Appearance before the Standing House Committee on Public Safety and National Security during its study of Bill C-8

An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts

Opening Remarks by Sharon Polsky MAPP

President

Privacy & Access Council of Canada

30 October 2025

Privacy and Access Council of Canada
Conseil du Canada de l'Accès et la vie Privée
Suite 330, Unit 440, 10816 Macleod Trail SE
Calgary AB Canada T2J 5N8
Telephone: 877.746.7222
Email: info@pacc-ccap.ca
Website: www.pacc-ccap.ca

Thank you for inviting me to address the Committee today. I am Sharon Polsky, President of the Privacy and Access Council of Canada, an independent, non-profit, non-partisan organization that is not funded by government or industry.

Since launching 30-plus years ago, the Internet has infiltrated our lives. I've spent those years consulting to governments, and to small, medium and Fortune 100 businesses, seeing how they apply law and policy, and identifying risks invariably caused by human nature and, increasingly, the Internet itself.

Scope.

The preamble says that this bill is to protect telco providers and critical systems, and provides the Minister with sweeping powers to order them to "do anything, or refrain from doing anything" to protect the Canadian telco system. (s15.2(2))

But it lacks safeguards to prevent abuse or ideological attack.

This new law to "add the promotion of the security of the Canadian telecommunications system" as a policy objective tells companies to plug the holes that were built into their systems …something they should have done long ago to comply with privacy and other laws.

Rephrasing the request won't change much — even with AMPs.

More on that later.

Who is Caught in the Critical Cyber Systems Net

Under Section 7 of Part 2, a Class of Operators can be declared, and any person or organization declared a member of that Class.

The bill applies to enterprises within the legislative authority of Parliament …and Section 9.1 ensnares the rest — the businesses and people whose products or services are in support of federally regulated enterprises.

Accountability.

The Auditor General noted that "Gaps in cyber security defences undermine the ability to protect critical information and manage cyber security risks." Those gaps will remain even if this bill becomes law.

The standards, laws, and frameworks already in place — and privacy, security, and risk assessments now done — cannot prevent outages like we saw last week, and again yesterday, each time grinding services around the globe to a halt thanks to a single technical problem. That's all it took — because accountability requirements are inadequate.

And what accountability can there be when even the existence of orders can be ordered to be kept secret, and when the Governor in Council can direct that orders NOT be published in the Gazette? (s.15.1(2))

Doing that leaves everyone in the dark — and speaks to an undemocratic lack of transparency and a shield against accountability.

Secrecy.

Section 15.21 requires the Minister to reveal how many times in the previous year secret orders were made, but statistics are cold comfort — especially given the broad information collection and sharing powers in this bill.

That needs to be changed.

Identifying Risk.

Part 2 of Bill C-8 allows ANY service or system to be designated a vital service or system; and requires that designated operators "mitigate supply-chain and third-party risks." It doesn't — but should — specify the risks to be mitigated.

Section 20(6) of the CCSP (Critical Cyber Systems Protection) prohibits a designated operator or class of operators from intercepting communications, but third parties that support critical services aren't included. That could easily be operationalized as encryption-busting back doors.

This and other governments have worked mightily to circumvent encryption.

C-8 needs clear language to ensure its broad powers cannot be used in any way, by anyone, to undermine or circumvent encryption — a ban even more urgent considering that Bill C-2's vague language would grant sweeping ministerial powers to order changes in Canada's telecommunication networks. (Part 15 of Bill C-2)

AMPs.

The bill says AMPs are only intended to promote compliance, and not intended to be punitive.

They *will* benefit the largest providers, which can recoup the cost from their broad customer base and further solidify their dominant position, and still evade accountability. Others will be bankrupted.

Implementation must be monitored, measured, and mandatory — with Sarbanes-Oxley-like penalties imposed, including personal (not corporate) liability — to make accountability inescapable.

But how *will* a Canadian regulator be able to monitor compliance, when Rogers runs its wireless network from India?

Measuring Manipulation.

Orders under 15.1 may be made about "any threat" including that of interference or manipulation.

Elections have been swayed by social media content. AI for news often misrepresents the story. Will that be deemed manipulative, or a threat, and platforms subject to being silenced?

And by what objective calculation ***does*** one measure gravity of 'manipulation'?

The bill must be clear.

Disproportionate Impact of Digital Purgatory.

Finally, ordering that someone be denied internet access because the Minister considers something they've done or said to be a threat, or manipulative, will mean cutting them off from phone service, which is now Internet-based.

Everyone in your house will be blocked from talking to friends; calling adaptive transport; or surfing the Internet. Your kids won't be able to get their homework or apply to university. Calling 911 will be impossible.

That is unjust and disproportionate …and what Bill C-8 allows.

Bill C-8 must be changed, or we will re-live what my grandparents fled a hundred years ago, after the Russian Revolution: People placed in isolation for their views conflated as the stuff of good government.