Canadian Civil Liberties Association | Opening Remarks
Senate Standing Committee on National Security, Defence & Veteran Affairs

November 16, 2026

Madam Chair, honourable members of the committee, good afternoon.

My name is Tamir Israel and I am Director of the Privacy, Surveillance and Technology Program at the Canadian Civil Liberties Association (CCLA).

We thank you for inviting us to speak before you today on Bill C-22, the *Lawful Access Act*.

I will focus my comments today on part 2 of the bill, but welcome any questions on part 1 as well.

Part 2 of the bill effectively grants the government a blank check to impose its evolving surveillance objectives onto electronic service providers in secret, at the cost of everyone's privacy and cybersecurity.

With the proliferation of AI-fueled cyber attacks that we are currently experiencing, part 2 of Bill C-22 is taking us several steps in the wrong direction.

The framework it puts in place combines unparalleled breadth with minimal safeguards and an oversight framework that limits scrutiny by independent experts, the courts and the general public because it was developed to oversee foreign espionage. It will undermine the privacy and cybersecurity of every person in Canada and will fall most heavily on the shoulders of people who are already over-surveiled, including Indigenous People, migrants, and political protesters.

Bill C-22 does not align us with our international partners because it expands on the breadth of comparable regimes among our investigative partners while leaving out the many of the critical safeguards.

Indeed, in its assessment of Bill C-22, the UN Office of the High Commissioner for Human Rights has found the proposal to be inconsistent with international human rights standards and it similarly fails to meet baseline restrictions imposed by the European legal system.

Over the years, governments have frequently overstated the necessity of the types of mechanisms contemplated by Bill C-22 while understating their intrusiveness.

For example, the US no longer has any data retention obligations in place after its foreign espionage regime for phone call log retention was publicly revealed by whistleblower Edward Snowden. This led to a 5 year audit of the program that concluded it had only

yielded one single significant investigative lead over the entire audit period, and the program was subsequently discontinued.

Over the years, we have also seen a long list of proposals from government entities to impose surveillance capabilities at the cost of cybersecurity, with encryption being a recurring target. These proposals are based on the demonstrably false premise that police can be provided exceptional access to data or infrastructure without creating security vulnerabilities that will be exploited by others.

The recent salt typhoon compromise in the US is a stark reminder of this. Once they had gained access to US telecom networks, the perpetrators of that attack commandeered tools imposed onto telecom networks by US laws, greatly increasing the harm of the breach.

Once in place, powers such as those contemplated here are hardly ever limited, they are only expanded. We should therefore expect to have this regime in place for decades to come and it is essential that we get the right framework in place.

We encourage you to withdraw SAAIA so that it can be more fundamentally reconsidered or at minimum to amend it so that it:

- limits the application of the regime to telecom providers;
- includes unambiguous safeguards that prohibit any attempt to bypass, circumvent, downgrade or otherwise weaken end-to-end encryption;
- requires judicial authorization on the basis of necessity and proportionality and subject to clear statutory appeal mechanisms;
- ensure that obligations are imposed in a manner that is public by default unless strictly necessary to preserve the integrity of an investigative technique; and
- remove the data retention regime or at minimum limit it so that it only applies to telecom providers and to data already under their control.

We will be filing a brief that elaborates on these and other recommendations along with our colleagues from the Citizen Lab.

Thank you for your time and I welcome your question.