Bill C-22, An Act respecting lawful access

Brief to the Standing Senate Committee on National Security, Defence and Veterans Affairs

Submitted October 23, 2026

Summary

I'm Garo Brik, an independent technologist and volunteer with Technologists for Democracy (TfD): a Canadian grassroots advocacy organization composed largely of technologists, whose mandate is to advocate for responsible and ethical use of technology.

I'm writing because Bill C-22 as written will:

- be **ineffective in its stated goal** to facilitate the investigation of illegal activity;
- create a **major threat to privacy** by mandating the retention of user metadata and providing personal information to authorized persons (i.e., law enforcement agents)**;**
- force ordinary Canadians, and especially vulnerable populations, into using digital tools that provide worse privacy and safety protections, **opening the door for Canadians to be exploited by criminals and foreign actors**; and
- **fail to address core deficiencies in our digital infrastructure** that lead to fraud and other digital crimes.

I won't belabour the arguments made by the Chamber of Commerce, Mozilla, Signal, Proton, the Canadian Civil Liberties Association, Apple, Google, the Canadian Bar Association, and 57 other organizations[1] since the Bill was amended. Instead this brief will focus on the most important or least discussed flaws of the Bill.

[1] ACT | The App Association, Access Now, Apple, ARTICLE 19, BC Freedom of Information and Privacy Association (BC FIPA), Beauceron Security, Bits of Freedom, British Columbia Civil Liberties Association (BCCLA), Canadian Bar Association, Canadian Chamber of Commerce, Canadian Civil Liberties Association (CCLA), Canadian Muslim Public Affairs Council (CMPAC), Centre for Free Expression (CFE), Chamber of Progress, Clinique pour la justice migrante, Coinbase Canada, Council of Canadians, Digitalcourage, Dyne.org Foundation, easyDNS Technologies, Electronic Frontier Foundation (EFF), Electronic Frontier Norway, Epicenter.works, ESWA, European Digital Rights (EDRi), Figment Inc., GoBolt, Google, Homo Digitalis, HOPR, i2Coalition, IFEX, Informal Systems, Initiative für Netzfreiheit, International Civil Liberties Monitoring Group (ICLMG), IT-Pol Denmark, Justice Centre for Constitutional Freedoms, Kape Technologies (ExpressVPN, Private Internet Access), Le Centre de Réfugiés / The Refugee Centre, Liga voor Mensenrechten vzw, Ligue des droits et libertés, Metrics Chartered Professional Accounting, Mozilla, Nord Security (NordVPN, NordPass), Nym Technologies, Open Rights Group, OpenMedia, Opt Out Rights, Osservatorio Nessuno OdV, Petrichor Labs, Privacy and Access Council of Canada, Proton, Psiphon, SHARE Foundation, Shopify, Signal, Software & Information Industry Association (SIIA), Start Point Organization, Stop Killing the Internet, Table de concertation des organismes au service des personnes réfugiées et immigrantes (TCRI), Tailscale, Tucows, Tuta, Vocdoni Association, Windscribe

2. Principles for Digital Safety and Freedom

2.1 The Right to Privacy

Canadians must be able to choose electronic service providers (ESPs) based on their privacy and security practices — without government interference. Modern digital privacy and security practices dictate that personal data should be treated as a toxic asset: treated with caution, kept only when necessary, and handled with proper safeguards. Blanket orders to retain all users' location and communication metadata are completely incompatible with these principles.

Privacy-preserving ESPs must not be criminalized. A large and growing number of such organizations are declaring the incompatibility of their services with this Bill, even after the amendments that have already been made. In the void they leave behind, privacy-preserving tools will be relegated to the purview of criminals, while ordinary users will lose all access to digital privacy.

The Government of Canada should *not* be granted the power to *force* Canadians to only use metadata-retaining ESPs. Nor should the Government be able to prevent Canadians from knowing whether their ESPs are retaining their information.

At minimum, the following amendments are needed to ensure the Bill respects privacy:

- The Government should have no power to *compel* any ESP to retain user data.
- The Government should have no power to *secretly* compel any ESP to modify its capabilities.

