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

May 4, 2026

Open Letter Calling for Amendments to Bill C-22

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

We write as lawyers and law professors who teach and practice in the areas of privacy law and constitutional rights in Canada. We welcome the effort that has gone into revising the lawful access framework since Bill C-2. Bill C-22 marks an improvement over its predecessor in several respects. But certain provisions of the bill as currently drafted raise serious constitutional concerns and fail to strike a reasonable balance between the legitimate needs of law enforcement and the privacy rights of Canadians. We urge Parliament to carefully consider the following issues before the bill proceeds further.

First, the new production order for subscriber information, to be added to the *Criminal Code* as section 487.0142, retains a legal threshold that is too low and a scope of disclosure that is too

broad. As affirmed by the Supreme Court of Canada's decision in *R v Spencer*, Canadians have had a strong privacy interest in anonymity online. The existing general production order — available since 2004 and readily obtained by telewarrant — already gives police an effective tool to link an IP address or phone number to a named subscriber, and requires them to establish reasonable grounds to believe that an offence has been committed. Bill C-22 creates a new, dedicated subscriber information order that reduces that standard to reasonable grounds to suspect. The courts have held that this distinction is not semantic: in *R v West*, the Ontario Court of Appeal excluded evidence obtained through a production order precisely because the officer had established only grounds to suspect rather than grounds to believe.

The scope of disclosure under the new order is a further concern. Although the definition of subscriber information has been narrowed compared to Bill C-2, the order still allows for production of a broad scope of information, including the types of services provided and the identifiers of every device associated with the account. This goes well beyond what is needed to connect a name to an IP address. It can be directed to a physician, a cable company, or a platform like iCloud, requiring disclosure of what cable packages a person subscribes to, what medical services they receive, or what devices they use. Much of this information carries a high privacy interest and calls for a higher legal standard. If Parliament seeks to create a subscriber information order that can withstand scrutiny under section 8 of the *Charter*, it should narrow the scope to basic identifying information — name, address, and the specific account identifier in question — and raise the threshold to reasonable grounds to believe.

Including analogous powers in the *Canadian Security Intelligence Service Act* (CSIS Act) raises even greater issues. Unlike criminal defendants, "persons of interest" to CSIS are never given an opportunity in court to challenge the intrusion of state power into their private lives. The *Charter* concerns are more acute with CSIS, and the Service should have to satisfy a "reasonable grounds to believe" threshold for all of these authorities.

Second, we are concerned that Bill C-22 introduces mandatory metadata retention without the constitutional basis to support it. Section 5(2)(d) of the *Supporting Authorized Access to Information Act* (SAAIA) in Part 2 of the Bill would authorize regulations requiring "core providers" to retain categories of metadata, including transmission data capturing the date, time, duration, type, and location of every communication, for up to one year. This amounts to a blanket obligation to preserve a detailed record of the movements and associations of every Canadian who uses a regulated service, with no requirement for individualized suspicion.

This kind of general and indiscriminate retention of metadata about entire populations has been rejected by the Court of Justice of the European Union as a disproportionate interference with fundamental privacy rights, and similar domestic retention laws have been struck down by the constitutional courts of several EU member states. The Canadian courts are likely to reach the same conclusion. Parliament's own judgment on this question is instructive. The current *Criminal Code* scheme for "preservation demands" and "preservation orders" has long proceeded on the assumption that compelling a provider to preserve personal data engages section 8 of the *Charter* and requires authorization — either lawful grounds or a warrant. A blanket obligation to retain the metadata of millions of Canadians for up to a year without any individualized trigger is not consistent with section 8 and will not survive a constitutional challenge.

Third, the SAAIA's surveillance-capability framework raises serious concerns about both the security of Canadians and the rule of law. The Act imposes sweeping obligations on "core providers" and potentially on any "electronic service provider" (ESP) to develop, implement, test, and maintain technical capabilities for law enforcement access, including capabilities related to extracting and organizing information. A more balanced approach would limit the scope of these powers to preclude an obligation to (i) make changes to products or services that a business provides in the ordinary course of business, (ii) collect and retain any data beyond

what the business requires for its own purposes, and (iii) make any changes that would affect the functionality (including ordering additional functionality) for any products or services offered by the business.

