September 28, 2022

To:
The Honourable Marco E. L. Mendicino, P.C., M.P.,
Minister of Public Safety.

CC:
The Honourable François-Philippe Champagne, P.C., M.P.,
Minister of Innovation, Science and Industry.

The Honourable Pierre Poilievre, P.C., M.P., Leader of the Opposition
Yves-François Blanchet M.P., Bloc Quebecois Leader
Jagmeet Singh M.P., NDP Leader
Elizabeth May M.P., Green Party Parliamentary Leader

Joint Letter of Concern regarding Bill C-26

Dear Minister,

We, the undersigned organizations, are writing to express our serious concerns regarding Bill C-26: *An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts*.

In your press release announcing this legislation, you were quoted as stating *"In the 21st century, cyber security is national security."* We agree, and we share your goal of helping both the public and private sector better protect themselves against cyberattacks.

However, in its current form, Bill C-26 is deeply problematic and needs fixing. As drafted, it risks undermining our privacy rights, and the principles of accountable governance and judicial due process which are the fabric of Canadian democracy. The legislation needs to be substantively amended to ensure it delivers effective cybersecurity protections while safeguarding these essential democratic principles.

As you know, Bill C-26 grants the government sweeping new powers over vast swathes of the Canadian economy. We believe these powers need to be strictly delimited and accompanied by meaningful safeguards and reporting requirements to ensure Canadians can hold their government and security agencies to account. **Put simply, with great power must come great accountability.**

With a view to improving this legislation, we share with you the following specific areas of concern:

- **Opens the door to new surveillance obligations:** Bill C-26 empowers the government to secretly order telecom providers *"to do anything or refrain from doing anything."* This opens the door to imposing surveillance obligations on private companies, and to other risks such as weakened encryption standards — something the public has long rejected as inconsistent with our privacy rights.

- **Termination of essential services:** Under Bill C-26, the government can bar a person or company from being able to receive specific services, and bar any company from offering these services to others, by secret government order. This opens the door to Canadian companies or individuals being cut off from essential services without explanation. Bill C-26 fails to set out any explicit regime, such as an independent regulator with robust powers, for dealing with the collateral impacts of government Security Orders.

- **Undermines privacy:** Bill C-26 empowers the government to collect broad categories of information from designated operators, within any time and subject to any conditions. This may enable the government to obtain identifiable and de-identified personal information and subsequently distribute it to domestic, and perhaps foreign, organizations.

- **No guardrails to constrain abuse:** Bill C-26 lacks mandatory proportionality, privacy, or equity assessments, or other guardrails, to constrain abuse of the new powers it grants the government — powers accompanied by steep fines or even imprisonment for non-compliance. These orders apply both to telecommunications companies, and to a wide range of other federally-regulated companies and agencies designated under the *Critical Cyber Systems Protection Act (CCSPA)*. Prosecutions can be launched in respect of alleged violations of Security Orders which happened up to three years in the past.

- **Secrecy undermines accountability and due process:** Bill C-26 enables the government to shroud its orders in secrecy, with no mandatory public reporting requirements. While there is an understandable need for some degree of confidentiality in this sphere, the public needs to have a sense of how these powers are being exercised, how often, and to what effect, if decision-makers are to be held to account. Individuals and services collaterally impacted by Bill C-26 must also be given an opportunity to challenge Security Orders.

- **Unknowable orders trump public regulation:** Bill C-26 tilts the balance so far toward secrecy, its orders and regulations may take precedence over decisions previously issued by regulatory agencies, risking confusion where such regulatory decisions are public while the Security Orders are not. This threatens the integrity and accessibility of Canada's regulatory frameworks, and renders the security-related rules currently in effect unknowable for members of the public.

- **Secret evidence in Court:** Even if Security Orders are subjected to judicial review, Bill C-26 could restrict applicants' access to evidence. The legislation does not include any consideration of security-cleared advocates to be appointed on applicants' behalf, as happens in other national security cases. While such provisions are an imperfect solution for due process, they do provide at least a minimal level of protection for applicants' rights. C-26 even empowers judges to make rulings based on secret evidence that is not provided, even in summary form, to applicants or their legal team. It also places the onus on the target of Security Orders to bring legal proceedings, with the associated cost burden.

- **Power without accountability for the CSE:** The *CCSPA* would let the Communications Security Establishment — Canada's signal intelligence and cybersecurity agency — obtain

and analyze security-related data from companies that Canadians entrust with their most sensitive personal information. This would include federally-regulated banks and credit unions, telecommunications and energy providers, and even some transit agencies. The CSE's use of this information is not constrained to the cybersecurity aspect of its mandate, and any uses would be largely subject to after-the-fact review rather than real-time oversight, resulting in a significant deficit in democratic accountability.

- **Lack of Justification:** Although the government claims that such sweeping and secretive new powers are required it has not published any sufficiently comprehensive data establishing the necessity and proportionality of the proposed powers.

In sum, cybersecurity is important and we need to get it right: All residents of Canada can agree on the need for cybersecurity. However, civil liberties, privacy, and confidence in the rule of law and accountable governance are foundational for that sense of security. It is imperative that in its efforts to deliver strong cybersecurity for people in Canada, the government also ensures accountability and upholds basic rights.

As Bill C-26 moves through the legislative process, we look forward to working with you, and parliamentarians from all parties, to ensure it delivers strong cybersecurity for everyone in Canada, while ensuring accountability and upholding our rights.

Sincerely,

Canadian Civil Liberties Association
Canadian Constitution Foundation
International Civil Liberties Monitoring Group
Leadnow
Ligue des droits et libertés
OpenMedia
Privacy & Access Council of Canada

**

Dr. Christopher Parsons, Senior Research Associate at the Citizen Lab, Munk School of Global Affairs & Public Policy, University of Toronto

Tamir Israel, Digital Rights Lawyer

Andrew Clement, Professor Emeritus, Faculty of Information, University of Toronto

**

Sent Wednesday 28 September by OpenMedia on behalf of the above organizations and individuals.