**Matt Hatfield, Campaigns Director, OpenMedia**

House Committee on Public Safety and National Security
Re: The impact of Bill C-26, an act respecting Cybersecurity, for Canadians

Monday, February 5, 2024

**Opening Remarks (Check against delivery):**

Good afternoon. I'm Matt Hatfield, and I'm the 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 join you from the unceded territory of the Sto:lo, Tsleil-Waututh, Squamish and Musqueam Nations.

I'd like to ask you a question: what does cybersecurity mean to you, as an individual, as a family member, and as a citizen?

For me, and for many people across Canada, our cybersecurity is inseparable from our privacy. So much of our everyday lives are conducted online — even more so since COVID. None of us feel secure with the thought of being spied on in our everyday lives — whether by hackers, hostile states, or even our own government.

For most Canadians, our cybersecurity is very much about that sense of personal security.

The draft of Bill C-26 you have in front of you threatens that security. It poses enormous risks to our personal privacy, without basic accountability and oversight to ensure the people given these powers don't abuse them against us. You must fix this.

Exhibit A is section 15.2 of the *Telecommunications Act* which grants the government the power to order telcos "to do anything or refrain from doing anything."

There are no limits here — no test for necessity, proportionality, and reasonableness, no requirement for consultation. The government could use these powers to order telcos to break the encryption we need to keep ourselves safe from hackers, fraudsters, and thieves.

They could even use these powers to disconnect ordinary people indefinitely from the Internet — perhaps because our 'smart' toaster oven, or an old phone we gave our kids, gets hijacked by a hostile botnet. Without a requirement that their orders be either proportional or time limited, that's a real risk.

It gets worse. The government would be allowed to keep even the existence of these orders, never mind their content, top secret, indefinitely. And even if these orders are challenged by

judicial review, the Minister could bring secret evidence before secret hearings, flying in the face of basic judicial transparency.

There's no excuse for this. Our close allies in Australia and the UK have shown how cybersecurity can be strengthened without compromising fundamental rights. Why do Canadians deserve lesser protections?

*And all this comes at a time when Parliament is working on strengthening our privacy laws through Bill C-27. You have to ask: does one hand of this government even know what the other hand is doing?*

We recognize that there are very real problems that Bill C-26 is trying to solve. When we read the government's stated objectives, we're on board!

Protecting the digital infrastructure that OpenMedia's community relies on? Sure! Removing risky equipment from hostile states? Of course. Forcing big banks, telcos and energy providers to better protect their customers? Absolutely!

But we can fulfil these objectives without sacrificing our rights, or balanced, effective governance. Let's talk about how.

First, the government's new powers must be constrained — robust necessity, proportionality, and reasonableness tests are an absolute must. As unbreakable encryption is the fundamental baseline that all of our personal privacy depends on, there must be an absolute prohibition on the government using these powers to break encryption.

Second, privacy rights must be entrenched. Personal information must be clearly defined as confidential, and forbidden from being shared with foreign states who are not subject to C-26's checks and balances.

Third, the government must not be allowed to conceal use of its new powers under a permanent veil of secrecy. Even expedited action must eventually receive due scrutiny from independent authority, and at an appropriate level of detail, the public at large.

Fourth, when the use of those powers is challenged in court, there must be no secret evidence — Special Advocates should be appointed to ensure all evidence is duly tested.

Fifth, any information the Canadian Security Establishment (CSE) obtains about Canadians under Bill C-26 should be used exclusively for the defensive, cybersecurity part of its mandate. And please remember that for consecutive years, the National Security and Intelligence Review Agency, NSIRA — the body explicitly established by Parliament to provide oversight of CSE — has complained about the CSE's failure to be held accountable. Knowing how difficult it has

proved for you to oversee their existing powers, please do not grant them broad new powers without tight, clear use and reporting mechanisms.

When cybersecurity works, it's a team sport. It requires buy-in from all of us — from citizens, businesses, and our government. We all need to be on Team Canada, and we all need to have trust in the regulatory framework that governs it.

There's zero chance of that happening with Bill C-26 in its current form. Adequate transparency, proportionality, and independent verification are the necessary baseline to earn and sustain the level of public trust we need for C-26 to work.

OpenMedia will be delivering a petition from nearly 10,000 Canadians to your committee this week asking you to implement those reasonable baseline protections. We urge you to listen to these voters and adopt the amendments package which civil society and experts have placed before you to get this legislation where it needs to be.

Thank you, and I look forward to your questions.