absence of built-in expiry mechanisms, temporary emergency powers risk becoming permanent instruments of opaque state control.

Bill C-8's powers could also undermine constitutional privacy protections. In *R v Spencer*, 2014 SCC 43 (CanLII), the Supreme Court held that subscriber information tied to internet activity, such as IP addresses, cannot be disclosed to police without judicial authorization (at paras 49–52). While Bill C-8 does not explicitly authorize warrantless data access, its broad, secret cybersecurity directives, which allow government officials to compel operators to "do anything or refrain from

doing anything" without oversight, have drawn strong criticism. Civil liberties advocates warn these compliance mandates could effectively serve as a back-door to surveillance, sidestepping traditional warrant processes as contemplated in *Spencer*. One pivotal warning by Citizen Lab states that Bill C-26, on which C-8 is modeled "threaten to establish a class of secret law and regulations," with "excessive secrecy" built into the scheme and "significant potential" for government overreach, highlighting the urgent need for accountability mechanisms (Citizen Lab, at 2).

Use of Shared Information and Law Enforcement Implications

Bill C-8 empowers designated operators and telecom carriers to provide cyber-related information, including incident reports, technical vulnerabilities, or potentially customer data, to the Minister of Industry and relevant regulators (Dentons Data, at para 10). This includes the sharing of information not only with federal regulators and the Communications Security Establishment (CSE), but also with provincial governments, foreign states, and international organizations, for the purpose of securing the Canadian telecommunications system (Bill C-8, Part 1, s 15.7(1)). The *CCSPA* does not explicitly restrict this data sharing to cybersecurity purposes, nor does it limit how long information can be retained or mandate oversight by the Privacy Commissioner (Bill C-8, Part 2, s 35).

While Bill C-8 does not explicitly grant law enforcement direct access, information disclosed under its cybersecurity compliance regime could still be forwarded to police or national security agencies. This raises the possibility of using compliance obligations as a back door for investigative surveillance, without warrant, reasonable grounds, or even public transparency. Civil liberties advocates have cautioned that the Bill should be amended to include strict use limitations and notification requirements when such information is transferred (CIGI, at para 8).

Critics have also warned that the government could issue directives compelling companies to weaken or bypass encryption tools. The *CCSPA* does not prohibit such orders (McMillan, at para 3). Surveillance backdoors are not a hypothetical risk, rather, they are a threat that has been established repeatedly as cyber spaces continue to expand. By introducing the possibility of intentional vulnerabilities, the Bill may hand foreign actors the very exploit paths it claims to defend against and ultimately means that security systems are being built on selective weakness which could amount to an overall erosion of Canada's vital security infrastructure (OpenMedia, at para 11). Encryption is only secure if it's universal; any deliberate vulnerability is a threat vector and may perpetuate censorship.

Alignment with International Norms or a Divergence?

At first glance, Bill C-8 appears to mirror global efforts to harden critical infrastructure against cyber threats. The EU's NIS2 Directive, adopted in 2022, similarly mandates incident reporting, supply chain risk management, and minimum cybersecurity standards across key sectors. However, the resemblance ends at surface level.

Unlike NIS2, which places significant emphasis on transparency, institutional accountability, and harmonized enforcement through national authorities, Bill C-8 consolidates authority within the federal Cabinet and delegates sweeping powers to the Minister without creating any independent

regulatory body. NIS2 also requires member states to establish a single point of contact, a national CSIRT (Computer Security Incident Response Team), and national strategies subject to periodic public reporting. Bill C-8 does none of these.

While Bill C-8 reflects the global shift toward stronger cyber regulation, it does so by bypassing the institutional safeguards that are fast becoming the international norm. As Wright and Olszynski observed in their commentary on Bill C-5, "[t]he linear structure of the proposed process is relatively simple, premised primarily on providing project proponents with an early green light from the federal government and limiting any chance of a late-stage red light" (see post here). A similar logic underlies Bill C-8: provide rapid governmental control, not deliberative or accountable governance.

Rather than standing as a Canadian counterpart to NIS2, Bill C-8 represents a regulatory divergence, prioritizing centralized, opaque executive discretion over transparent, public-facing accountability mechanisms. That divergence is not merely procedural, it reflects a broader question: what kind of cybersecurity governance model does Canada want to lead with, one based on secrecy, or one rooted in rule of law?

Limitations of Scope

In addition to these international limitations, Bill C-8 only applies to federally regulated entities, meaning that provincial and municipal systems, such as elections, hospitals, schools, local transit, and likely small contractors fall outside its jurisdiction (Bill C-8, Part 2, s 7(1)). Recent ransomware attacks on these key provincial and municipal systems would not have been prevented under the current framework (See CBC; CBC; Bitdefender). The Bill also fails to address ransomware payments, leaving it unclear whether designated entities are permitted, or expected, to pay. Critically, election infrastructure is not explicitly protected: federal political parties, election agencies, and voting technology vendors do not fall within the list of sectors covered by the *Critical Cyber Systems Protection Act,* despite long-standing concerns about election interference and digital threats to democracy (Public Safety Canada).

Conclusion

Bill C-8 marks a significant development in Canadian cybersecurity law. It aims to fill a longstanding regulatory void by imposing clear compliance duties and enforcement mechanisms for critical infrastructure. However, the Bill's ambitious scope comes with constitutional constraints. While the removal of secret evidence provisions found in the defunct Bill C-26 was a step in the right direction, concerns remain about the opacity of ministerial orders, the potential misuse of data, and the lack of judicial or independent oversight.

Bill C-8 does not just regulate cybersecurity, it concentrates state power, sidesteps accountability, and contributes to legislative overreach with minimal limits. Internationally, frameworks like the EU's NIS2 Directive embed transparency, oversight, and institutional checks into cybersecurity governance. Bill C-8 diverges from this direction by choosing centralized control over public accountability.

If passed in its current form, Bill C-8 risks undermining the very democratic values it claims to protect. Parliament should amend the Bill to include judicial safeguards, use restrictions, and

mandatory transparency mechanisms to ensure that national security does not come at the expense of constitutional governance.

This post may be cited as: Dav More & Tulika Bali, "Securing the Infrastructure, Straining the Constitution? Bill C-8's Cybersecurity Overhaul" (5 September 2025), online: ABlawg, http://ablawg.ca/wp-content/uploads/2025/09/ Blog_DM&TB_BillC-8.pdf