Matt Hatfield, Executive Director, OpenMedia

House Committee on Public Safety and National Security
Re: Bill C-22, an Act respecting Lawful Access – its impact on Canadians

Tuesday, June 2, 2026

Opening Remarks (Check against delivery):

Good afternoon. 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.

Do not let the Public Safety Minister convince you that limited amendments will fix Bill C-22. They will not; nothing short of striking the majority of Part 2 will protect Canadian privacy. The government's current approach is an enormous own-goal against our economy and our security, and you are the only people who can stop it. I won't repeat the facts you've heard from Professors Diab and Geist, Apple, Meta, and others; I'll use my time to explain why light amendments cannot do the job of making this Bill safe.

In recent weeks, the Minister has said the government will amend C-22 to bring it in line with our allies' lawful access — like America's CALEA. So let's compare. C-22 can require telecom companies, online services, and even hardware makers to let the government install surveillance equipment on their platforms, and to retain a year of metadata on every person in Canada. That isn't catching us up to CALEA — the two aren't in the same league. CALEA covers only telecom companies and requires no metadata retention, nothing approaching a year's data on everyone by default. Of the Five Eyes, only Australia mandates mass metadata retention — and there it's deeply controversial, and being reformed.

Taking a step back: in the modern threat environment, CALEA is not a success. CALEA has been in effect since the 1990s, but in recent years, the backdoors required by CALEA are increasingly a key entry point for foreign hackers to compromise US privacy. In 2024, Chinese state hackers used it to compromise the systems of America's largest telecoms, affecting more than a million people. Just this February, the FBI found CALEA's backdoors had led to breaches in their systems, and reported it to Congress as a major security failure. We aren't catching up to a working global standard; we're leapfrogging well beyond what any ally has done, creating a more vulnerable version of a system that's failing other governments.

What about the Minister's promise that selective amendments can fix the bill? The security and legal experts you've heard have been clear: this bill will not protect encryption in any way that matters. The government's promise is to provide a narrow, technical protection — that C-22 won't force a company to break encryption. But breaking encryption as a standard and defeating

it are not the same thing. A working lock is no protection if you're required by law to leave the door open. C-22's capability orders can compel a provider to build in access to information before it's encrypted or while it's temporarily decrypted — at the device level, within software, or as data is being handled. None of that breaks encryption as a standard; all of it circumvents the protection encryption is meant to provide. That's a foundational problem of C-22, not a simple definitional problem to fix.

In fact, this Bill is written to make sure none of its definitions can actually protect Canadian rights. Much is made of the difference between an electronic service provider and core electronic service provider, with the strongest default obligations on core providers; although the government will decide who a core provider is later, by regulation. But section 7(1) lets the Minister impose any obligation that a core provider faces on *any* service provider. Because these orders have no gazetting requirement, counter–intuitively, every invasive requirement a core provider faces can be applied to any provider — with *less* public scrutiny.

The same logic — maximal flexibility, ineffective by design safeguards — governs the definition of systemic vulnerability. That definition today isn't good enough; but even a strengthened, good-faith version won't fix C-22, because section 47(1)(c) explicitly grants Cabinet the regulatory power to reinterpret any term used in the bill.

As the case for Bill C-22 has crumbled, the Minister has claimed that opposition is driven by foreign Big Tech firms attacking Canadian sovereignty. That's plainly not true. Canadian tech success stories like Windscribe and Shopify have rallied against this broken bill as strongly as anyone. OpenMedia's community has sent nearly 25,000 messages to MPs opposing C-22 and Bill C-2 before it, and helped rally more than 300 organizations against C-2's privacy provisions. We don't take a dollar from Big Tech; our budget comes from small donations by ordinary people in Canada. The truth is that Big Tech firms were late to this conversation, and it was ordinary Canadians who sounded the alarm from day one.

The Minister has said that the government wants to have a filing cabinet of every Canadian's metadata ready for law enforcement when they need it. To that, I say that democracies do not keep a filing cabinet of every citizen's sensitive information in case it's useful to spies or police.

This process has been pushed so quickly that the system is not keeping up. OpenMedia submitted our brief more than two weeks ago, on May 15th, yet due to the sheer volume of input you've received, I learned today committee members have not yet received it. This is a symptom of a rushed, under-resourced process for a bill that has massive stakes. On behalf of our community, I urge you to take the time to receive and review all the public evidence, and thoroughly reform or abandon Part 2 of C-22 before moving it forward.

Thank you, and I look forward to your questions.