Matt Hatfield, Executive Director, OpenMedia

House Committee on Public Safety and National Security
Re: The impact of Bill C-8, an act respecting Cybersecurity, for Canadians

Thursday, December 4th, 2025

Opening Remarks (Check against delivery):

Good morning. I'm Matt Hatfield, and I'm Executive Director of OpenMedia, a grassroots community of 230,000 people in Canada that work together for an open, accessible and surveillance-free Internet. I'm joining you from the unceded land of the Tsawout (Say-ut) on Salt Spring Island in BC.

Loopholes matter. A bad loophole you pass in this legislation does not just weaken this law: it will prove far more important than the law's intended purpose. Right now, Bill C-8 contains several serious loopholes that you must fix.

Bill C-8 is built on and very closely resembles Bill C-26, the cybersecurity legislation this committee's predecessor passed last year. Both bills give future industry ministers the power to permanently and secretly disconnect Canadian citizens from the Internet without notifying them, or explaining the decision; to issue orders to our telecom companies to do or not do anything the minister *says* is necessary to protect our telecom infrastructure; and to keep you, our elected representatives, entirely in the dark about what their orders to companies actually say. That is simply too much unchecked power. Canada does need cybersecurity legislation: but you should not pass this legislation as it is worded today.

In section 15.2(2), the minister is given the power to order telecomm providers do anything or not do anything they believe necessary to secure the Canadian telecommunications system. Constructively, C-8 now states the minister's use of these powers should be reasonable and within the Act's purpose. But who will decide if that standard is met? Not the public: we're only informed of the existence of these orders in a yearly report. And not you or your colleagues on NSICOP: the minister only has to tell you why *they* think what they're doing is reasonable, not show you that it is. That is not transparency and accountability; it is accountability theatre. The minister is required to think hard about whether their decisions are reasonable and proportionate, and to promise you in writing that they are; but there's no oversight to check. This is much like a law that requires me to give you a very good explanation for why I think my hands should be in the cookie jar, but doesn't let you check what I'm actually doing in there.

Our democratic allies don't write legislation like this. In the UK, the government cannot issue this kind of order without consulting Ofcom, the independent regulator. Different uses of order-making powers require the approval of an independent technical board, a reviewing judge, or both. In Bill C-8, the minister alone decides. In Australia, if a telecom company believes an

order would compromise the privacy or security of their network, they can demand a technical review by an independent judge *and* technical expert; in Canada, the minister alone decides. Not coincidentally, these baked-in expert reviews also protect the government from accidentally creating technical disasters by issuing orders with consequences they don't understand, that break rather than protect telecom infrastructure.

In sum, Canada's approach in Bill C-8 is not a system of democratic checks and balances; it is a blank cheque to future ministers to build a growing system of permanent secret orders, whose reasonableness and proportionality is entirely in their hands.

The necessary fixes to Bill C-8 remain those we recommended during the last stages of Bill C-26's review. First, the government's new powers must be constrained by actual independent review. The minister's opinion that they are necessary and proportionate is not good enough; a judge and technical expert should have full access to these orders either before they are issued; or in emergency circumstances, within 30 days, and have the ability to overturn orders that go too far.

Second, Bill C-8's legitimate purpose is systemic infrastructure protection, not being misused to surveil Canadians. This means the bill must explicitly prohibit orders that have the effect of creating a 'systemic weakness' or backdoor in encryption—language already used by our allies in Australia. If a door is opened for the Minister, it is opened for hackers too. Further, personal information must be clearly defined as confidential, and if any is incidentally collected in the process of carrying out C-8, it should be rapidly destroyed. In all circumstances, C-8 must forbid personal information collected under it from being shared with foreign intelligence agencies who are not subject to our laws.

Third, the government must not be allowed to keep how it is using these new powers permanently secret; not from you, and not from the public. Outside of immediate emergency situations, the standard of disclosure of what is happening under C-8 should be one level higher than C-8 currently requires. That means that the public should be informed not just of how many orders are being made, but the minister's description of what they are accomplishing and why they are necessary; and NSICOP should be provided with a full description of the orders, so MPs can judge if the minister's public report is telling Canadians the truth.

More than 10,000 Canadians have written to our government to demand this cybersecurity legislation pass only once it includes robust rights protections. That's your job to do. We urge you to listen to these voters and adopt the amendments that civil society has placed before you to get this legislation where it needs to be.

Thank you, and I look forward to your questions.