Matt Hatfield, Executive Director, OpenMedia

Senate Committee on National Security, Defence, and Veterans Affairs
Re: Bill C-22, an Act respecting Lawful Access

Monday, November 16, 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 joining you from the unceded land of the Tsleil-Waututh, Squamish and Musqueam Nations.

We believe Bill C-22 is the most dangerous digital policy legislation Canada has ever proposed. Yet it has had almost no serious study; a House study cut unusually short, submitted briefs left untranslated for weeks and never provided to MPs, and very few amendments. I understand you're under pressure to rush it through now, too. Please, don't give in. You must make significant improvements to C-22 before it can pass.

We are in truly unprecedented times. New autonomous AI agents are uniquely good at sniffing out cybersecurity vulnerabilities; the speed, frequency, and severity of cyberattacks are all going up, every single month. We're being told we're facing an "unprecedented rise in cybersecurity incidents", a "perfect storm for [cybersecurity] offense" that is "going to be pretty insane, at least for two to three years." Those are direct quotes from the UK's National Cyber Security Centre, cybersecurity company Mandiant and Alex Stamos, Facebook's former chief security officer – not privacy advocates or alarmists.

Responsible companies and governments are responding sensibly. They're racing to close old and new vulnerabilities; and tightening how much unnecessary data they retain, to limit the harm if their systems are breached. Bill C-22 proposes the exact opposite. In the face of many actors becoming vastly more effective at breaching digital systems, our government wants to create the broadest set of sensitive data targets Canada has ever seen; not for suspected criminals, but on any service our government designates, for all Canadians. Who you messaged with, when and for how long, what services you've used, the domains you visited, and your physical location every hour of every day; all metadata government can ask every company you do business with to retain about you by default.

Since Bill C-22 passed the House, our government has also been more honest about what they want itl to do: create a "minor opening" in "extenuating circumstances" to Canadians' private messages. That is not, and has never been, possible. Having a minor opening in private messaging is like your front door being a little unlocked, or being a tiny bit pregnant. The "minor opening" our government is ordering will be found and used by many bad actors, from

authoritarian governments, to hackers, to abusive partners. And new AI agents will be the main tool they use to get it done. CALEA, the far more limited backdoor system the US forced on its telecom systems, has already been used by bad actors to compromise them; and that was well before autonomous AI hackers became the norm.

Our government's best - maybe only - defence for of Bill C-22's enormous scope and intent, is that they won't actually use the extraordinary powers they're asking you to give them. But we'll never know currently if they do, because the government can issue secret, permanent orders, to any provider they choose. This should not be how democracy works.

Senators are appointed for experience and good judgment, not for being cybersecurity experts. But your good judgment is all we need. When our government is told about an incoming severe wildfire season, we don't order companies to install extra gasoline tanks around Canadian communities. Yet we're doing the digital equivalent in Bill C-22.

In the next few days, our written brief will set out necessary fixes to Bill C-22: striking mandatory metadata retention, ending permanent secret orders, and preventing any systemic breach to encrypted systems. In an appendix we will present the voices of nearly 13,000 Canadians who want the Bill changed. Please listen to them.

Thank you, and I look forward to your questions.