OpenMedia is a community-based organization that works to keep the Internet open, affordable, and surveillance free.

Matt Hatfield, Executive Director, OpenMedia

Standing Senate Committee on National Security, Defence and Veterans Affairs (SECD)

Re: Bill C-8, An Act respecting cyber security, and finishing the work the other house began

May 25, 2026

Opening Remarks (Check against delivery):

Good evening. I'm Matt Hatfield, Executive Director of OpenMedia, a grassroots community of 230,000 people in Canada who work together for an open, accessible and surveillance-free Internet. I'm grateful to be with you tonight on the unceded territory of the Algonquin Anishinaabe Nation.

I want to begin with something I don't often get to say at a committee: the other House's amendment work got a lot of this Bill right. When civil society and the Privacy Commissioner came to the House with severe concerns with the last version of Bill C-8, many were heard, and real improvements are made in the text in front of you. Every order must now be reasonable in relation to the gravity of the threat. The Minister must weigh the impact on Canadians' privacy before acting. The bill states the government cannot order a provider to decode an encrypted private communication, and cannot use these powers to intercept private communications. An individual cannot be cut off from service except against a genuine technical threat. Personal information is treated as confidential by default and must be disposed of when it is no longer needed. These are real protections, and the members who fought for them deserve credit.

But the job of fixing Bill C-8 is not entirely done, and I am hoping you will finish the job.

Bill C-8 carefully limits why information may be collected, and why it may be shared between departments: in each case, the purpose must relate to making or enforcing one of these cybersecurity orders. That is good drafting. But it stops one step short. Once information has lawfully passed to an agency like the Communications Security Establishment, nothing in this bill limits what that agency may then use it for. The gate into the building is guarded; once inside, the data can be put to other purposes. During study of the predecessor bill, a CSE official testified to the agency's interest in using information gathered under these powers beyond its cybersecurity mandate. So this is not a theoretical gap — it is one the government has told Parliament it intends to walk through.

The fix is small and surgical: say in the statute that information obtained under this Act is used only for cybersecurity and information assurance — not repurposed for foreign intelligence or unrelated operations. This is the recommendation Citizen Lab put to the House. It does not touch the government's cybersecurity powers at all. It simply holds them to their stated purpose.

Second, the standard throughout this bill is that an action be "reasonable in relation to the gravity of the threat." The Privacy Commissioner asked this Parliament for something more

exacting and more familiar in privacy law: that any collection, use, or disclosure of personal information be both necessary to achieve the purpose, and proportionate to the benefit. That is the test our privacy framework uses everywhere else, yet this bill did not adopt it. You can.

Third, an order under this bill can carry a provision forbidding anyone from revealing that it exists — and that secrecy has no end. The bill tells the Minister to weigh transparency before imposing silence, which is welcome, but once imposed there is no sunset and no requirement to return to a court to justify keeping it hidden. Some secrecy may be necessary in this work, particularly in emergency circumstances. But permanent, unreviewed secrecy is a different thing, and Parliament should not grant it without limit. I urge you to ensure that the public is eventually informed of the existence of secret orders to service providers, if not their full text; and that representatives in NSIRA and NSICOP can ultimately review and comment on the text of these orders.

Underlying all of this is a check the other House wanted. Its committee adopted independent authorization of non-emergency orders by a judge — a safeguard at the front of the process. It was not voted down; it was removed before third reading on a procedural ruling about the bill's scope. It belongs back in Bill C-8.

I know this committee weighs carefully when to ask democratically elected officials to think again. This is the right time to do so because you would be acting on proposals that the other house considered, even passed; that were directly proposed by Canada's privacy commissioner; or both!

Four narrow amendments would complete the work begun on Bill C-8:

1. **Limit use to cybersecurity.** State in the statute that information obtained under this Act is used only for cybersecurity and information assurance, and is not to be repurposed for foreign intelligence or unrelated operations. The bill limits why data is shared; it should also limit how it is used.

2. **Require necessity and proportionality.** Adopt the Privacy Commissioner's standard: any collection, use, or disclosure of personal information must be necessary to the Act's purpose and proportionate to the benefit — and where information is shared abroad, the governing agreement must guarantee minimum privacy safeguards.

3. **Put a clock on secrecy.** Non-disclosure provisions should be time-limited, with any extension requiring an order of the Federal Court — so that secrecy is justified and revisited, not permanent by default.

4. **Restore independent authorization.** Put back the judicial check the House committee adopted, so that a judge with technical expertise reviews these orders and the information demands behind them, whether or not a company ordered to comply contests the decision. This was a committee safeguard lost here on procedure; the Senate is the place it can be restored on the merits.

More than 10,000 Canadians have written to ask that this bill become law only once it protects our rights as well as our networks. The other house brought it much of the way to doing that. What remains to do is putting in place basic limits that citizens of a democracy expect: that data taken for one purpose is used for that purpose; that orders are proportional, not just ‘reasonable’; that our rights are defended by appointed judges, not a private corporation’s decision to fight; and that no secret order stays secret forever. Completing the job of adopting those safeguards into the law is a job that now, only the Senate can do. I hope you will. Thank you, and I look forward to your questions.
