Le 21 avril 2026

Le très honorable Mark Carney, C.P., O.C., député
Premier ministre du Canada

L'honorable Gary Anandasangaree, C.P., député
Ministre de la Sécurité publique

L'honorable Sean Fraser, C.P., député
Ministre de la Justice et procureur général du Canada

L'honorable Pierre Poilievre, C.P., député
Chef de l'opposition officielle

M. Yves-François Blanchet, député, chef du Bloc Québécois
M. Avi Lewis, chef du Nouveau Parti démocratique
Mme Elizabeth May, O.C., députée, chef du Parti vert du Canada

CC : Tous les députés, Chambre des communes, Ottawa (Ontario) K1A 0A6

Appel conjoint au retrait du projet de loi C-22

Monsieur le Premier ministre, Messieurs les Ministres et Madame et Messieurs les chefs des partis de l'opposition,

Nous soussignés, organismes et particuliers, vous écrivons pour demander le retrait total du projet de loi C-22, *Loi concernant l'accès légal*. Malgré de modestes améliorations par rapport à celui qui l'a précédé, le projet de loi C-2, le projet de loi C-22 continue de créer une architecture de surveillance sans précédent et extraordinairement dangereuse qui pourrait se répercuter sur chaque outil numérique sur lequel les personnes comptent chaque jour au Canada. Sans aucune consultation, le projet de loi C-22 ajoute également de nouveaux pouvoirs considérables qui étaient absents du projet de loi C-2 et qui pourraient contraindre chaque fournisseur de services numériques à enregistrer et à conserver des données exhaustives sur la vie numérique de chaque personne au Canada.

La portée énormément envahissante du projet de loi C-22 et les pouvoirs illimités sans précédent qu'il instaure constituent le dernier d'une série d'élargissements des pouvoirs de l'État dans la législation récente — des projets de loi qui, individuellement et collectivement, posent une menace redoutable pour les droits de la personne au Canada.

Si le projet de loi C-22 est adopté tel quel, il portera l'atteinte la plus vaste au droit canadien à la vie privée dans l'histoire moderne, en plus de compromettre de manière inacceptable la cybersécurité de tout le monde au Canada. Nous vous exhortons à retirer le projet de loi C-22, à revoir ses éléments problématiques et à vous engager à mener des consultations publiques sérieuses sur cet ensemble de mesures législatives.

En vertu de la partie 2 du projet de loi C-22, le gouvernement peut transformer chaque service numérique en outil de surveillance par l'État.

La partie 2 du projet de loi C-22, la *Loi sur le soutien en matière d'accès autorisé à de l'information*, est fondamentalement un régime aux capacités de surveillance de masse. En vertu des paragraphes 5(2) et 7(1) proposés à la partie 2, le gouvernement pourrait imposer à un éventail énorme de « fournisseurs de services électroniques », y compris les fournisseurs de services de télécommunication, les fournisseurs de médias sociaux et de services infonuagiques, les outils d'intelligence artificielle et tous les appareils « intelligents », la création et l'installation d'outils de surveillance et de portes dérobées qui compromettraient la confidentialité. Cette loi pourrait même être utilisée pour contraindre les entreprises canadiennes à construire des portes dérobées dans leurs produits avant de les exporter. Il en résulte une menace intolérable à la confidentialité et à la cybersécurité qui excède largement les pouvoirs des services de police et des organismes de sécurité aux États-Unis. La justification de la portée excessive de cette disposition est obscure.

Les protections ajoutées récemment à la partie 2 du projet de loi Bill C-22 ne résolvent pas ses problèmes fondamentaux.

Le gouvernement a ajouté de nouvelles protections à la partie 2 du projet de loi C-22, mais celles-ci ne remédient pas aux défauts fondamentaux de cette proposition. La définition de la vulnérabilité systémique de la cybersécurité dans le projet de loi est compromise à dessein et, comme *toutes* les définitions à la partie 2, elle peut être modifiée à l'avenir par le gouvernement en vertu de l'alinéa 47(1)c).

Dans le même ordre d'idée, certains arrêtés mentionnés à la partie 2 nécessitent maintenant l'approbation du commissaire au renseignement, mais même cette protection repose sur un cadre de sécurité nationale et sur des auditions sans opposition et vraisemblablement secrètes et échoue donc au test de référence en matière de responsabilité, de transparence et d'équité procédurale.

La nouvelle proposition dans la partie 2 du projet de loi C-22 contraindrait les entreprises à enregistrer et à conserver les données sur l'emplacement et les interactions numériques de chaque personne.

Sans consultation ni avis public préalables, la partie 2 du projet de loi C-22 conférera au gouvernement le pouvoir d'exiger que tous les fournisseurs de services numériques enregistrent et conservent des métadonnées détaillées sur *chaque* personne au Canada ou à l'étranger, portant ainsi atteinte à la vie privée de millions de personnes non soupçonnées d'avoir commis un crime ou de présenter une menace pour la sécurité. Ce pouvoir et les autres composantes de la partie 2 obligeront les entreprises à acquérir la capacité d'assurer le suivi de renseignements dont elles n'ont jamais disposé et qui ne sont pas nécessaires à leurs activités commerciales, puis à les collecter et à les conserver pendant un an. Ces nouvelles exigences accroîtraient de manière considérable l'ensemble de nos données sensibles détenues par des centaines de services, créant

ainsi des cibles tentantes pour les mauvais acteurs et mettant en péril la sécurité de millions de personnes.

