21 April, 2026

The Right Honourable. Mark Carney, P.C., O.C., M.P.
Prime Minister of Canada

The Honourable Gary Anandasangaree P.C., M.P.
Minister of Public Safety

The Honourable Sean Fraser P.C., M.P.
Minister of Justice and Attorney General of Canada

The Honourable Pierre Poilievre P.C., M.P.
Leader of the Official Opposition

Mr. Yves-François Blanchet M.P., Leader, Bloc Québécois
Mr. Avi Lewis, Leader, New Democratic Party
Ms. Elizabeth May O.C., M.P., Leader, Green Party of Canada

CC: All Members of Parliament, House of Commons, Ottawa, Ontario, K1A 0A6

Version française incluse ci-dessous

Joint Call for the Withdrawal of Bill C-22

Dear Prime Minister, Ministers, and Honourable Leaders of the Opposition,

We, the undersigned organizations and individuals, are writing to call for the full withdrawal of Bill C-22, *An Act respecting lawful access*. Despite modest improvements since its predecessor, Bill C-2, Bill C-22 continues to create an unprecedented and extraordinarily dangerous surveillance architecture that could impact every digital tool people in Canada depend on every day. Without any consultation, Bill C-22 also adds sweeping new powers that were absent from Bill C-2 and could compel any digital service provider to record and keep comprehensive data on the digital life of every single person in Canada.

The enormous overreach of Bill C-22 and the unprecedented, open-ended powers it introduces are the latest in a series of legislative expansions of state power in recent legislation– bills that, individually and collectively, pose a dire threat to human rights in Canada.

If adopted as-is, Bill C-22 will be the most expansive invasion of Canadian privacy rights in modern history, and will put the cybersecurity of everyone in Canada at unacceptable risk. We urge you to withdraw Bill C-22, reconsider its problematic elements, and commit to meaningful public consultations on this legislative package.

Under Part 2 of Bill C-22, the government can transform any digital service into a state surveillance tool

Part 2 of Bill C-22, the *Supporting Authorized Access to Information Act* (SAAIA), is fundamentally a mass surveillance capabilities regime. Under proposed sub-sections 5(2) and 7(1) of Part 2, the government could force the creation and installation of privacy-compromising surveillance tools and backdoors in an enormous and ill-defined set of "electronic service providers", including telecom providers, social media and cloud service providers, AI tools, and any "smart" device. The law could even be used to force Canadian companies to build backdoors into their products before they export them abroad. The result creates an untenable threat to privacy and cybersecurity, and far exceeds powers available to police and security agencies in the United States. It is not clear on what basis this significant overbreadth can be justified.

Newly added safeguards in Part 2 of Bill C-22 do not address its fundamental problems.

The government has added some new safeguards to Part 2 of Bill C-22, but these fail to address fundamental flaws in the proposal. The Bill's definition of systemic cybersecurity vulnerability is compromised by design and, like *all* definitions in Part 2, can be redefined by the government in the future under section 47(1)(c).

Similarly, while some Part 2 orders now require approval from the Intelligence Commissioner, even this protection relies on a national security framework with unopposed and presumptively secret hearings, failing the baseline test for accountability, transparency, and procedural fairness.

New proposal in Part 2 of Bill C-22 would force companies to record and retain every single person's location and digital interaction data

Without any prior public consultation or notice, Part 2 of Bill C-22 will now also empower the government to require any digital service provider to record and retain detailed metadata on *every* single person in Canada or abroad, damaging the privacy of millions who are not suspected of committing any crime or posing any security threat. Combined with Part 2's other components, companies will be forced to develop the capacity to track information that was never before available to them and is not necessary for their business purposes, then to collect and retain that information for up to one year. These novel requirements would dramatically expand the pool of our sensitive data held by hundreds of services, creating tempting targets for bad actors and risking the safety of millions.

This blanket power to force creation of population-wide data troves – including our physical movements, who we interact with online, and when we've used these services – has no precedent in Canadian history. Bill C-22 places no limits on the purposes for which these data troves can then be accessed by government agencies. These powers will also operate as an

exception to our privacy laws, meaning private companies impacted by the bill will be able to use these forcibly created data troves for their own commercial ends.

Bill C-22 paves the way for expanded information-sharing with foreign governments with poor human rights track records

Bill C-22 could facilitate Canada's adoption of controversial information-sharing agreements and may therefore implicate Canada in transnational repression.

Elements of Bill C-22 erode key privacy protections in a manner that would align Canadian and U.S. surveillance practices despite key constitutional differences. First introduced in Bill C-2 in direct response to U.S. pressure, these changes could clear the path to adoption of an expanded information-sharing agreement Canada has been negotiating with the U.S. since 2022.