When initially proposed in Bill C-2, the SAAIA had also raised concerns about the meaning of "systemic vulnerability." This is now defined in Bill C-22 and service providers are not required to comply with an order under the act if compliance would introduce a "substantial" risk of unauthorized access to "secure" information. But the definition of the term remains too narrow. It requires an excessive threshold of substantiality of risk that inherently exposes persons and data in Canada to cyber adversaries and national security threats. Moreover, the definition applies only to vulnerabilities in the electronic protections of an electronic *service*, meaning it may not extend to the operating systems of devices. A ministerial order could require a company like Apple or Google to build extraction capabilities into its operating system without triggering the safeguard, even if the practical effect would be to undermine end-to-end encryption or device security. The international experience under even narrower legislation — including the vulnerabilities exposed in United States telecommunications networks following the Salt Typhoon intrusion — illustrates concretely how mandated surveillance access creates security risks that adversaries can and do exploit. The legislative scheme further presumes that ESPs will all indeed object and pursue judicial review of orders that present cybersecurity and national security dangers, when international experience has taught that not all will do so.

The SAAIA framework also operates almost entirely in secret. Ministerial orders and conditions imposed on electronic service providers who are not core providers are subject to sweeping confidentiality requirements. There is no independent assessment of the necessity and proportionality of particular orders before they take effect, and no meaningful role for the Privacy Commissioner of Canada. The Intelligence Commissioner's approval is now required

for orders directed at non-core providers, but that office's mandate concerns national security and telecommunications infrastructure integrity, not the privacy of individual Canadians. Affected ESPs have no right to make representations to the Intelligence Commissioner. Parliament should subject ministerial orders and all provider obligations under the SAAIA to meaningful independent oversight, including review by the Privacy Commissioner, before they take effect. The Minister should also be required to justify, on a per-order basis, the need for secrecy associated with these orders, and any confidentiality requirements should sunset.

We recognize that the government has made an effort to address the most serious failings of Bill C-2. The changes made to the confirmation of service demand are an example of targeted reform in response to constitutional concerns. The concerns we have raised here are equally susceptible to targeted amendment.

Canadians deserve privacy protections that are consistent with the *Charter* and with the values that the Supreme Court of Canada has consistently affirmed. We offer these observations in the hope that they will contribute to a bill that can withstand the legal challenges that are certain to follow and that protects the security of all Canadians.

Yours sincerely,

Robert Diab
Professor of Law
Thompson Rivers University

Michael Karanicolas
Associate Professor of Law and Palmer Chair in Public Policy & Law
Schulich School of Law, Dalhousie University

David TS Fraser
Partner, McInnes Cooper
Adjunct faculty, Schulich School of Law at Dalhousie University

Michael Geist
Canada Research Chair in Internet and E-commerce Law
University of Ottawa, Faculty of Law

Cynthia Khoo
Principal Lawyer, Tekhnos Law
Senior Fellow, The Citizen Lab, University of Toronto

Lisa Austin
Professor of Law
Jackman Law, University of Toronto

Steve Coughlan
Professor of Law
Schulich School of Law, Dalhousie University

Suzie Dunn
Assistant Professor of Law
Schulich School of Law, Dalhousie University

Kate Robertson
Senior Research Associate
Citizen Lab, Munk School of Global Affairs & Public Policy, University of Toronto

Teresa Scassa
Canada Research Chair in Information Law and Policy
University of Ottawa

Matt Malone
Balsillie Scholar
Balsillie School of International Affairs

Katie Szilagyi
Associate Professor of Law
University of Manitoba

Matthew Dylag
Assistant Professor of Law

Schulich School of Law, Dalhousie University

*Academic affiliations listed for identification purposes only.