2.2 Digital Sovereignty and International Co-operation

The vast majority of Canadian digital communication takes place on platforms owned and operated internationally. The powers granted by a lawful access regime can only be effective if they are compatible with the jurisdictions that control the technology Canadians use.

Canada is currently seeking greater alignment with the European Union, a global leader in advancing digital rights. Many aspects of the Bill are incompatible with those rights, jeopardize future Canadian inclusion in the Union, and **will be unenforceable in practice against providers in that jurisdiction.**

Similarly, **multiple US officials and organizations have declared the Bill's incompatibility with that jurisdiction's lawful access regime**.

Any data-sharing treaty with these countries may therefore expose Canadians' data without actually granting Canadian law enforcement access to the data they need. The Bill will then create a situation where ESPs cannot operate in Canada, Canadian law enforcement cannot access the data they need, and foreign governments have unfettered access to Canadians' data.

All of the following elements of the Bill contravene US or EU law, and should be removed:

- ordering the production of any kind of information without judicial review;
- ordering the modification of an ESP's capabilities;
- any kind of mandatory data retention; and
- any kind of exception in the definitions of decryption or system vulnerability.

2.3 Modern Access Regimes

The Bill's authors argue that our current lawful access regime is inadequate compared to our Five Eyes peers (i.e., Australia, New Zealand, the United Kingdom, and the United States). The Bill itself, however, does not mirror those countries' lawful access regimes. Every single one of those countries applies its lawful access regime only to telecoms and ISPs.
The Government has repeatedly dismissed concerns raised by technology companies, saying they continue to operate in countries with lawful access regimes. This ignores the fact that those countries' lawful access regimes **do not target those companies.**

We should follow the example of our peers, and amend the Bill as follows:

- The definition of ESP in the Bill should be constrained to refer to telecoms and ISPs, and not modifiable by regulation.

2.4 Software Supply Chain Security

The Act invokes the notion of a vulnerability which creates "a risk that relates only to information related to persons with respect to whom a warrant [...] applies." While conceptually appealing, modern software distribution practices allow users to verify that they have received the same version of software as every other user. Any ESP which prioritizes protecting its users would not have the capacity to distribute a targeted vulnerability like the Bill imagines. Retaining this provision in the Bill creates the potential for confusion and misapplication of modern software security standards.

The following exception therefore *must* be removed from the Bill:

- The definition of systemic vulnerability should contain no exception for targeted application.

3. A Progressive Approach

Section 2 above presents extensive amendments to Part 2. If all amendments are deemed sensible and applied, the Bill will be a substantially different piece of legislation. A simpler option for making progress on lawful access is to **reject Part 2, and approve Part 1**. This allows us to:

- make progress on lawful access now, protecting Canadians and bringing our regime into alignment with our peers;
- give the House of Commons the opportunity to use the feedback it has gained throughout this process to write a new version of Part 2 which is compatible with other jurisdictions and does not expose Canadians to undue risk or harm; and
- prevent the Senate from taking on too great a role in rewriting legislation.

4. How to Actually Protect Canadians

As we discuss the question of how to ethically protect Canadians from digital crime, it may be instructive to instead consider the following modern protections that can prevent fraudulent and criminal activity on the internet:

- fix the security deficiencies that allow phone number spoofing in Canada, a flaw commonly exploited by scammers to project legitimacy;
- end the widespread practice of promoting fraud and scams through digital advertising markets by holding companies responsible for fraudulent advertisements displayed to their users; and
- proliferate trusted digital ID services through government-affiliated institutions (e.g., libraries and post offices) that Canadians can use to verify the identities of the people they interact with digitally.

These and other simple and effective protections can drastically reduce the amount of digital risk Canadians experience every day without posing any risk to our privacy or unduly increasing the power of law enforcement.

5. Closing

Thank you for your time and consideration of these amendments. I and other members of TfD are available to the committee to provide further consultation, especially on technical aspects of the Bill.

Let us seek to advance the parts of this Bill that protect Canadians, and reconsider those parts which leave us more vulnerable.