Open letter from European civil society organisations on encryption and privacy threats in Canada's Bill C-22

To:

Ursula von der Leyen, President of the European Commission
Maroš Šefčovič, Commissioner – Trade and Economic Security
Michael McGrath, Commissioner – Democracy, Justice, the Rule of Law and Consumer Protection
Members of the European Parliament

We, the undersigned organisations and experts, write to urge you to act before Canada's Senate completes its consideration of Bill C-22, the Lawful Access Act, and to press Canada to remove the bill's surveillance capability mandates and its blanket data retention regime. The bill was referred to Canada's Senate in June of this year, which is the bill's second and final stage in Parliament before it becomes law. The Senate committee's study of the legislation will commence after Parliament resumes its fall sitting dates in late September, and could be concluded as early as October of this year.

This is not a domestic Canadian matter. Bill C-22 reaches any provider whose services are used by people in Canada, any Canada-based provider whose services are used by people outside Canada, and to providers with no Canadian users at all, if they have a Canadian entity or are an entity belonging to a corporate group that carries out any business activity in Canada. It would allow a Canadian minister to order a European company, in secret, to weaken the security of products used across the EU, and to retain the metadata of European users. It would also do so as the EU and Canada negotiate a Digital Trade Agreement and deepen the integration of their digital economies.

Bill C-22 has been widely criticised, including by the Internet Architecture Board and members of the Global Encryption Coalition. Bipartisan members of the United States Congress have written directly to Canada's Minister of Public Safety, warning that the bill would degrade cybersecurity. Europe should not stay silent.

- **The bill mandates capabilities that break security for everyone.** It compels an unidentified class of "electronic service providers", such as messaging apps, cloud storage, connected vehicles, camera networks, and health trackers, to develop "any form of technical capability" and to host any device, equipment etc., enabling government access. The exception for "systemic vulnerabilities" in "electronic protections" does not save it, as non-systemic vulnerabilities remain permitted; systemic ones may be pushed into other network components, and the government retains wide discretion over the definitions. A capability built to compromise one target is a reusable weakness against every other user. The stated intention of using the bill only for targeted surveillance does not match with the language in the proposal, which could facilitate mass surveillance through weakened security systems or backdoors enabling access to data.

- **The bill does not prohibit orders that defeat end-to-end encryption.** Canada's government rejected explicit prohibitions sought by the Privacy Commissioner of Canada, Signal and others, who testified that the law should bar measures that negate the purpose of encryption without touching encryption directly. The narrow amendment permitting objection to "decryption" orders leaves the most damaging techniques on the table that effectively undermine end-to-end encryption: client-side scanning, compelled hidden accounts inside encrypted chat groups, and engineered entry points of the kind zero-click spyware exploits. The European Parliament has repeatedly opposed the weakening of encryption, most recently by excluding end-to-end encrypted communications from the scope of Regulation (EU) 2026/1881 on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse. The ECHR has held that weakening encryption for all users of a service cannot be necessary in a democratic society. Bill C-22 rests on the premise the Court rejected.
- **Its metadata retention is irreconcilable with EU law and will jeopardise Canada's adequacy status in the EU.** There are no required limits on which Canadian or foreign agencies may access the data, on what the providers may do with the retained data, or on its fate when the period ends. The European Court of Justice has held repeatedly (Digital Rights Ireland, Tele2/Watson, La Quadrature du Net) that the general and indiscriminate retention of telecommunications traffic and location data is incompatible with the Charter. In Opinion 1/15, it rejected the EU-Canada PNR Agreement partly for the absence of such safeguards in Canadian law. Nothing since has changed: Canada's federal privacy law dates from 2000, and Canada is not a party to Convention 108+. Without any restrictions on general and indiscriminate data collection for broadly defined purposes, European data will be swept into Canada on terms EU law forbids and stockpiled in a form that invites attack.
- **Secrecy is the default, and Europe will have no remedy.** Under Bill C-22, secrecy attaches automatically to capability obligations; exemptions are discretionary and refusable for any reason. There is no independent judicial authorisation, only review, which can be deferential and limited in the admissibility of evidence, and in right of appeal. Service providers are required to give fifteen days' notice to the minister before they are able to file a challenge, and have to comply in the meantime. The United Kingdom's notice to Apple shows what follows: the Home Office fought to conceal the existence of proceedings, and when U.S. legislators sought relief from secrecy, the tribunal found it had no power to grant it. Where a Canadian minister targets an EU provider or EU data, no affected user or institution will have recourse to the European Court of Human Rights.

We therefore ask you to:

1. Call for the removal of Bill C-22's sweeping surveillance capability and metadata retention mandates.
2. Call for the introduction of a provision that categorically prevents any measures that would, directly or indirectly, undermine or weaken end-to-end encryption.
3. Call for amendments to Bill C-22 to ensure alignment with the principles of necessity, proportionality, and strict access limitations, for data retention, storage, and use.
4. Raise Bill C-22 in the Digital Trade Agreement negotiations with Canada. A partner cannot credibly seek deeper digital integration while legislating the power to compel European providers to weaken their products in secret.
5. Initiate a review of Canada's adequacy under Article 45(4) GDPR, and clarify what safeguards transfers to Canada would require should the bill pass as drafted. If no appropriate safeguards could be implemented, use the European Commission's powers to suspend the adequacy pursuant to Article 45(5).
6. Support an oral question on Bill C-22's implications for people in the EU addressed to the European Commission according to Rule 142 of the European Parliament's Rules of Procedure with a resolution.
7. State publicly that measures weakening encryption are incompatible with the EU's own commitments to cybersecurity and fundamental rights and that Bill C-22 will not be treated as a precedent for policy-making.

Canada's government advanced this bill while curtailing debate and refusing the amendments experts across the spectrum proposed. The Senate is the last opportunity to correct it. We ask you to use the influence the European Union holds, and to use it now.

Signatories

- Access Now
- ARTICLE 19
- Bits of Freedom
- Digitalcourage
- Electronic Frontier Norway
- Epicenter.works – for digital rights
- ESWA
- European Digital Rights (EDRi)
- Homo Digitalis
- Initiative für Netzfreiheit
- IT-Pol Denmark
- Liga voor Mensenrechten vzw
- Open Rights Group
- Osservatorio Nessuno OdV
- SHARE Foundation

- Stop Killing the Internet