From: khasir.hean@gmail.com
To: SECU@parl.gc.ca
cc: techfordemocracy.ca@gmail.com

Date: Friday, May 22, 2026, 2:23:49 PM
Subject: Comment on Bill C-22 - Technologists for Democracy

Dear members of the Standing Committee on Public Safety and National Security:

On behalf of Technologists for Democracy, I am writing to provide our perspective on Bill C-22, An Act Respecting Lawful Access. Technologists for Democracy is a grassroots organization composed largely of technologists, whose mandate is to advocate for responsible and ethical use of technology.

We **do not support Bill C-22** as it is written, as we are concerned that it **opens the door for Canadians to be exploited by criminals and foreign actors**.

Our three main concerns are as follows:

1. **Retaining user metadata and providing personal information to authorized persons** (i.e., law enforcement agents) **is a major threat to privacy.**
2. **Providing information to authorized persons is a major threat to cybersecurity** and is fundamentally incompatible with the concept of end-to-end encryption.
3. **Bill C-22 may inadvertently lead to the creation of vulnerabilities that can be exploited by malicious actors**, and is a **major threat to digital sovereignty**.

Retaining data and information always comes with the risk of information leakage, as protocols are not properly followed, or new vulnerabilities are discovered. In a digital context, the nature of computing means that zero-day vulnerabilities (i.e., exploits which no one was previously aware of) are always possible. By providing access to information to authorized persons, there is no guarantee that malicious actors will not be able to also access said information.

Additionally, many electronic service providers provide communication services with end-to-end encryption (E2EE). This means that only the sender and recipient are able to access messages sent amongst each other. The security of such a system is not guaranteed, of course, but limiting access to fewer persons reduces the risk of vulnerability and points of failure. Providing access to authorized law enforcement agents would reduce the security of E2EE systems and contravene the fundamental privacy-first philosophy of E2EE.

In terms of digital sovereignty, malicious actors from anywhere in the world would have additional opportunities to exploit Canadian data. This Lawful Access Act would require the retention of metadata and provisioning of access to authorized law enforcement agents, both of which increase the risk of data leakage as previously mentioned. We are highly concerned that this Bill would only act to increase the risk of foreign interference and loss of control over Canadian data.

Personal data should be treated as a toxic asset: treated with caution, kept only when necessary, and handled with proper safeguards.

We urge the Committee to seriously reconsider Bill C-22 and reject it as written.

Sincerely,

Khasir Hean, on behalf of Technologists for Democracy
Organizer & Machine Learning Engineer

TfD techfordemocracy.ca