Once Bill C-22 becomes law, Canada will also be in a position to adopt a controversial information-sharing treaty it signed in 2023, compelling it to share information with any other treaty party, including a number of eligible state signatories that have a history of abusing cross-border policing mechanisms to persecute diaspora communities.

Canada's privacy and cross-border information sharing safeguards have not kept pace with the growing threat of cross-border surveillance, a threat that is particularly acute if information-sharing with the U.S. is expanded without addressing the general lack of enforceable Canadian privacy rights in U.S. law. Aggressive information-sharing with the US has led to severe negative consequences for people in Canada in the past, including illegal detention and torture.

Expanded powers to access customer data improved, but remain flawed

Bill C-22 makes some improvements to Bill C-2's proposal for wide-ranging warrantless access to sensitive subscriber information. The warrantless demand power can now only be used to require telecommunications service providers to confirm if someone is a customer. However, Bill C-22's approach to subscriber data remains flawed, dropping the judicial authorization standard for a warrant from "reason to believe" to the far lower "reason to suspect" threshold despite Supreme Court decisions recognizing the significant privacy interests engaged by this form of data access.

Ossified oversight cannot limit abuse of Bill C-22

Bill C-22 represents a dramatic expansion of Canada's surveillance capabilities while key safeguards remain stagnant. Critical oversight bodies like the Office of the Privacy Commissioner (OPC) and the National Security and Intelligence Review Agency (NSIRA) are increasingly under-resourced and compelled to carry out their expanding tasks with outdated powers. Indeed, Canada's key privacy law, the *Privacy Act*, relies on safeguards adopted in the 1980s and is no longer fit for purpose.

The evidentiary record weighs against Bill C-22

Bill C-22 also represents an abandonment of evidence-based policy-making. It remains technologically impossible to create backdoors for use by Canadian law enforcement and security agencies alone. All such measures become permanent architectural features — available to be probed, exploited, and compromised by foreign intelligence services and criminal actors who need no legal authority to use them.

The 2024 Salt Typhoon attack on US telecommunications networks– which has been declared a "national defence crisis"–and recent intrusions into the FBI's systems targeted exactly the kind of government mandated backdoors to telecom infrastructure Bill C-22 would now impose on *every* digital service. Worse, it could place an unprecedented full year of metadata on every person in Canada and abroad as the pot of gold for every hacker and hostile state who passes through these doors.

Accordingly, we call on all Members of Parliament to reject Bill C-22; and we call on the government to commit to meaningful, good faith and evidence-based consultation with the public regarding these and any future proposals to expand surveillance powers in Canada.

Signed as Organizations:

1. British Columbia Civil Liberties Association
2. Canadian Anti Monopoly Project (CAMP)
3. Canadian Association of University Teachers (CAUT)
4. Canadian Civil Liberties Association / l'Association canadienne des libertés civiles
5. Canadian Council for Refugees
6. Canadian Muslim Public Affairs Council (CMPAC)
7. Centre for Free Expression (CFE)
8. Clinique pour la justice migrante / Migrant justice clinic
9. International Civil Liberties Monitoring Group
10. Ligue des droits et libertés
11. Migrant Workers Alliance for Change
12. OCASI - Ontario Council of Agencies Serving Immigrants
13. OpenMedia
14. Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic (CIPPIC)

Signed as Individuals:

1. Safiyya Ahmad, Lawyer
2. Noura Aljizawi, Senior Researcher, Citizen Lab, Munk School of Global Affairs & Public Policy, University of Toronto
3. Brent Arnold, Capstan Legal
4. Jane Bailey, Professor, University of Ottawa Faculty of Law
5. Colin Bennett, Professor Emeritus at the University of Victoria

6. Andrew Clement, Professor Emeritus at the University of Toronto
7. Ron Deibert, Director of the University of Toronto's Citizen Lab
8. Lex Gill, Senior Fellow, Munk School of Global Affairs & Public Policy, University of Toronto
9. Pantea Jafari, Jafari Law
10. Mark E. Jeftovic, CEO at easyDNS Technologies Inc.
11. Michael Karanicolas, Associate Professor and James S. Palmer Chair in Public Policy & the Law, Dalhousie University
12. Shera Kelly, Individual
13. Kate Robertson, Senior Research Associate, Citizen Lab, Munk School of Global Affairs & Public Policy, University of Toronto
14. Teresa Scassa, Canada Research Chair in Information Law and Policy, Professor at the University of Ottawa
15. Maria Vamvalis, PhD