Appearance before the Standing Senate Committee on National Security, Defence and Veterans Affairs during its review of Bill C-26

Opening Remarks by Sharon Polsky MAPP
President
Privacy & Access Council of Canada

18 November 2024

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 so much for the invitation 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 its launch over 30 years ago, the Internet has become an integral part of our everyday lives. It enables research, commerce, communication, and democratic freedoms.

The Internet also facilitates harmful conduct — such as harassment, ransom demands, and hostile activities by unfriendly states — all sorts of behaviors that existed long before the Internet enabled such aberrant activities to be carried out with great ease and broad reach.

Bill C-26 is one of several bills advanced by Canada's government to protect Canadians from such harms. But it also illustrates how proposed cures can be worse than the disease itself.

In the name of strengthening cybersecurity, the bill grants the government sweeping powers to order telecommunication providers — the very same telcos that now are the repositories of our most intimate, sensitive and health-related data — to, and I quote, *"do a specified thing or refrain from doing a specified thing."* Similar powers, of course, apply to operators designated under Part 2 of the bill.

Bill C-26's omission of vital democratic checks and balances to constrain such alarmingly broad powers rightfully sparked an avalanche of criticism— because this is not a zero-sum game.

I think we can all agree on the need for cybersecurity, but not when it's at the cost of our civil liberties.

I do want to acknowledge the work of members of the Other Place in curbing some of this bill's most egregious excesses. But even with that, Bill C-26 still contains significant flaws that risk compromising civil liberties *and* cybersecurity.

Let me give you a few practical examples:

- First, Bill C-26 gives the government the power to order telecommunication providers to adopt standards that *weaken* encryption and, with it, privacy. This endangers the freedom of everyone in Canada, including political representatives, to safely engage in national and international commerce and communications, and enjoy private communications.

- Second, Bill C-26 allows the government to indefinitely keep secret any order made to telcos and other Designated Operators.

  While secrecy might be warranted in some circumstances, it should not be the default or allowed to remain indefinitely.

  Such excessive secrecy shields accountability, undermines trust, and precludes our members and, indeed, all Canadians, from being able to understand how government uses its powers, and hold it to account.

- Third, Bill C-26 allows the Minister to require telcos and Designated Operators to disclose personal and de-identified information. Once collected, the information can be shared across our Government 2.0, and with foreign entities — and easily re-identified in many cases.

  PACC members work hard every day to safeguard privacy, and it's alarming to know that their work risks being undercut by the secret stroke of a Minister's pen.

- Fourth, Bill C-26 dramatically expands the CSE's ability to obtain personal information from telcos, financial institutions, and many other companies that Canadians now trust. But it lacks the safeguards needed to constrain how the CSE can use that information.

  Indeed, the testimony of CSE officials makes it clear that they fully intend to use the information they gather for both offensive *and* defensive purposes, and share it with our Five Eyes partners.

In short, this legislation remains fundamentally flawed from a privacy perspective. That's why we, along with other civil society organizations and experts across Canada, have submitted recommendations to address these flaws.

Let me be clear and echo my colleagues on the panel: we want to fix this legislation, not kill it.

We recognize that cybersecurity is a team sport, and that public trust is critical for this to be a win. But a bill that fails the democratic legitimacy test will fail to strengthen cybersecurity *and* trust.

I know there's been discussion about not letting the "perfect be the enemy of the good" but, in its current form, with respect, Bill C-26 is far from "good". It needs fixing …and it is fixable.

If adopted, our proposed amendments — which are balanced, practical and achievable— will result in a cybersecurity framework that all Canadians can trust.

Given the Senate's constitutional role, you have a critical part to play in ensuring that Bill C-26 delivers strong cybersecurity.

Senators, you have the ability to amend Bill C-26 to broaden oversight of its implementation and its operation to ensure it protects privacy, delivers genuine accountability, and upholds the rights of everyone in Canada.

I look forward to your questions.