Canadian Civil Liberties Association | Opening Remarks
House Standing Committee on Public Safety and National Security (SECU)

May 26, 2026

Mr 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*.

Part 1 of Bill C-22 represents a meaningful improvement over its predecessor legislation. However, elements of part 1 continue to suffer from overbreadth. These include use of low standards for judicially authorized access to sensitive subscriber data and a framework that invites unconstitutional collection of publicly available data.

Elements of Part 1 would also allow Canada to adopt at least one if not two international information-sharing agreements despite a growing tendency to use these tools for cross-border repression.

CCLA is preparing a joint brief with Kate Robertson and Cynthia Khoo from the Citizen Lab that will elaborate on these and other problematic elements of Bill C-22, and I invite any questions the Committee may have regarding Part 1.

I will focus the remainder of my remarks on Part 2 of the Bill, which would enact the Supporting Authorized Access to Information Act, or SAAIA.

At various points in time, governments in Canada and around the world have sought to expand their surveillance capabilities at the cost of cybersecurity, with encryption a recurring target. Too frequently, these expansions have been justified by the expectation that surveillance capabilities will only be used by lawfully authorized government agencies. Yet time and again this expectation has been proven false.

The Salt Typhoon attack, which successfully targeted wiretapping capabilities imposed under a comparable, if narrower, US law, is the latest and perhaps most potent reminder of this hard lesson.

With this troubling historical track record in mind, SAAIA is fundamentally flawed in three inter-related ways.

First, SAAIA is exceedingly broad.

It applies to any provider of any service that has a digital component. Under the Australian version of this law, everything from a fast food chain that provides its customers WiFi, to an electronics store that helps maintain customer's phones and computers, to any retailer that has a mobile phone application or online website has been listed as an anticipated target.

SAAIA is also broad in terms of what obligations the government can impose. These range from requiring the ability to covertly reset customer passwords, to requiring an automated tool that generates realistic undercover profiles on social media platforms, to requiring the ability to block a target's use of encrypted private messaging in order to force the use of insecure alternatives.

SAAIA's metadata retention mechanism is equally broad—services can be required to retain a detailed record of every single person's movements, inter-personal interactions, what applications they use, and more.

From a comparative perspective, it is notable that half of Canada's Five Eyes partners have limited their surveillance capability regimes to imposing wiretapping obligations onto Telecommunications carriers.

Second, SAAIA's limitations and safeguards fail to constrain the multiple ways that privacy, encryption and other data protections might be compromised in light of SAAIA's broad scope.

SAAIA's systemic vulnerability limitation, for example, would not apply to a set of "client-side scanning" proposals, which would require private messaging or other services to install an algorithmic monitoring tool on everyone's phone. Because these tools bypass encryption rather than compromising it directly, they fall outside the systemic vulnerability limitation as drafted.

Third, courts remain the primary vehicle for authorizing CSIS and Police surveillance activities. But SAAIA does not rely on judicial authorization despite authorizing powers that frequently rival their Criminal Code counterparts in breadth.

If police want to force a company to keep a specific customer's metadata for 90 days, for example, they need a court order. But to force the same company to keep the same metadata on every single customer for up to one year, the government need only impose an obligation through SAAIA.

Judicial review is available, and even required, in some instances under SAAIA, but judicial review is highly deferential to government decision-making and is no substitute for

independent authorization, de novo review or full appeal rights. This is particularly the case where obligations can be imposed in secret.

In sum, SAAIA poses a significant threat to privacy and cybersecurity as currently drafted and should not become law.

Australia's technical capability regime was amended 173 times during a detailed committee study and, despite these changes, was still held to be "likely incompatible with … the rights to privacy and freedom of expression" in a mandatory human rights assessment of the legislation.

It is unclear how SAAIA's many overlapping flaws can be remedied through the highly attenuated legislative study it is receiving.

We therefore urge that you recommend that the government advance Bill C-22 without Part 2. This legislation will be in place for years to come, and it is critically important that the government get it right. The stakes are simply too high.