Ce vaste pouvoir d'imposer la création de mines de données à l'échelle de la population — y compris sur nos déplacements physiques, sur les personnes avec qui nous interagissons en ligne et sur les moments où nous avons utilisé ces services — est sans précédent dans l'histoire canadienne. Le projet de loi C-22 n'impose aucune limite aux fins pour lesquelles les organismes gouvernementaux pourront ensuite accéder à ces mines de données. Ces pouvoirs dérogeront également à nos lois sur la protection de la vie privée, étant donné que les entreprises privées visées par le projet de loi pourront utiliser ces mines de données créées sous la contrainte pour leurs propres intérêts commerciaux.

Le projet de loi C-22 ouvre la porte à l'accroissement de l'échange d'information avec les gouvernements étrangers au piètre bilan en matière de droits de la personne.

Le projet de loi C-22 pourrait faciliter l'adoption par le Canada d'accords d'échange d'information prêtant à controverse et impliquer le Canada dans la répression transnationale.

Plusieurs éléments du projet de loi C-22 érodent les protections fondamentales de la vie privée d'une manière qui harmoniserait les pratiques de surveillance canadiennes avec celles des États-Unis, en dépit d'importantes différences constitutionnelles. Ajoutés au projet de loi C-2 en réponse directe aux pressions des États-Unis, ces changements pourraient ouvrir la voie à l'adoption d'une entente élargie d'échange d'information que le Canada négocie avec les États-Unis depuis 2022.

Quand le projet de loi C-22 entrera en vigueur, le Canada sera également en mesure d'adopter un traité controversé d'échange d'information qu'il a signé en 2023 et qui l'obligerait à communiquer des renseignements à toutes les parties au traité, y compris à plusieurs États signataires admissibles qui ont des antécédents de recours abusif aux mécanismes policiers transfrontaliers pour persécuter les communautés de la diaspora.

Les protections canadiennes de la vie privée et de l'échange transfrontalier d'information ne sont suivi le rythme des menaces croissantes de surveillance transfrontalière qui seront particulièrement graves, si l'échange d'information avec les États-Unis est accru sans remédier à l'absence générale de droits canadiens à la protection de la vie privée exécutoires en vertu des lois des États-Unis. L'échange d'information excessif dans le passé avec les États-Unis a entraîné de graves conséquences pour des personnes au Canada, y compris la détention illégale et la torture.

Des améliorations ont été apportées à l'accroissement de l'accès aux données sur les clients, mais il demeure déficient.

Le projet de loi C-22 a apporté quelques modifications à la proposition du projet de loi C-22 concernant l'accès de grande envergure et sans mandat aux renseignements sensibles sur les abonnés. Le pouvoir d'exiger ceux-ci sans mandat ne peut maintenant être utilisé que pour

demander aux fournisseurs de services de télécommunication si une personne fait partie de leur clientèle. En revanche, l'approche des données sur les abonnés demeure déficiente dans le projet de loi C-22 en faisant passer la norme de l'autorisation judiciaire pour un mandat de la « raison de croire » au seuil très inférieur de la « raison de soupçonner », malgré les décisions de la Cour suprême reconnaissant que d'importants droits à la vie privée sont en jeu dans cette forme d'accès aux données.

La surveillance rigide ne peut pas limiter l'utilisation abusive du projet de loi C-22.

Le projet de loi C-22 constitue un accroissement considérable des capacités de surveillance du Canada alors que les principales protections demeurent inchangées. Des organismes de contrôle, comme le Commissariat à la protection de la vie privée et l'Office de surveillance des activités en matière de sécurité nationale et de renseignement, sont dotés de ressources de plus en plus insuffisantes et doivent exercer leurs fonctions en pleine expansion en disposant de pouvoirs désuets. En effet, la principale loi du Canada sur la protection de la vie privée, la *Loi sur la protection des renseignements personnels,* s'appuie sur des mesures de protection adoptées dans les années 1980 et n'est plus adaptée aux besoins.

Le dossier de preuve joue contre le projet de loi C-22.

Le projet de loi C-22 représente également un abandon de l'élaboration des politiques fondées sur des données probantes. Il demeure techniquement impossible de créer des portes dérobées à l'usage exclusif des organismes d'application de la loi et de sécurité canadiens. Tous les dispositifs de ce genre deviennent des caractéristiques architecturales permanentes — mises à la disposition des services de renseignement étrangers et des criminels qui n'ont besoin d'aucune base juridique pour les scruter, les exploiter et les compromettre.

L'attaque de Salt Typhoon en 2024 sur les réseaux de télécommunications des États-Unis — qui a été déclarée une « crise de défense nationale » — et les récentes intrusions dans les systèmes du FBI ont ciblé précisément le genre de portes dérobées exigées par le gouvernement dans l'infrastructure de télécommunications que le projet de loi C-22 imposerait maintenant pour *chaque* service numérique. Pire encore, il pourrait imposer la rétention d'une année complète de métadonnées sur chaque personne au Canada et à traverseraient ces portes.

Par conséquent, nous demandons à tous les députés de rejeter le projet de loi C-22; et nous demandons au gouvernement de s'engager à une consultation du public constructive, de bonne foi et fondée sur des données probantes concernant ces propositions et les futures propositions d'élargissement des pouvoirs de surveillance au Canada.

Signatures au nom d'une organisation

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)

Signatures de particuliers

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